En säker och tillgänglig statlig e-legitimation

Delbetänkande av Utredningen om säker och tillgänglig digital identitet

Stockholm 2023

STATENS OFFENTLIGA UTREDNINGAR

SOU 2023:61

SOU och Ds finns på regeringen.se under Rättsliga dokument.

Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2021:1.
Information för dem som ska svara på remiss finns tillgänglig på regeringen.se/remisser.

Layout: Kommittéservice, Regeringskansliet
Omslag: Elanders Sverige AB
Tryck och remisshantering: Elanders Sverige AB, Stockholm 2023

ISBN 978-91-525-0730-8 (tryck)
ISBN 978-91-525-0731-5 (pdf)
ISSN 0375-250X

Till statsrådet Erik Slottner

Regeringen beslutade den 22 december 2022 att tillkalla en särskild utredare med uppdrag att utreda och lämna förslag på hur staten kan utfärda en e-legitimation på högsta tillitsnivå. Utredaren ska också se över behovet av anpassningar som följer av den reviderade eIDAS-förordningen.

Som särskild utredare förordnades från och med den 22 december 2022 rådmannen Henrik Ardhede.

Som huvudsekreterare i utredningen anställdes från och med den 9 januari 2023 hovrättsassessorn Helena Forsaeus. Som utredningssekreterare anställdes från och med den 9 januari 2023 seniora handläggaren Björn Scharin och från och med den 23 januari 2023 hovrättsassessorn Anna Carlson.

Som sakkunniga förordnades från och med den 7 februari 2023 kanslirådet Richard Halltell (Finansdepartementet), ämnessakkunnige Magnus Thomann (Justitiedepartementet), departementssekreteraren Johanna Wasteson Lundberg (Finansdepartementet) och departementssekreteraren Ylva Wide (Finansdepartementet). Samma dag förordnades som experter strategen Anneli Hagdahl (Myndigheten för digital förvaltning), rättsliga experten Johannes Holmström (Skatteverket), digitaliseringsstrategen Torbjörn Karlsson (Sveriges Kommuner och Regioner), verksamhetsutvecklaren Ulf Palmgren (Försäkringskassan), strategiska projektledaren Fresia Perez (Sunet), stf. operativa chefen Mikaela Rosenlind Magnusson (Sveriges Certifieringsorgan för IT-säkerhet vid Försvarets materielverk), näringspolitiske experten Fredrik Sand (TechSverige), inspektören Björn Seeth (Polismyndigheten), seniora handläggaren Gustav Söderlind (Myndigheten för samhällsskydd och beredskap) och enhetschefen Helene Thorgren (Bolagsverket).

Johanna Wasteson Lundberg entledigades från sitt uppdrag som sakkunnig den 24 april 2023 och samma dag förordnades rättssak-

kunniga Malin Wictor (Finansdepartementet) att vara sakkunnig i utredningen. Helene Thorgren entledigades från sitt uppdrag som expert den 11 september 2023 och samma dag förordnades verksjuristen Lena Göransson Norrsjö (Bolagsverket) att vara expert i utredningen.

Utredningen redogör för uppdraget med användande av vi-form även om det inte funnits fullständig samsyn i alla delar. Utredningen, som har tagit sig namnet Utredningen om säker och tillgänglig identitet, överlämnar härmed delbetänkandet *En säker och tillgänglig statlig e-legitimation* (SOU 2023:61). Till betänkandet fogas två särskilda yttranden. Återstående frågor som omfattas av utredningens uppdrag kommer att behandlas i slutbetänkandet i maj 2024.

Gränna i oktober 2023

Henrik Ardhede

/Helena Forsaeus
Anna Carlson
Björn Scharin

Innehåll

Förkortningar

EU-rättsakter

EU:s förordning om en gemensam digital ingång	Europaparlamentets och rådets förordning (EU) 2018/1724 av den 2 oktober 2018 om inrättande av en gemensam digital ingång för tillhandahållande av information, förfaranden samt hjälp- och problemlösningstjänster och om ändring av förordning (EU) nr 1024/2012
Dataskyddsförordningen	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG
eIDAS-förordningen	Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG
Genomförandeförordningen (EU) 2015/1502	Kommissionens genomförandeförordning (EU) 2015/1502 av den 8 september 2015 om fastställande av tekniska minimispecifikationer och förfaranden för tillitsnivåer för medel för

	elektronisk identifiering i enlighet med artikel 8.3 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

Övriga förkortningar

a.a.	anfört arbete
Brå	Brottsförebyggande rådet
CEN	European Committee for Standardization
Digg	Myndigheten för digital förvaltning
Dir.	Kommittédirektiv
Ds	Departementsserien
EU	Europeiska unionen
f./ff.	följande sida/sidor
ENISA	Europeiska unionens cybersäkerhetsbyrå
ETSI	European Telecommunications Standards Institute
ibid.	ibidem, eller på samma ställe, dvs. på samma sida/sidor som föregående fotnotsreferens
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
MSB	Myndigheten för samhällsskydd och beredskap

NBC	Polismyndighetens Nationella bedrägericentrum
PKI	Public Key Infrastructure
PTS	Post- och telestyrelsen
Prop.	Regeringens proposition
SGSI	Swedish Government Secure Intranet
SIS	Svenska institutet för standarder
SKR	Sveriges Kommuner och Regioner
SOU	Sveriges Offentliga Utredningar
Sunet	Swedish University Computer Network

Sammanfattning

Uppdraget i korthet

Att föreslå utformning av en statlig e-legitimation

Rådets kompromissförslag till Europaparlamentets och rådets förordning om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av en ram för europeisk digital identitet (den reviderade eIDAS-förordningen), COM(2021) 281, innebär bl.a. att det ska bli obligatoriskt för varje medlemsstat att anmäla en e-legitimation på den högsta tillitsnivån enligt ett förfarande för gränsöverskridande identifiering.[1] Tillitsnivån på e-legitimationen avgör hur tillförlitligt det är att personen som identifierar sig är den man utger sig för att vara.

Med anledning av bl.a. förslagen i den reviderade eIDAS-förordningen har utredningen getts i uppdrag att, för det första, lämna förslag på hur en kostnadseffektiv statlig e-legitimation på högsta tillitsnivå kan utformas och tillhandahållas av Myndigheten för digital förvaltning och att, för det andra, analysera och föreslå förändringar som följer av den reviderade eIDAS-förordningen. Syftet är att stärka samhällets säkerhet och robusthet, motverka bedrägerier som begås med hjälp av e-legitimationer och underlätta för så många som möjligt att kunna få tillgång till en e-legitimation.

I detta delbetänkande redovisas utredningens förslag avseende det första deluppdraget.

[1] Ständiga representanternas kommitté (Coreper I), 25 november 2022, Förslag till Europaparlamentets och rådets förordning om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av en ram för europeisk digital identitet – Allmän riktlinje, s. 55. eIDAS-förordningen är den vanligen förekommande benämningen av Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.

Problem- och behovsbild

Tillgänglighet, säkerhet och redundans

En statlig e-legitimation som komplement till de kommersiella som redan finns i Sverige, har efterfrågats även av andra anledningar än de förväntade kraven i den reviderade eIDAS-förordningen. I våra direktiv anges att ett statligt alternativ till befintliga e-legitimationer bör utredas ur fler perspektiv, särskilt i fråga om tillgänglighet, säkerhet och redundans.

I synnerhet bland äldre personer, personer med funktionsnedsättningar och personer utan svenskt personnummer råder ett mer eller mindre stort digitalt utanförskap. Även svenskar i utlandet kan i vissa fall ha svårt att få tillgång till en svensk e-legitimation. Staten har ett ansvar att säkerställa att e-legitimationer blir tillgängliga för så många som möjligt. I likhet med vad som framförts i tidigare utredningar om en statlig e-legitimation anser vi att en grundidentifiering (se nedan) som uppfyller kraven för den högsta tillitsnivån och utförs av staten, medför att också andra e-legitimationer, som baseras på den statliga, kan bli säkrare. I förening med andra säkerhetshöjande åtgärder vid e-legitimationens användande kan riskerna för identitetsrelaterad brottslighet då minskas.

Id-växling, dvs. att kunna skaffa en alternativ e-legitimation för vissa specifika ändamål, kan komma att underlättas genom en statlig e-legitimation på högsta tillitsnivån. En statlig e-legitimation skulle således inte bara stärka den civila beredskapen genom att utgöra ett komplement till befintliga e-legitimationer; den kan också underlätta för andra aktörer att erbjuda e-legitimationer och betrodda tjänster, vilket i sin tur också kan stärka beredskapen och även bidra till ökad konkurrens på e-legitimationsmarknaden. I kapitel 6 redovisas problem- och behovsbilden närmare.

En statlig e-legitimation för så många som möjligt

Myndigheten för digital förvaltning ska utfärda den statliga e-legitimationen

I enlighet med vårt uppdrag föreslår vi att en statlig e-legitimation på tillitsnivå hög enligt eIDAS-förordningen ska utfärdas av Myndigheten för digital förvaltning (avsnitt 7.6).

Enligt våra förslag ska den statliga e-legitimationen tillhandahållas efter ansökan till den som, vid personlig inställelse hos en identitetskontrollerande myndighet, har styrkt sin identitet och har svenskt personnummer, alternativt ett samordningsnummer för personer med styrkt identitet vilket inte är vilandeförklarat. Vi föreslår också en minimiålder. Den statliga e-legitimationen får utfärdas från och med det kalenderår sökanden fyller nio år. För barn under arton år krävs att barnets vårdnadshavare har lämnat skriftligt medgivande (avsnitt 7.4).

Den statliga e-legitimationen ska ha en giltighetstid om högst fem år (avsnitt 7.7).

Delat myndighetsansvar

Polismyndigheten och Skatteverket bedöms var och en vara lämpliga som identitetskontrollerande myndighet

Vårt uppdrag omfattar att bl.a. föreslå vilken eller vilka myndigheter som ska ansvara för grundidentifieringen i samband med utfärdandet av den statliga e-legitimationen, och vilka kontroller av sökandens identitet som ska genomföras vid en sådan grundidentifiering.

Med grundidentifiering avses i detta betänkande ett förfarande som leder fram till att en identitetshandling utfärdas, innefattande en process i vilken det ingår personlig inställelse för sökanden vid såväl ansökan om som utlämnandet av identitetshandlingen, att sökanden styrker sin identitet på ett tillförlitligt sätt, och att vissa fysiska kännetecken av sökanden dokumenteras. Vårt förslag om ansöknings- och utgivningsprocess för den statliga e-legitimationen innefattar samtliga dessa moment (avsnitt 7.5).

Vår tolkning av uppdraget är att grundidentifieringen ska utföras av en annan myndighet än Myndigheten för digital förvaltning. Vi gör bedömningen att det är antingen Polismyndigheten eller Skatteverket

som kan komma i fråga för att genomföra grundidentifieringen på ett tillräckligt säkert, effektivt och tillgängligt sätt, och att regeringen ska bemyndigas att bestämma vilken myndighet som ska ansvara för uppgiften (avsnitt 7.6).

Vi förordar Polismyndigheten framför Skatteverket. Polismyndigheten har redan i dag en utbredd närvaro i samhället och har till antalet närmare dubbelt så många utgivningsställen för identitetshandlingar som Skatteverket. Vidare har Polismyndigheten en i omfattning och tid större erfarenhet beträffande identitetskontroller. Att polisen utses som identitetskontrollerande myndighet för den statliga e-legitimationen bedömer vi sammantaget vara den mest kostnadseffektiva lösningen. Därtill menar vi att Polismyndigheten vid identitetskontrollerna – i sin egenskap av brottsbekämpande myndighet – bättre kan motverka utmaningar kopplade till den identitetsrelaterade brottsligheten.

Utlandsmyndigheterna och Utrikesdepartementet bedöms ha erforderliga förutsättningar att hantera grundidentifiering i samband med ansökningar om statlig e-legitimation utanför riket (avsnitt 7.6).

Utformningen av den statliga e-legitimationen

Den statliga e-legitimationen ska tillhandahållas på ett kontaktlöst aktivt kort som även är eller kan certifieras som en anordning för att skapa kvalificerade elektroniska underskrifter

Den statliga e-legitimationen ska tillhandahållas på en bärare som utformats på ett sätt som uppfyller kraven för nivå hög enligt eIDAS-regelverket. Bäraren av e-legitimationen ska vara ett kontaktlöst aktivt kort som ska skyddas mot obehörig användning, läsning och kopiering av uppgifter som e-legitimationen innehåller (avsnitt 7.2).

E-legitimationen bör dock, enligt vår bedömning, finnas även på ett statligt utfärdat identitetskort så snart som möjligt (avsnitt 7.6). Skatteverkets identitetskort för folkbokförda i Sverige får utfärdas enbart till personer som har fyllt 13 år och är folkbokförda i landet enligt folkbokföringslagen (1991:481). Det nationella identitetskortet får utfärdas av Polismyndigheten till endast svenska medborgare. Dessa statliga identitetshandlingar kan därmed för närvarande inte utgöra bärare för den statliga e-legitimationen, om den ska kunna tillhandahållas till hela den föreslagna personkretsen (avsnitt 7.2).

I våra direktiv konstateras dels att det är tidskrävande att ta fram ett kombinerat identitetskort och e-legitimation, dels att förslagen i den reviderade eIDAS-förordningen, i kombination med ett förändrat säkerhetsläge, kan medföra vissa krav på skyndsamhet att ta fram en statlig e-legitimation på högsta tillitsnivån. Vårt förslag kan mot den bakgrunden ses som en alternativ lösning för att möta skyndsamhetskraven. En e-legitimation på ett separat kort tillgodoser samtidigt behovet av att personer som saknar svenskt personnummer men har tillräcklig anknytning till Sverige för att tilldelas ett samordningsnummer, kan få en svensk e-legitimation, oberoende av om personkretsen för exempelvis Skatteverkets identitetskort även fortsättningsvis omfattar enbart folkbokförda personer.

Den statliga e-legitimationen ska innehålla de attribut som behövs i e-legitimationer som ges ut till privatpersoner, dvs. innehavarens namn och personnummer, alternativt samordningsnummer för personer med styrkt identitet. Därutöver ska den statliga e-legitimationen i ett lagringsmedium på bäraren innehålla innehavarens ansiktsbild och fingeravtryck (avsnitt 7.2).

Vi bedömer att den statliga e-legitimationen bör kunna användas för att framställa kvalificerade elektroniska underskrifter. Bäraren för e-legitimationen ska därför antingen vara eller kunna certifieras som en anordning för att framställa kvalificerade elektroniska underskrifter (avsnitt 7.3).

Finansiering

Ansökningsavgift och förstärkta anslag till berörda myndigheter

En ansökan om statlig e-legitimation ska förenas med en ansökningsavgift. Den kan finansiera delar av det arbete som fordras för att utföra grundidentifieringen. Uppbyggnaden av detta arbete, liksom det som krävs för verksamheten att utfärda den statliga e-legitimationen, förutsätter dock anslagsfinansiering. Det är vidare en förutsättning för att skapa långsiktighet i dessa verksamheter (avsnitt 7.9).

Krav på offentlig sektor att godta vissa e-legitimationer för identifiering i digitala tjänster

Godkända e-legitimationer måste kunna användas

Vi föreslår att det ska ställas lagkrav på offentliga aktörer att för sina digitala tjänster tillåta identifiering med de e-legitimationer som utfärdas av leverantörer som är godkända enligt ett auktorisationssystem för elektronisk identifiering och för digital post.[2] Utöver statliga myndigheter, kommuner och regioner omfattas sådana företag som yrkesmässigt bedriver verksamhet, vilken till någon del är offentligt finansierad, inom förskola, skola, hälso- och sjukvård samt omsorg. Enligt vår bedömning krävs denna reglering bl.a. för att uppnå de i våra direktiv uppställda målen om ökad tillgänglighet och ökad redundans genom en mer diversifierad marknad för e-legitimationer.

Den föreslagna skyldigheten gäller endast om tillitsnivån för e-legitimationen motsvarar en tillitsnivå som är lika hög eller högre än den tillitsnivå som den offentliga aktören kräver för åtkomst till den digitala tjänsten.

Statliga myndigheter, kommuner och regioner som har behov av tjänster för elektronisk identifiering ska använda de tjänster som tillhandahålls genom auktorisationssystem. Närmare bestämmelser om vilken typ av tjänster som kravet avser, och om hur skyldigheten ska fullgöras, meddelas genom myndighetsföreskrifter (avsnitt 7.13).

Författningsreglering

En ny lag och förordning om elektronisk identifiering

Den lagreglering som är nödvändig med anledning av förslaget om en statlig e-legitimation samlas i en ny lag. I den lagen regleras också det föreslagna kravet om att godta vissa e-legitimationer. För övriga bestämmelser, bl.a. sådana som behövs för verkställigheten av lagen, föreslås en förordning (avsnitt 7.1).

I lagen tas in centrala bestämmelser om den uppgifts- och ansvarsfördelning som aktualiseras mellan berörda myndigheter i den gemensamma utgivningsprocessen, bl.a. personuppgiftsansvar och behand-

[2] Prop. 2023/24:6. I propositionen föreslås att valfrihetssystem enligt lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering ska ersättas av auktorisationssystem för sådana tjänster.

ling av personuppgifter (avsnitt 7.11). Vidare införs bestämmelser om kraven för att tillhandahållas en statlig e-legitimation (avsnitt 7.4), om återkallelse och spärr av utfärdad e-legitimation (avsnitt 7.7), om överklagande och verkställbarhet av beslut, och om användning av vissa e-legitimationer (avsnitten 7.8 och 7.13).

Våra förslag medför behov av följdändringar i bl.a. offentlighets- och sekretessförordningen (2009:641) samt i regeringens förslag till lag om auktorisationssystem i fråga om tjänster för elektronisk identifiering och digital post.

Ny och ändrad reglering föreslås träda i kraft den 1 mars 2026.

Sammanfattning, lättläst svenska

EU vill göra ett digitalt id-kort

Sverige är med i något som heter EU.
I EU jobbar svenska politiker tillsammans med andra europeiska länders politiker.
Där bestämmer de olika regler och lagar för oss i Europa.

De som bestämmer i EU vill göra ett särskilt digitalt id-kort.
Så att det blir enklare att veta vem som är vem i alla länder i EU.

Digitala id-kort kallas också för e-legitimation.

Utredning om e-legitimation i Sverige

Sverige vill också göra en ny e-legitimation.
De som bestämmer i Sverige vill ta reda på saker om Sveriges e-legitimation.
Det gör man i något som kallas för en utredning.
I en utredning får man svar på saker man har frågor om med hjälp av experter.

I utredningen vill man få svar på om den nya e-legitimationen skulle vara säkrare än de som redan finns.
Till exempel om man kan förhindra bedrägerier eller att någons e-legitimation används utan lov.

Man vill också få reda på om den nya e-legitimationen skulle bli mer tillgänglig för fler.
Äldre personer kan ha lite svårare att använda teknik som till exempel en mobiltelefon.
I utredningen vill man veta om den nya e-legitimationen skulle vara enklare att använda för äldre och personer med funktionsnedsättning.

Har man inget personnummer är det svårt att få en e-legitimation i dag.
De som bor i Sverige men inte är medborgare har ibland inget personnummer.
I utredningen vill man veta om de utan personnummer skulle få det enklare med den nya e-legitimationen.

Nu är utredningen klar.
Det finns förslag om den nya e-legitimationen.
Förslagen är till de som bestämmer i Sverige.

E-legitimation för så många som möjligt

Det finns redan företag som gör e-legitimationer i dag.
Den nya e-legitimationen skulle göras av svenska staten.
Myndigheten som ska göra e-legitimationen heter Myndigheten för digital förvaltning.
Den myndigheten kallas för Digg.

Om Sverige gör en egen e-legitimation vill man att den ska vara tillgänglig för fler.
Till exempel för äldre, människor med funktionsnedsättning och de som saknar personnummer.

Är man inte svensk medborgare kan man få ett samordningsnummer.
Det är som ett personnummer, till exempel för de som bor i Sverige under en kortare tid.
Ett annat exempel är de som bor i ett grannland men jobbar i Sverige.

Samordningsnummer med styrkt identitet kallas det säkraste samordningsnumret.
Det kan man få om man bevisat vem man är.

Den nya e-legitimationen skulle kunna skaffas av de som har ett personnummer eller det säkraste samordningsnumret.
Man skulle få e-legitimationen från det året man fyller 9 år.

Barn under 18 år måste söka e-legitimation med hjälp av sina föräldrar.
E-legitimationen kommer att fungera i 5 år.
Sen behöver man göra en ny.
Polisen eller Skatteverket kollar att personnummer eller samordningsnummer är rätt.

E-legitimationen skulle skapas för att vara så säker som möjligt.
E-legitimationen finns på ett plastkort.
Kortet skulle göra att e-legitimationen inte blir kopierad eller används av andra.
Längre fram vill man sätta e-legitimationen på ett vanligt id-kort.
Men just nu går det inte.
Det skulle ta för lång tid att göra det nu.

E-legitimationen skulle innehålla samma saker som ett id-kort eller pass.
Där kommer personnummer eller samordningsnummer att finnas.
I e-legitimationen kommer det även att finnas en bild på personen.
Det kommer också att finnas fingeravtryck från personen.

E-legitimationen kommer att kosta pengar

För att göra de nya e-legitimationerna behövs det pengar.
En del av pengarna skulle komma från de som skaffar e-legitimationen.
De som vill ha en e-legitimation betalar en liten summa pengar när de ansöker.
Det kallas för ansökningsavgift.
Resten av pengarna skulle komma från svenska staten.

Nya regler för e-legitimation

Om Sverige gör en ny e-legitimation behöver de politiker som bestämmer göra nya regler.
Det kallas för ny lag.

I lagen skulle det stå vilka som ska vara ansvariga för att e-legitimationen fungerar som den ska.
Man kan också läsa om vilka som får och inte får e-legitimationen.
Om man bryter mot reglerna kan man bli av med e-legitimationen.
Den nya lagen skulle börja gälla den 1 mars 2026.

Om man är svensk men inte bor i Sverige

Det ska bli enklare för svenskar som inte bor kvar i Sverige att få e-legitimation.
När man behöver något från svenska staten men är utomlands går man till en särskild plats.
Det kallas för konsulat eller ambassad.
De som inte bor i Sverige men som ändå tillhör landet skulle också kunna få den nya svenska e-legitimationen.

Om man inte har svenskt personnummer

De som bor i Sverige men inte har ett personnummer har svårt att få en e-legitimation i dag.
Den statliga e-legitimationen skulle man kunna få med ett samordningsnummer med styrkt identitet.

E-legitimationer ska kunna användas på fler ställen

Man kan använda e-legitimation för att skriva sin namnteckning digitalt.
En namnteckning är som ett bevis på att man går med på något.
Till exempel att man vill köpa en sak eller tjänst.
Den nya svenska e-legitimationen ska kunna användas för att bevisa vem man är för offentlig verksamhet.

Offentlig verksamhet är till exempel förskola, sjukhus och omsorg.
E-legitimationen skulle kunna användas när man sätter sitt barn i kö på en förskola.
Eller när man behöver gå till doktorn.

Den statliga e-legitimationen skulle fungera på alla myndigheter, kommuner och regioner.
Den skulle även fungera hos privata företag som jobbar med offentlig verksamhet.
De e-legitimationer som redan finns i dag skulle också fungera på alla myndigheter, kommuner, regioner och företag som jobbar med offentlig verksamhet.

1 Författningsförslag

1.1 Förslag till lag om elektronisk identifiering

Härigenom föreskrivs följande.

Lagens innehåll och förhållande till annan reglering

1 § Denna lag innehåller bestämmelser om medel för elektronisk identifiering som utfärdas av staten samt krav på erkännande av vissa medel för elektronisk identifiering.

Bestämmelser om medel för elektronisk identifiering finns också i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, här benämnd EU:s förordning om elektronisk identifiering, samt i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

Ord och uttryck i lagen

2 § Med elektronisk identifiering, medel för elektronisk identifiering, nättjänst och autentisering avses i denna lag detsamma som i EU:s förordning om elektronisk identifiering.

3 § Med en offentlig aktör avses i denna lag

1. en statlig eller kommunal myndighet, eller en beslutande församling i en kommun eller region,

2. en sammanslutning som inrättats särskilt för att tillgodose behov i det allmännas intresse, under förutsättning att behovet inte är av indu-

striell eller kommersiell karaktär, och som består av en eller flera myndigheter eller församlingar som anges i 1,

3. en privat aktör som yrkesmässigt bedriver verksamhet som till någon del är offentligt finansierad och som

a) aktören bedriver i egenskap av enskild huvudman inom skolväsendet eller huvudman för en sådan internationell skola som avses i 24 kap. skollagen (2010:800),

b) utgör hälso- och sjukvård enligt hälso- och sjukvårdslagen (2017:30) eller tandvård enligt tandvårdslagen (1985:125),

c) bedrivs enligt socialtjänstlagen (2001:453), lagen (1988:870) om vård av missbrukare i vissa fall, lagen (1990:52) med särskilda bestämmelser om vård av unga eller lagen (1993:387) om stöd och service till vissa funktionshindrade, eller

d) utgör personlig assistans som utförs med assistansersättning enligt 51 kap. socialförsäkringsbalken, eller

4. en enskild utbildningsanordnare med tillstånd att utfärda examina enligt lagen (1993:792) om tillstånd att utfärda vissa examina, och som till största delen har statsbidrag som finansiering av högskoleutbildning på grundnivå eller avancerad nivå eller av utbildning på forskarnivå.

Ansökan om och utfärdande av statligt medel för elektronisk identifiering

4 § Statligt medel för elektronisk identifiering får, efter ansökan, utfärdas av den myndighet som regeringen bestämmer (utfärdande myndighet).

5 § Statligt medel för elektronisk identifiering får utfärdas till en person som innevarande kalenderår är eller ska fylla nio år och som har antingen ett svenskt personnummer enligt folkbokföringslagen (1991:481) eller ett sådant samordningsnummer som tilldelats personer som styrkt sin identitet enligt lagen (2022:1697) om samordningsnummer, som inte är förklarat vilande.

För den som är under arton år krävs vårdnadshavares skriftliga medgivande.

6 § Den sökande är skyldig att styrka sin identitet och övriga personuppgifter.

7 § Kontroll av att sökandens identitet är styrkt ska göras av den eller de myndigheter som regeringen bestämmer (identitetskontrollerande myndighet).

8 § I samband med ansökan är sökanden skyldig att låta den identitetskontrollerande myndigheten ta ett fingeravtryck och en ansiktsbild i digitalt format.

9 § Fingeravtrycken och ansiktsbilden enligt 8 § ska sparas i ett lagringsmedium i bäraren av det statliga medlet för elektronisk identifiering.

Fingeravtrycken och de biometriska data som tas fram ur dessa ska omedelbart förstöras när det statliga medlet för elektronisk identifiering har lämnats ut eller en ansökan om sådant medel har återkallats eller avslagits.

10 § En ansökan ska avslås om förutsättningarna i 5 och 6 §§ inte är uppfyllda. Detsamma gäller om det som anges i 8 § eller som föreskrivits i enlighet med 11 § andra stycket 1 inte har iakttagits, och sökanden inte har följt en uppmaning att avhjälpa bristen.

11 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om undantag från skyldigheten att lämna fingeravtryck när det gäller minderåriga och personer som av fysiska skäl är permanent förhindrade att lämna fingeravtryck.

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om

1. ansökan om samt utfärdande och utlämnande av ett statligt medel för elektronisk identifiering, och
2. utformningen av det statliga medlet för elektronisk identifiering.

Återkallelse och spärr av statligt medel för elektronisk identifiering

12 § Ett statligt medel för elektronisk identifiering ska återkallas och spärras om

1. det fanns hinder mot att utfärda ett sådant medel vid tiden för utfärdandet och hindret fortfarande består,

2. någon väsentlig uppgift som ett sådant medel innehåller är felaktig eller inte längre gäller,

3. det är nödvändigt av säkerhetsskäl för att någon annan än den som ett sådant medel är utställt till kan misstänkas obehörigt förfoga över det, eller om innehavaren av medlet på annat sätt förlorat kontrollen över det,

4. ett sådant medel inte har aktiverats inom sex månader efter att ansökan gjordes, eller

5. innehavaren av ett sådant medel har avlidit.

På begäran av innehavaren får ett statligt medel för elektronisk identifiering återkallas och spärras.

13 § Om ett statligt medel för elektronisk identifiering tidigare har utfärdats till sökanden ska det spärras senast i samband med att ett nytt sådant medel utfärdas.

14 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om förfarandet vid spärr av statligt medel för elektronisk identifiering.

Behandling av personuppgifter

15 § Bestämmelserna i 16, 17, 19–23 och 25 §§ samt föreskrifter som meddelats enligt 18 och 24 §§ i denna lag kompletterar Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), här benämnd EU:s dataskyddsförordning.

Vid behandling av personuppgifter enligt denna lag gäller lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning och föreskrifter som har meddelats i anslutning till den lagen, om inte annat följer av 16–25 §§ eller föreskrifter som meddelats i anslutning till dessa paragrafer.

Databas över statligt medel för elektronisk identifiering

16 § Den utfärdande myndigheten ska med hjälp av automatiserad behandling föra en databas med en samling uppgifter om statliga medel för elektronisk identifiering som myndigheten har utfärdat.

17 § En kopia av den ansiktsbild som enligt 9 § ska finnas i ett lagringsmedium i bäraren av det statliga medlet för elektronisk identifiering, och de biometriska uppgifter som tas fram ur ansiktsbilden får behandlas i databasen.

18 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om

1. vilka uppgifter databasen ska eller får innehålla, och
2. den längsta tid som personuppgifter får behandlas i databasen.

Personuppgiftsansvar

19 § Den utfärdande myndigheten är personuppgiftsansvarig för den behandling av personuppgifter som sker i samband med ansökan om och utfärdandet av ett statligt medel för elektronisk identifiering.

Den identitetskontrollerande myndigheten är personuppgiftsansvarig för den behandling av personuppgifter som sker i samband med att myndigheten kontrollerar att sökandes identitet är styrkt enligt 7 §.

Ändamål

20 § Personuppgifter får behandlas av den utfärdande myndigheten om det är nödvändigt för att

1. handlägga ärenden om statligt medel för elektronisk identifiering
2. administrera en databas över innehavare av statliga medel för elektronisk identifiering, och
3. möjliggöra en säker användning av statliga medel för elektronisk identifiering.

Personuppgifter får behandlas av den identitetskontrollerande myndigheten om det är nödvändigt för att, i samband med ansökan, kunna kontrollera den sökandes identitet.

Personuppgifter som har samlats in enligt första stycket får också behandlas av den utfärdande myndigheten

1. om det är nödvändigt för att tillhandahålla information som behövs i Polismyndighetens verksamhet för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa uppbörd eller upprätthålla allmän ordning och säkerhet,

2. om det är nödvändigt för att fullgöra uppgiftsutlämnande som sker i överensstämmelse med lag eller förordning, och

3. för andra ändamål, under förutsättning att uppgifterna inte behandlas på ett sätt som är oförenligt med det ändamål för vilket uppgifterna samlades in.

Behandling av känsliga personuppgifter

21 § Personuppgifter som avses i artikel 9.1 i EU:s dataskyddsförordning (känsliga personuppgifter) får behandlas endast om det är absolut nödvändigt för ändamålet med behandlingen.

Känsliga personuppgifter får dock behandlas

1. i databasen när det är tillåtet enligt 17 § och föreskrifter som meddelats enligt 18 §, och

2. vid sökning som är tillåten enligt 22 §.

Integritetshöjande och säkerhetshöjande åtgärder

22 § Det är förbjudet att använda ansiktsbilder samt biometriska uppgifter som har tagits fram ur sådana bilder som sökbegrepp. Trots förbudet får den ansiktsbild som tas enligt 8 §, och de biometriska uppgifter som tas fram ur ansiktsbilden, användas vid sökning i databasen i samband med ansökan om medel för elektronisk identifiering. Sökning är då tillåten endast för att kontrollera sökandens identitet och innehav av sådant medel.

Sådana övriga känsliga personuppgifter som avses i 21 § och uppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden får inte användas som sökbegrepp.

23 § Tillgången till personuppgifter ska begränsas till det som var och en behöver för att kunna fullgöra sina arbetsuppgifter.

24 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela

1. närmare föreskrifter om tillgången till personuppgifter, och
2. ytterligare föreskrifter om säkerhetsåtgärder till skydd för personuppgifter.

Rätten att göra invändningar

25 § Artikel 21.1 i EU:s dataskyddsförordning om rätten att göra invändningar gäller inte vid sådan behandling som är tillåten enligt denna lag eller föreskrifter som har meddelats i anslutning till lagen.

Krav på erkännande av vissa medel för elektronisk identifiering

26 § När medel för elektronisk identifiering krävs för att få tillgång till en nättjänst som tillhandahålls av en offentlig aktör, och tjänsten helt eller delvis riktar sig till privatpersoner, ska medel erkännas för autentisering för tjänsten om

1. medlet för elektronisk identifiering tillhandahålls av leverantör som är godkänd i enlighet med lagen (20XX:XXX) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post, och
2. tillitsnivån för medlet för elektronisk identifiering motsvarar en tillitsnivå som är lika hög eller högre än den tillitsnivå som den offentliga aktören kräver för åtkomst till nättjänsten.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om

1. vilka typer av tjänster för elektronisk identifiering som kravet i första stycket avser,
2. hur skyldigheten ska fullgöras, och
3. undantag från kravet.

Användning av statligt medel för elektronisk identifiering

27 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om villkor för när och hur ett statligt medel för elektronisk identifiering får användas.

Övriga bestämmelser

28 § Beslut enligt denna lag får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

29 § Beslut enligt denna lag gäller omedelbart, om inte något annat anges i beslutet.

Denna lag träder i kraft den 1 mars 2026.

1.2 Förslag till lag om ändring i förslag till lag om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post

Härigenom föreskrivs att 2 § lagen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post

dels ska ha följande lydelse,

dels att det i lagen ska införas en ny paragraf, 23 §, av följande lydelse.

Lydelse enligt proposition 2023/24:6	*Föreslagen lydelse*
	2 §
Med ett *auktorisationssystem* avses i denna lag ett system där	
1. den myndighet som tillhandahåller systemet godkänner att leverantörer av tjänster för elektronisk identifiering av enskilda eller för digital post får ingå ett avtal inom systemet och ingår avtal med var och en av de godkända leverantörerna om utförande av sådana tjänster,	
2. en enskild har rätt att välja den leverantör som ska utföra tjänsterna för den enskildes räkning, *och*	2. en enskild har rätt att välja den leverantör som ska utföra tjänsterna för den enskildes räkning,
3. en offentlig aktör *kan* använda tjänsterna i sin verksamhet enligt avtal med den tillhandahållande myndigheten.	3. en *sådan* offentlig aktör *som avses i 4 § första stycket 1–3 a ska* använda tjänsterna *för elektronisk identifiering och kan använda tjänsterna för digital post* i sin verksamhet enligt avtal med den tillhandahållande myndigheten, *och*
	4. en sådan offentlig aktör som avses i 4 § första stycket 3 b–5 och andra stycket kan använda tjänsterna i sin verksamhet enligt avtal med den tillhandahållande myndigheten.

23 §

Regeringen eller den myndighet som regeringen bestämmer får besluta om undantag från skyldigheten i 2 § 3.

Denna lag träder i kraft den 1 mars 2026.

1.3 Förslag till förordning om elektronisk identifiering

Härigenom föreskrivs följande.

Förordningens innehåll

1 § Denna förordning innehåller bestämmelser som kompletterar lagen (20XX:XXX) om elektronisk identifiering.

Ord och uttryck som används i denna förordning har samma betydelse som i lagen.

Utfärdande och identitetskontrollerande myndigheter

2 § Myndigheten för digital förvaltning är utfärdande myndighet av statligt medel för elektronisk identifiering.

3 § Myndigheten X är identitetskontrollerande myndighet för ansökningar om statligt medel för elektronisk identifiering som görs inom riket.

Regeringskansliet får besluta i vilken utsträckning beskickningar och karriärkonsulat ska fullgöra uppgifter som identitetskontrollerande myndighet i fråga om ansökningar om statligt medel för elektronisk identifiering som görs utom riket. Regeringskansliet får också besluta att ett honorärkonsulat i begränsad utsträckning ska fullgöra sådana uppgifter.

Ansökan om och utfärdande av statligt medel för elektronisk identifiering

4 § Ansökan om statligt medel för elektronisk identifiering ska göras hos en identitetskontrollerande myndighet.

Den identitetskontrollerande myndigheten ska registrera nödvändiga uppgifter i den databas för statliga medel för elektronisk identifiering som den utfärdande myndigheten har rätt att föra enligt lagen (20XX:XXX) om elektronisk identifiering.

5 § Sökanden är skyldig att inställa sig personligen.

Om sökanden är under arton år ska sökanden ge in ett skriftligt medgivande från hans eller hennes vårdnadshavare, om det inte finns synnerliga skäl att ändå utfärda ett statligt medel för elektronisk identifiering.

I fråga om barn som är under arton år ska en handling som styrker uppgift om vem som är vårdnadshavare uppvisas, om denna uppgift inte framgår av för den identitetskontrollerande myndighetens tillgängliga uppgifter.

6 § För personer som av fysiska skäl är permanent förhindrade att lämna fingeravtryck gäller undantag från skyldigheten i 8 § lagen (20XX:XXX) om elektronisk identifiering att låta den identitetskontrollerande myndigheten ta den sökandes fingeravtryck.

7 § Om en sökande för att styrka sin identitet uppvisar en identitetshandling som är försedd med ett fotografi av innehavarens ansikte eller innehåller ett lagringsmedium där fingeravtryck eller ansiktsbild är sparade, får den identitetskontrollerande myndigheten kontrollera att dessa motsvarar fingeravtryck och ansiktsbild som enligt 8 § lagen (20XX:XXX) ska tas av sökanden vid ansökningstillfället.

När en kontroll enligt första stycket har genomförts, ska fingeravtrycken och de biometriska data som då har tagits fram omedelbart förstöras.

8 § Ett statligt medel för elektronisk identifiering ska finnas på ett kontaktlöst kort och ska utfärdas på tillitsnivå hög enligt artikel 8.2 c i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, här benämnd EU:s förordning om elektronisk identifiering.

Ett kort enligt första stycket ska antingen vara en certifierad anordning för skapande av kvalificerade elektroniska underskrifter som avses i artikel 3.12 i EU:s förordning om elektronisk identifiering, eller kunna certifieras som en sådan anordning.

Ett medel för elektronisk identifiering ska innehålla efternamn, förnamn, namn som visas för användaren, och personnummer enligt folkbokföringslagen (1991:481), alternativt samordningsnummer för

personer med styrkt identitet enligt lagen (2022:1697) om samordningsnummer.

9 § Myndigheten X får, efter att ha hört Regeringskansliet (Utrikesdepartementet), meddela de ytterligare föreskrifter som behövs för verkställigheten av kontrollen att en sökande har styrkt sin identitet enligt 6 § lagen (20XX:XXX) om medel för elektronisk identifiering när det gäller ansökan om sådant medel som görs inom riket.

Regeringskansliet får, efter att ha hört Myndigheten X, meddela motsvarande föreskrifter för sådana identitetskontrollerande myndigheter utom riket som avses enligt denna förordning.

Myndigheten för digital förvaltning får med stöd av 8 kap. 7 § regeringsformen meddela de ytterligare föreskrifter som behövs för verkställigheten av denna förordning.

Utlämnande av statligt medel för elektronisk identifiering

10 § Om ansökan bifalls av den utfärdande myndigheten, ska den identitetskontrollerande myndigheten skyndsamt lämna ut medlet för elektronisk identifiering till sökanden personligen.

Giltighetstid samt återkallelse och spärr

11 § Ett statligt medel för elektronisk identifiering ska utfärdas med en giltighetstid av högst fem år.

12 § För sökande som av fysiska skäl är tillfälligt förhindrade att lämna fingeravtryck ska det statliga medlet för elektronisk identifiering ges giltighet endast så lång tid som det fysiska hindret förväntas bestå. Giltighetstiden får dock inte överstiga sju månader.

13 § Myndigheten för digital förvaltning får meddela ytterligare föreskrifter om begränsning av giltighetstiden i särskilt angivna fall.

Behandling av personuppgifter

14 § Den databas som Myndigheten för digital förvaltning ska föra enligt lagen (20XX:XXX) om elektronisk identifiering ska innehålla

1. sökandens fullständiga namn, personnummer alternativt samordningsnummer, födelsetid, och behövliga kontaktuppgifter,
2. kopia av den ansiktsbild som tagits vid ansökan och biometriska uppgifter som tagits fram ur ansiktsbilderna,
3. dagen för utfärdandet av det statliga medlet för elektronisk identifiering samt dess giltighetstid och status,
4. unik identifierare för det statliga medlet för elektronisk identifiering och dess serienummer,
5. aktiveringskod,
6. kondensat av innehavarens personliga kod,
7. uppgift om hur sökanden har styrkt sin identitet,
8. uppgift om att ansökan har avslagits och skälen för detta beslut, och
9. uppgift om att det statliga medlet för elektronisk identifiering har återkallats och spärrats, samt vad som har utgjort skäl för återkallelsen.

En handling som har kommit in eller upprättats i ett ärende får behandlas i databasen.

15 § Databasen som avses i 14 § får tillföras sådana uppgifter från Skatteverkets folkbokföringsdatabas som anges i 14 § första stycket 1.

16 § Uppgifter och handlingar vilka finns i databasen som avses i 14 § ska gallras senast tio år efter utgången av det kalenderår då det ärende som uppgifterna eller handlingarna hänför sig till avslutades.

Riksarkivet får, efter att ha inhämtat synpunkter från Myndigheten för digital förvaltning, meddela föreskrifter om

1. att uppgifter och handlingar får bevaras för arkivändamål av allmänt intresse eller vetenskapliga, statistiska eller historiska ändamål under längre tid än som anges första stycket, och

2. avskiljande och begränsningar av åtkomsten till uppgifter och handlingar som bevaras för sådana ändamål som anges i 1.

17 § En innehavare av ett statligt medel för elektronisk identifiering har rätt att hos den identitetskontrollerande myndigheten kontrollera den information som har sparats i lagringsmediet på bäraren av det medlet för elektronisk identifiering.

18 § Myndigheten för digital förvaltning får meddela närmare föreskrifter om

1. tillgången till personuppgifter inom myndigheten, och
2. andra säkerhetsåtgärder till skydd för personuppgifter inom myndigheten.

Myndigheten X får meddela närmare föreskrifter om

1. tillgången till personuppgifter inom myndigheten, och
2. andra säkerhetsåtgärder till skydd för personuppgifter inom myndigheten.

Regeringskansliet (Utrikesdepartementet) får meddela närmare föreskrifter om

1. tillgången till personuppgifter inom sådana identitetskontrollerande myndigheter utom riket som avses enligt denna förordning, och
2. andra säkerhetsåtgärder till skydd för personuppgifter inom sådana identitetskontrollerande myndigheter utom riket som avses enligt denna förordning.

Krav på erkännande av vissa medel för elektronisk identifiering

19 § Myndigheten för digital förvaltning får meddela föreskrifter om

1. vilken typ av tjänster som kravet i 26 § första stycket lagen (20XX:XXX) om elektronisk identifiering avser,
2. hur skyldigheten ska fullgöras, och
3. undantag från kravet.

Ansökningsavgift

20 § För prövning av ansökan om statligt medel för elektronisk identifiering ska sökanden betala en ansökningsavgift på 400 kronor. Avgiften ska betalas i samband med ansökan. Om avgiften inte är betald

då tillämpas bestämmelserna i 11 § avgiftsförordningen (1992:191). För prövning av ansökan tillämpas i övrigt bestämmelserna i 12–14 §§ avgiftsförordningen.

Denna förordning träder i kraft den 1 mars 2026.

1.4 Förslag till förordning om ändring i offentlighets- och sekretessförordningen (2009:641)

Härigenom föreskrivs att 6 § offentlighets- och sekretessförordningen (2009:641) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
6 §[1]	
Sekretess gäller i nedan angiven verksamhet, som avser registrering av betydande del av befolkningen, för 1. uppgift om en enskilds personliga förhållanden, om det av särskild anledning kan antas att den enskilde eller någon närstående till honom eller henne lider men om uppgiften röjs, och 2. uppgift i form av fotografisk bild av den enskilde, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider men. För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.	
Verksamheten avser	**Verksamheten avser**
fastighetsregistret	fastighetsregistret
kommunala fastighetsregister	kommunala fastighetsregister
	Myndigheten för digital förvaltnings databas över statliga medel för elektronisk identifiering
passregister och register över nationella identitetskort	passregister och register över nationella identitetskort
röstlängdsregister	röstlängdsregister
Skatteverkets databas över identitetskort för folkbokförda i Sverige	Skatteverkets databas över identitetskort för folkbokförda i Sverige
Socialstyrelsens register över legitimerad hälso- och sjukvårdspersonal och personal med bevis om rätt att använda yrkestiteln undersköterska	Socialstyrelsens register över legitimerad hälso- och sjukvårdspersonal och personal med bevis om rätt att använda yrkestiteln undersköterska
Statens jordbruksverks register över hund- och kattägare	Statens jordbruksverks register över hund- och kattägare

[1] Senaste lydelse 2023:297.

Statens tjänstepensionsverks pensionsregister	Statens tjänstepensionsverks pensionsregister
Totalförsvarets plikt- och prövningsverks register över totalförsvarets personal	Totalförsvarets plikt- och prövningsverks register över totalförsvarets personal
Transportstyrelsens vägtrafikregister	Transportstyrelsens vägtrafikregister

Denna förordning träder i kraft den 1 mars 2026.

1.5 Förslag till förordning om ändring i förordningen (2014:115) med instruktion för utrikesrepresentationen

Härigenom föreskrivs att det i förordningen ska införas en ny paragraf, 3 kap. 10 b §, och närmast före 3 kap. 10 b § en ny rubrik av följande lydelse.

3 kap.

Identitetskontroll i ärende om statligt medel för elektronisk identifiering

10 b §

Beskickningar och konsulat ska utföra identitetskontroll enligt lagen (20XX:XXX) om elektronisk identifiering.

Denna förordning träder i kraft den 1 mars 2026.

2 Utredningens uppdrag och arbete

2.1 Utredningens uppdrag

Regeringen beslutade den 22 december 2022 kommittédirektiv om att ge en särskild utredare i uppdrag att utreda och lämna förslag på hur staten kan utfärda en e-legitimation på högsta tillitsnivå. Utredaren ska också se över behovet av anpassningar som följer av den reviderade eIDAS-förordningen.

Av utredningsdirektiven framgår bl.a. att utredningen ska lämna förslag på hur en kostnadseffektiv e-legitimation på tillitsnivå hög enligt eIDAS-förordningen kan utformas och tillhandahållas av Myndigheten för digital förvaltning (Digg). Utredningen ska vidare lämna förslag på vilken eller vilka myndigheter som ska ansvara för grundidentifieringen vid utfärdandet av en statlig e-legitimation och vilka kontroller av identitet som ska genomföras vid en sådan grundidentifiering, samt analysera om det bör ställas krav på förlitande parter som tillhandahåller digitala tjänster inom offentlig sektor att acceptera alla e-legitimationsalternativ på marknaden förutsatt att de lever upp till den tillitsnivå som tjänsterna kräver. Utredningen ska även lämna nödvändiga författningsförslag.

I delredovisningen den 16 oktober 2023 ska uppdraget att föreslå hur staten kan utfärda en e-legitimation på högsta tillitsnivå ingå.

Uppdraget att analysera och föreslå förändringar som följer av revisionen av eIDAS-förordningen ska slutredovisas den 31 maj 2024.

Utredningens direktiv finns bifogade till delbetänkandet i bilaga 1.

2.2 Utredningens arbete

Utredningsarbetet påbörjades i januari 2023. Under utredningstiden har vi hittills haft tre sammanträden med sakkunnig- och expertgruppen.

Frågan om tillhandahållande av statlig e-legitimation har tidigare utretts av både myndigheter och statliga utredningar. Vi har tagit del av detta skriftliga material och andra relevanta underlag. I synnerhet den rapport som Digg utifrån ett regeringsuppdrag publicerade i januari 2023 om hur en statlig e-legitimation kan utformas. Utredningen ska enligt direktiven beakta förslagen och de synpunkter som framkommit inom ramen för regeringsuppdraget.

För att komplettera det skriftliga underlaget har vi vidare genomfört ett 20-tal möten och samtal med aktörer i offentlig förvaltning, intresseorganisationer och utfärdare av privata e-legitimationer.

I syfte att inhämta synpunkter från en bredare grupp av myndigheter samt berörda privata aktörer och organisationer har vi även genomfört två digitala möten med öppen anmälan. Mötena hölls i mars 2023. Vid mötet för representanter för offentlig förvaltning och intresseorganisationer medverkade cirka 60 deltagare och vid mötet med privata aktörer cirka 40 deltagare.

Vi har enligt våra direktiv haft att beakta relevant arbete som bedrivs inom Regeringskansliet och utredningsväsendet samt särskilt beakta det arbete som bedrivs hos Digg. Vi har under utredningstiden haft flera möten och kontakter med Digg. Vi har även haft kontakt med flera statliga utredningar, däribland Postfinansieringsutredningen (I 2020:03) och Utredningen om interoperabilitet vid datadelning (I 2022:03).

Visst underlag till konsekvensutredningen har tagits fram av Governo AB på vårt uppdrag.

2.3 Utredningens prioriteringar

I relation till den begränsade tid vi haft till förfogande har vi valt att prioritera frågor som enligt vår bedömning är de mest centrala för att skapa förutsättningar för att en statlig e-legitimation på den högsta tillitsnivån kan tillhandahållas inom den tid som kraven i den kommande reviderade eIDAS-förordningen förväntas medföra.

2.4 Delbetänkandets disposition

I kapitel 3 definieras några för delbetänkandet centrala begrepp och termer.

I kapitel 4 redogörs för e-legitimationsområdet i Sverige.

Kapitel 5 innehåller en översiktlig internationell utblick.

I kapitel 6 beskrivs varför en statlig e-legitimation behövs.

Kapitel 7 innehåller utredningens överväganden och förslag.

I kapitel 8 redogör vi för konsekvenserna av våra förslag.

I kapitel 9 behandlas ikraftträdande och i kapitel 10 finns författningskommentarerna.

3 Definitioner av vissa centrala begrepp och termer

3.1 Identitet

Det finns inte någon legaldefinition av begreppet identitet. Vad gäller identitetsbegreppet som sådant kan det i vissa sammanhang ha en subjektiv dimension, exempelvis en persons självbild.[1] Det kan här även noteras att begreppet identitet också används i förhållande till objekt med koppling till t.ex. sakernas internet och robotiserade processer.[2] I detta betänkande avses emellertid med identitet endast viss information rörande en person som är att anse som objektiva fakta.

I ärenden om svenskt medborgarskap har i rättspraxis uttalats att sådana objektiva fakta om identiteten består av sökandens namn, födelsetid och, som huvudregel, medborgarskap.[3] I förarbetena till lagen (2022:1697) om samordningsnummer anges att det är tillräckligt för tilldelning av samordningsnummer att uppgift om personens namn, födelsetid och medborgarskap är styrkta och också kan kopplas till en fysisk person.[4]

3.2 Identitetshandling

En identitetshandling används för att en person ska kunna identifiera sig, eller styrka sin identitet. En identitetshandling innehåller alltså, om de utfärdats på ett säkert sätt, ofta de uppgifter om en person som behövs för att fastställa dennes identitet. I många identitetshandlingar lagras dessutom biometriska uppgifter som kan användas

[1] *Id-kort för folkbokförda i Sverige* (SOU 2007:100), s. 25.
[2] Se t.ex. Inera, *IAM Strategi Med kommunernas behov i fokus*, 5 maj 2020, s. 8.
[3] Migrationsöverdomstolens avgörande MIG 2019:18.
[4] Prop. 2021/22:276 s. 55 f.

för att kontrollera handlingens äkthet och innehavarens identitet.[5] Begreppet identitetshandling får enligt vår bedömning anses vara teknikneutralt och kan avse både en fysisk identitetshandling eller en e-legitimation. I betänkandet används även begreppen id-handling eller id-kort. När samlingsbegreppet statliga identitetshandlingar används avses det nationella identitetskortet, Skatteverkets identitetskort för folkbokförda samt i tillämpliga fall pass.

3.3 Identitetsbeteckningar

I Sverige finns två identitetsbeteckningar för fysiska personer som används i folkbokföringsverksamheten och i samhället i övrigt; personnummer och samordningsnummer.

Personnummer är enligt 18 § folkbokföringslagen (1991:481) avsett att utgöra en identitetsbeteckning för varje folkbokförd person. Även om personen skulle avregistreras från folkbokföringen, exempelvis vid utflyttning, behåller personen sitt personnummer. Personnumret och den historiska informationen som är kopplad till detta finns kvar i folkbokföringsdatabasen.

För att upprätthålla tilltron till personnumret som identifikationsbegrepp är det reserverat för personer som är folkbokförda (se mer om personnummer i avsnitt 7.4.2).

Personer som inte är folkbokförda i Sverige kan under vissa förutsättningar tilldelas ett samordningsnummer av Skatteverket.[6]

På motsvarande sätt som personnummer är samordningsnummer unika såtillvida att två identiska samordningsnummer inte förekommer. Om en person med ett samordningsnummer senare blir folkbokförd ersätts samordningsnumret med ett personnummer. Individens koppling till samordningsnumret finns emellertid kvar i registret. Den huvudsakliga regleringen av samordningsnummer finns i lagen om samordningsnummer som trädde i kraft i september 2023 (se mer om samordningsnummer och den nya lagen i avsnitt 7.4.2).

Personnummer och samordningsnummer utgör inte känsliga personuppgifter i dataskyddsförordningens mening, men behandlingen av dessa uppgifter omfattas genom nationell lagstiftning av särskilda villkor (se mer om detta i avsnitt 7.11.8).

[5] *Om folkbokföring, samordningsnummer och identitetsnummer* (SOU 2021:57), s. 199.
[6] Denna identitetsbeteckning har motiverats av risken för personförväxling och behovet av en säker kommunikation mellan myndigheter, se prop. 1997/98:9 s. 78 ff.

Det kan här noteras att i förordning (EU) 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, härefter kallad eIDAS-förordningen, används begreppet personidentifieringsuppgift i stället för identitetsbeteckning. I artikel 3.3 definieras personidentifieringsuppgifter som en uppsättning uppgifter som gör det möjligt att fastställa identiteten på en fysisk eller juridisk person eller en fysisk person som företräder en juridisk person. Det rör sig således bl.a. om identitetsbeteckningar för att identifiera en fysisk person och det kan exempelvis vara ett personnummer, samordningsnummer eller annan unik identifierare i form av exempelvis en tjänsteidentitet.

3.4 Identifiering och autentisering

Av artikel 3.1 i eIDAS-förordningen framgår att elektronisk identifiering är en process inom vilken personidentifieringsuppgifter i elektronisk form, som unikt avser en fysisk eller juridisk person eller en fysisk person som företräder en juridisk person, används.

I artikel 3.5 i eIDAS-förordningen definieras autentisering som en elektronisk process som gör det möjligt att bekräfta den elektroniska identifieringen för en fysisk eller juridisk person, eller ursprunget för och integriteten hos uppgifter i elektronisk form. Svenska datatermgruppen definierar autentisering som kontroll av uppgiven identitet, t.ex. vid inloggning, vid kommunikation mellan två system eller vid utväxling av meddelande mellan användare.[7] Internetstiftelsen å sin sida definierar autentisering som att helt enkelt kunna visa upp och styrka sin identitet för en annan part.[8]

Det förekommer flera olika metoder av autentisering. I samband med autentisering brukar det talas om en-, två- eller flerfaktorsautentisering. Användning av lösenord eller PIN-kod brukar ses som enfaktorsautentisering som baseras på något en person vet eller kan. Med dessa metoder går det egentligen bara att veta att lösenordet och PIN-koden används, men inte av vem.

Tvåfaktorsautentisering kan vara en kombination av lösenord, dvs. något som personen kan, med något som personen har, exempelvis ett smartkort eller en applikation i en mobiltelefon, alternativt i kom-

[7] www.termado.com/DatatermSearch/?ss=autentisering (hämtad 2023-03-26).
[8] internetstiftelsen.se/guide/digitala-identiteter/ordlista/ (hämtad 2023-03-26).

bination med någon form av inloggning med biometrisk avläsning, t.ex. med fingeravtryck. Även andra autentiseringslösningar kan användas såsom koddosor, USB-stickor, engångslösenord via sms m.m.

Ett annat begrepp som förekommer med koppling till autentisering är stark autentisering. Med stark autentisering avses ofta kontroll av en identitet på två eller flera olika sätt.[9]

3.5 E-legitimation

Begreppen e-legitimation och elektronisk identitetshandling förekommer inte i eIDAS-förordningen. Där används i stället medel för elektronisk identifiering som i artikel 3.2 definieras som en materiell och/eller immateriell enhet som innehåller personidentifieringsuppgifter och som används för autentisering för nättjänster.

Med begreppet e-legitimation avses en identitetshandling som kan användas för att identifiera innehavaren på elektronisk väg. Med hjälp av en e-legitimation kan innehavaren identifiera sig och myndigheter eller andra aktörer som har digitala tjänster få en bekräftelse på vem personen är. En e-legitimation innehåller, liksom en fysisk identitetshandling, uppgifter som entydigt kan kopplas till en viss person.[10]

Alla former av medel för elektronisk identifiering kan således inte anses utgöra en e-legitimation utan det krävs att det rör sig om en handling som har en både tydlig och säker koppling till innehavarens identitet. Detta sker vanligtvis, men inte uteslutande, genom en certifikatbaserad lösning.

En e-legitimation kan finnas som en applikation i en mobiltelefon eller surfplatta eller som en fil på en dator. Den kan också finnas på en fysisk bärare, såsom ett smartkort. Kortet innehåller då ett chip där informationen lagras.[11]

Utredningen om effektiv styrning av nationella digitala tjänster använde begreppet elektronisk identitetshandling i stället för e-legitimation. Anledningen var enligt utredningen att en identitetshandling syftar till att visa en individs identitet och används för att kontrollera att individen är den som han eller hon utger sig för att vara medan be-

[9] Se t.ex. definitionen av stark autentisering i 2 kap. Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40) och 1 kap. 4 § lagen (2010:751) om betaltjänster.
[10] *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14), s. 129.
[11] Ibid.

greppet legitimation säger något om personens behörighet. Utredningen menade att begreppet e-legitimation är missvisande eftersom det antyder att det rör sig om uppgifter som utvisar både identitet och behörighet.[12]

2017 års ID-kortsutredning använde emellertid begreppet e-legitimation med motiveringen att det är ett inarbetat begrepp som bl.a. används i det tillitsramverk som Myndigheten för digital förvaltning ansvarar för och som gäller för det kvalitetsmärke som för närvarande benämns Svensk e-legitimation (se mer om tillitsramverket och kvalitetsmärket i avsnitt 4.3). Utredningen noterade vidare att det även är det begrepp som huvudsakligen används av de nuvarande svenska utfärdarna av e-legitimationer.[13]

Vi delar den bedömning som gjordes av 2017 års ID-kortsutredning och använder oss därför av begreppet e-legitimation i betänkandet.

Vad gäller författningstext är dock medel för elektronisk identifiering det uttryck som används både i eIDAS-förordningen och nationella författningar. I författningsförslagen kommer därför detta begrepp att användas i stället för e-legitimation.

3.6 E-tjänstelegitimation

En e-tjänstelegitimation är en e-legitimation för den som tjänstgör vid eller innehar uppdrag för en organisation och som anskaffats av organisationen. En e-tjänstelegitimation kan utöver identitetsuppgifter även innehålla uppgifter om användarens anställning och/eller behörighet. Den kan både finnas i en applikation eller på en fysisk bärare.[14]

3.7 Grundidentifiering

Uttrycket grundidentifiering, som inte förekommer i några författningar, används ofta för den identitetskontroll som sker i samband med utfärdandet av en id-handling.

[12] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 171 f.
[13] *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14), s. 129 f.
[14] *Användning av e-legitimation i tjänsten i den offentliga förvaltningen* (SOU 2021:62), s. 46 f.

Utredningen om effektiv styrning av nationella digitala tjänster analyserade några av de befintliga grundidentifieringsprocesserna.[15] Av genomgången framgick att processerna skilde sig åt och att olika krav ställs inför utfärdande av olika identitetshandlingar. Detta gällde såväl för de fysiska identitetshandlingar som staten respektive privata aktörer utfärdade som för e-legitimationer.[16] I nästan alla processer gällde att individen ska styrka sin identitet. Då handlade det om att sammanföra registrerade uppgifter om en viss individ med en viss fysisk person. Med registrerade uppgifter avsågs framför allt sådana uppgifter som framgår av folkbokföringsregistret. Sättet som individen kunde styrka sin identitet på skilde sig åt. Hade individen redan en viss sorts identitetshandling var den ofta tillräcklig för att styrka identiteten. Om individen saknade en identitetshandling av visst bestämt slag krävdes att andra personer med vissa närmare angivna kopplingar till individen intygade dennes identitet.[17]

Det som skilde de olika identitetshandlingarna åt var primärt ansöknings- och utlämnandeprocessen. Där ställdes i många fall krav på att individen ska inställa sig personligen hos den utfärdande aktören vid såväl ansökan som utlämnande. I vissa fall fanns det dock inga sådana krav, exempelvis var det möjligt att hämta ut ett körkort via ett postombud.[18] Ytterligare en skillnad var hur uppgifter om individen dokumenteras, dvs. i vissa fall ansvarade utfärdaren för att fotografera eller ta fingeravtryck av individen, i andra fall kunde individen ta med sig eller skicka in ett fotografi som hade tagits av annan men som ofta skulle uppfylla vissa kriterier. Utredningen bedömde att det inte är alla processer som leder fram till identitetshandlingar som grundar sig på utförd grundidentifiering. För att en process ska innehålla grundidentifiering bedömde utredningen att vissa styrande principer skulle vara uppfyllda. Dessa principer var att

[15] 6 § passlagen (1978:302), 3 § andra stycket förordningen (2005:661) om nationellt identitetskort, 2 § lagen (2015:899) om identitetskort för folkbokförda i Sverige, 3 kap. 15 § körkortsförordningen (1998:980) samt processen vid utfärdande av BankID.
[16] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 173 ff.
[17] Skatteverkets föreskrifter om identitetskort, SKVFS 2009:14 och Rikspolisstyrelsens föreskrifter och allmänna råd om polismyndigheternas hantering av pass och nationellt identitetskort, RPSFS 2009:14, FAP 530-1.
[18] 8 kap. 3 § körkortsförordningen (1998:980) samt Transportstyrelsens föreskrifter om utlämnande av körkort, TSFS 2014:17.

- ansökan om en identitetshandling måste göras vid ett personligt besök hos den utfärdande aktören,
- individen ska styrka sin identitet på ett tillförlitligt sätt,
- den utfärdande aktören ansvarar för att dokumentera fysiska kännetecken genom att åtminstone ta ett fotografi av individen, och
- identitetshandlingen ska lämnas ut vid ett personligt besök hos utfärdaren.[19]

Med grundidentifiering avser vi, i likhet med det som redovisas ovan, ett förfarande som leder fram till att en identitetshandling utfärdas, innefattande en process i vilken det ingår personlig inställelse för sökanden vid såväl ansökan om som utlämnandet av identitetshandlingen, att sökanden styrker sin identitet på ett tillförlitligt sätt, och att vissa fysiska kännetecken av sökanden dokumenteras. Vi redogör för vikten av en säker grundidentifiering i våra förslag i kapitel 7.

3.8 Identitetsintygsutfärdare och identitetsintyg

Identitetsintygsutfärdare är den som utfärdar identitetsintyg. Ett identitetsintyg är ett av en identitetsintygsutfärdare utställt intyg i elektronisk form med uppgifter om en användares identitet och eventuella attribut.[20] Identitetsintyget utfärdas till en förlitande part och kan endast användas vid ett tillfälle. Utfärdande av identitetsintyg sker ibland av e-legitimationsutfärdaren, men det förekommer också att identitetsintyget utfärdas av en separat identitetsintygsutfärdare.

3.9 Id-växling

Med id-växling avses i betänkandet när en e-legitimation, som utfärdas efter en grundidentifiering, kan utgöra underlag vid utfärdande av andra e-legitimationer.[21] Id-växling kan emellertid också förekomma i andra sammanhang.

[19] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 175 ff.
[20] *E-legitimationsnämnden och Svensk e-legitimation* (SOU 2010:104), s. 173.
[21] *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14), s. 321.

3.10 Certifikat

I eIDAS-förordningen definieras i artikel 3.14 och 3.29 certifikat som ett intyg som kopplar valideringsuppgifter för en elektronisk underskrift eller en elektronisk stämpel till en fysisk person respektive juridisk person och bekräftar åtminstone namnet eller pseudonymen på den personen. Annorlunda uttryckt kan ett certifikat beskrivas som ett elektroniskt intyg som bl.a. innehåller uppgifter som möjliggör validering av t.ex. en elektronisk underskrift eller elektronisk stämpel. Certifikat är även, vad avser autentisering av webbplatser, ett intyg som gör det möjligt att autentisera en webbplats och koppla webbplatsen till den fysiska eller juridiska person som certifikatet utfärdats för.

3.11 Förlitande part

En förlitande part är enligt artikel 3.6 i eIDAS-förordningen en fysisk eller juridisk person som förlitar sig på en elektronisk identifiering eller betrodda tjänster. Med andra ord är den förlitande parten exempelvis den aktör som tillhandahåller en digital tjänst där åtkomst ges efter att identifiering skett med en e-legitimation.

4 E-legitimationsområdet i Sverige

4.1 Grundläggande tekniska funktioner

Det finns olika sätt att identifiera en användare. Exempelvis genom användning av certifikat (Public Key Infrastructure [PKI]), via användning av engångslösenord eller med symmetrisk kryptering som en koddosa för autentisering till en identitetsintygsutfärdare. Utfärdaren använder sedan autentiseringen för att ställa ut ett identitetsintyg som innehåller en användares elektroniska identitet och attribut där ett attribut skulle kunna vara ett personnummer. Identitetsintyget kan vidare innehålla uppgifter om tillitsnivå avseende det enskilda identitetsintyget.

När en användare använder en e-legitimation hos en förlitande part sker det i ett flöde. I det flödet förekommer flera olika moment som kan utföras av olika aktörer. Flödet består av anvisningstjänst, identitetsintygsutfärdare, legitimeringstjänst, e-legitimationsutfärdare och behörighetskontrolltjänst.

Anvisningstjänst används i samband med inloggning till digitala tjänster när tjänsterna tillåter användning av flera olika e-legitimationer från flera olika e-legitimationsutfärdare. Tjänsten låter en användare välja vilken e-legitimation den vill använda. I legitimeringstjänsten legitimerar sig användaren genom att använda sin e-legitimation, t.ex. ange koden för att använda nyckeln på ett smartkort eller en mobil e-legitimation. Tjänsten kontrollerar e-legitimationen och skickar vidare resultatet till identitetsintygsutfärdaren. Utfärdare av identitetsintyg tar emot och kontrollerar legitimeringen som skett av legitimeringstjänsten mot utfärdaren av e-legitimationer. Därefter utfärdas identitetsintyget som stämplas elektroniskt av identitetsintygsutfärdaren så att förlitande part kan kontrollera intygets äkthet. Den förlitande partens digitala tjänst kan vid behov kontrollera be-

hörighetsinformation som finns i den digitala tjänstens register eller i förekommande fall hämta det från en behörighetskontrolltjänst.

4.2 eIDAS-förordningen

4.2.1 Förordningens innehåll

Inom EU finns bestämmelser om elektronisk identifiering framför allt i eIDAS-förordningen. Förordningen innehåller även bestämmelser om betrodda tjänster.[1]

I detta avsnitt följer en redogörelse över de bestämmelser i förordningen som vi anser är av relevans för frågeställningarna i betänkandet. Det är inte en fullständig redogörelse för förordningens bestämmelser om elektronisk identifiering och betrodda tjänster.

I skrivande stund pågår förhandlingar om ett förslag till revidering av eIDAS-förordningen (se avsnitt 4.2.7).

4.2.2 Bestämmelser om elektronisk identifiering

Förordningens syfte vad gäller elektronisk identifiering är att säkerställa en väl fungerande inre marknad och uppnå en lämplig säkerhetsnivå för medel för elektronisk identifiering. Medel för elektronisk identifiering definieras i artikel 3.2 som en materiell och/eller immateriell enhet som innehåller personidentifieringsuppgifter och som används för autentisering för nättjänster. E-legitimationer är ett medel för elektronisk identifiering och vi använder oss för enkelhetens skull fortsättningsvis av begreppet e-legitimationer i möjligaste mån. Det kan dock inte uteslutas att medel för elektronisk identifiering omfattar även andra lösningar för autentisering än e-legitimationer.

I förordningen används vidare termen system för elektronisk identifiering, som i artikel 3.4 definieras som ett system för elektronisk identifiering genom vilket medel för elektronisk identifiering utfärdas till en fysisk eller juridisk person eller en fysisk person som företräder en juridisk person. I det fortsatta kallar vi dessa system för e-legitimationssystem för att inte göra texten onödigt svårläst.

[1] Betrodda tjänster är enkelt uttryckt elektroniska tjänster som erbjuder vissa utpekade funktioner kopplade till elektroniska underskrifter, elektroniska stämplar, elektroniska tidsstämplingar eller certifikat för autentisering av webbplatser. Dessutom är elektroniska tjänster för rekommenderade leveranser betrodda tjänster i sig.

Förordningen reglerar vad som gäller när e-legitimationer används över landsgränserna inom EU genom att dels ställa krav på e-legitimationerna, dels ställa krav på medlemsstaterna att erkänna e-legitimationer från andra medlemsstater. Förordningen gäller enligt artikel 2.1 e-legitimationssystem som har anmälts av en medlemsstat och enligt skäl 12 i förordningens ingress syftar förordningen till att undanröja hinder för gränsöverskridande användning av e-legitimationer som används i medlemsstaterna för autentisering för åtminstone offentliga tjänster. Däremot är syftet med förordningen enligt samma skältext inte att ingripa i fråga om e-legitimationssystem och tillhörande infrastrukturer som inrättats i medlemsstaterna. Förordningen ska således inte tolkas som att den ställer krav på e-legitimationer som endast används nationellt, kraven på e-legitimationerna aktualiseras först när de ska användas över landsgränserna.

4.2.3 Anmälan av e-legitimationssystem för gränsöverskridande användning

För att e-legitimationer ska kunna användas i andra medlemsstater krävs att medlemsstaten där e-legitimationen har sitt ursprung har anmält det aktuella e-legitimationssystemet. Ett system får anmälas om det uppfyller ett antal krav som föreskrivs i artikel 7 i förordningen. Det är endast medlemsstater som kan anmäla system, men det behöver inte vara medlemsstaten som utfärdar e-legitimationerna i systemet. E-legitimationerna kan vara utfärdade av den anmälande medlemsstaten, på uppdrag av den anmälande medlemsstaten eller oberoende av den anmälande medlemsstaten men erkännas av medlemsstaten.

En anmälan delas in i tre steg. Det första steget är s.k. föranmälan. Under detta steg förser den anmälande medlemsstaten andra medlemsstater med information om det system som anmäls.

Nästa steg är en sakkunnigbedömning. Under detta steg bedöms kvaliteten och säkerheten i det anmälda systemet utifrån kraven i eIDAS-förordningen och aktuell genomförandeförordning. Bedömningen genomförs av andra medlemsstater och avslutas med ett utlåtande som antas av samtliga medlemsstater.

Det sista steget är formell anmälan och publicering i EU:s officiella tidning.

Sverige har tre e-legitimationer som är föranmälda och granskade av andra medlemsstater. En av dessa e-legitimationer, Freja+, är anmäld och kan därmed användas för gränsöverskridande e-legitimering inom EU.

Med anmälan av e-legitimationssystem följer ansvar för medlemsstaten. Om säkerhetsincidenter inträffar, exempelvis intrång, som påverkar tillförlitligheten i systemets gränsöverskridande autentisering ska den anmälande medlemsstaten enligt artikel 10.1 utan dröjsmål tillfälligt upphäva eller återkalla den gränsöverskridande autentiseringen eller de berörda utsatta delarna i systemet samt informera andra medlemsstater och EU-kommissionen. Medlemsstaten åläggs enligt artikel 11.1 även skadeståndsansvar för skada som åsamkats en fysisk eller juridisk person avsiktligt eller på grund av oaktsamhet genom underlåtenhet att uppfylla vissa skyldigheter. Skyldigheterna relaterar bl.a. till att medlemsstaten ska se till att den aktuella fysiska eller juridiska personen tillskrivs de personidentifieringsuppgifter som unikt representerar personen.

Enligt artikel 7 e ska den part som utfärdar e-legitimationer inom ett anmält system se till att legitimationerna tilldelas rätt person i enlighet med de tekniska specifikationer, standarder och förfaranden som gäller för den relevanta tillitsnivån. Om utfärdaren avsiktligt eller på grund av oaktsamhet genom underlåtenhet inte uppfyller denna skyldighet är utfärdaren enligt artikel 11.2 ansvarig för skada som åsamkats en fysisk eller juridisk person vid en gränsöverskridande transaktion.

4.2.4 Förordningens tre tillitsnivåer

Förordningen fastställer tre tillitsnivåer för de e-legitimationer som utfärdats inom ett e-legitimationssystem: låg, väsentlig och hög. Tillitsnivåerna bör enligt skäl 16 i förordningens ingress återge graden av tillit till en e-legitimation vid fastställande av en persons identitet och skapa visshet om att den person som gör anspråk på en viss identitet faktiskt är den person som har tilldelats denna identitet.

Tillitsnivån låg ska ge en begränsad grad av tillförlitlighet avseende en persons påstådda eller styrkta identitet och nivån väsentlig ska ge en väsentlig grad av tillförlitlighet. Tillitsnivån hög ska ge en högre grad av tillförlitlighet än tillitsnivån väsentlig avseende en persons påstådda eller styrkta identitet.

Vår bedömning är att tillitsnivåerna genom förordningen är fullharmoniserade vid gränsöverskridande användning av e-legitimationer. Detta mot bakgrund av förordningens syfte att undanröja hinder för gränsöverskridande användning av e-legitimationer som används i medlemsstaterna för autentisering för åtminstone offentliga tjänster.

Förordningen ger inte uttryck för att medlemsstaterna har möjlighet att ställa andra krav på tillit för tillgång till sina nättjänster vid gränsöverskridande autentisering. Som framgår ovan syftar förordningen inte till att ingripa i fråga om e-legitimationssystem och tillhörande infrastrukturer som inrättats i medlemsstaterna. Det är när e-legitimationer som ingår i systemen ska användas över gränserna som förordningens bestämmelser aktualiseras. Det bör därmed vara möjligt för medlemsstaterna att t.ex. tillämpa nationella tillitsnivåer, något förordningen för övrigt tar höjd för. Dessa bör emellertid i så fall endast kunna tillämpas vid nationell användning av e-legitimationer.

Enligt skäl 16 i förordningens ingress beror tillitsnivån på den grad av tillit en e-legitimation ger i fråga om en persons påstådda eller styrkta identitet med beaktande av olika processer (t.ex. styrkande och kontroll av identitet, och autentisering), förvaltningsverksamhet (t.ex. den enhet som utfärdar e-legitimationer och förfaranden för att utfärda sådana medel) och de tekniska kontroller som tillämpas. I kommissionens genomförandeförordning (EU) 2015/1502 fastställs tekniska minimispecifikationer och förfaranden för respektive tillitsnivå. Dessa ska användas för att specificera tillitsnivån för e-legitimationer som utfärdats inom ett anmält e-legitimationssystem.

Specifikationerna och förfarandena bygger på den internationella standarden ISO/IEC 29115. Utöver de delar som nämns ovan avser de bl.a. också krav på effektiva ledningssystem för informationssäkerhet.

4.2.5 Den offentliga förvaltningen ska erkänna utländska e-legitimationer

För att uppnå förordningens syfte innehåller den bestämmelser om s.k. ömsesidigt erkännande av e-legitimationssystem. Det kan kortfattat beskrivas som att medlemsstaterna ska erkänna varandras anmälda system. I artikel 6 i förordningen föreskrivs att när det enligt nationell rätt eller enligt nationella administrativa förfaranden krävs elektronisk identifiering där e-legitimationer och autentisering används

för att få åtkomst till en nättjänst som tillhandahålls av ett offentligt organ i en medlemsstat, ska de e-legitimationer som utfärdats i en annan medlemsstat erkännas i den första medlemsstaten för gränsöverskridande autentisering för tjänsten. Begreppet nättjänst definieras inte i förordningen men tjänster som vi i Sverige vanligen kallar för digitala tjänster eller e-tjänster omfattas.

För att ömsesidigt erkännande ska bli aktuellt krävs dock att tre förutsättningar är uppfyllda:

- E-legitimationen ska vara utfärdad inom ramen för ett anmält e-legitimationssystem.
- Tillitsnivån för e-legitimationen ska motsvara en tillitsnivå som är lika hög eller högre än den tillitsnivå som det berörda offentliga organet kräver för åtkomst till nättjänsten, förutsatt att tillitsnivån för e-legitimationen motsvarar tillitsnivån väsentlig eller hög.
- Det offentliga organet i fråga använder tillitsnivån väsentlig eller hög i samband med åtkomst till nättjänsten.

Förordningens krav på ömsesidigt erkännande gäller inte för e-legitimationer på tillitsnivå låg eller för nättjänster som använder tillitsnivå låg för åtkomst. För anmälda e-legitimationer som motsvarar tillitsnivån låg gäller i stället att dessa får erkännas av det offentliga organ som tillhandahåller nättjänsten, men det är inget krav.

Erkännandet av e-legitimationssystem ska ske senast tolv månader efter det att kommissionen offentliggör förteckningen över anmälda system. Det kan i sammanhanget noteras att trots kravet på erkännande av anmälda medel för elektronisk identifiering innebär det inte att den som loggat in på detta sätt i praktiken alltid har möjlighet att använda tjänsterna. Det är vanligt att den som använder en utländsk e-legitimation för att logga in i en svensk digital tjänst i dagsläget hamnar i ett s.k. digitalt väntrum där det inte går att utföra det förfarande tjänsten avser. Detta är en följd av att många digitala tjänster inom den offentliga förvaltningen ställer krav på användning av exempelvis personnummer. Även om innehavaren av den utländska e-legitimationen har ett svenskt personnummer finns det ingen koppling mellan den utländska e-legitimationen och personnumret som möjliggör att tjänsten kan användas.[2]

[2] Skatteverket, *Fördjupad utredning rörande koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar* (Dnr 2 02 27351-19/113), s. 31.

Det kommer dock för vissa digitala tjänster att förändras i och med att krav i EU-förordningen (EU) 2018/1724 om en gemensam digital ingång börjar gälla. Kraven innebär bl.a. att användare i gränsöverskridande situationer ska kunna identifiera sig samt underteckna eller stämpla handlingar på elektronisk väg i enlighet med eIDAS-förordningen.

4.2.6 Kvalificerade elektroniska underskrifter

Utredningen ska enligt direktiven analysera om den statliga e-legitimationen ska kunna användas för att framställa kvalificerade elektroniska underskrifter. Elektroniska underskrifter är en betrodd tjänst som regleras i eIDAS-förordningen. Det finns tre nivåer av elektroniska underskrifter i eIDAS-förordningen. De två högre nivåerna är avancerade respektive kvalificerade elektroniska underskrifter.

I artikel 3 i eIDAS-förordningen definieras en kvalificerad elektronisk underskrift som en avancerad elektronisk underskrift som skapas med hjälp av en kvalificerad anordning för underskriftsframställning och som är baserad på ett kvalificerat certifikat för elektroniska underskrifter.

Kraven på kvalificerade elektroniska underskrifter innebär att den som ska tillhandahålla tjänsten ska vara en kvalificerad tillhandahållare av betrodda tjänster och att den betrodda tjänsten är kvalificerad. För att bli en kvalificerad tillhandahållare ska denne anmäla sig till en tillsynsmyndighet och tillsammans med anmälan bifoga en rapport från en bedömning av överensstämmelse som har gjorts av ett ackrediterat organ för bedömning av överenstämmelse. Organet för bedömning av överenstämmelse ska granska att tillhandahållaren och den tjänst som den tillhandahåller uppfyller de krav som finns i eIDAS-förordningen. De krav som ska följas i förordningen är de allmänna krav som gäller för tillhandahållare och betrodda tjänster och de specifika krav som finns för tjänsten kvalificerade elektroniska underskrifter.

De allmänna kraven gäller t.ex. de allmänna säkerhetskraven och kraven på incidentrapportering i artikel 19, kraven på granskning och periodicitet på omgranskning av tillhandahållare och tjänst i artikel 20 och krav på att ha tillräckliga ekonomiska medel eller ansvarsförsäkring för att bära risken för skadestånd enligt artikel 13 samt att enligt

artikel 24 ha en plan för att säkerställa kontinuitet i händelse av upphörande av tjänsten.

4.2.7 Revidering av eIDAS-förordningen

EU-kommissionen presenterade den 3 juni 2021 ett förslag till ändringar i eIDAS-förordningen.[3] De föreslagna ändringarna bestod dels av att nuvarande bestämmelser justeras eller tas bort, dels av att nya bestämmelser införs.

Vad gäller elektronisk identifiering föreslog kommissionen bl.a. att en europeisk digital identitetsplånbok ska införas. En digital identitetsplånbok är enligt den föreslagna definitionen en produkt och en tjänst som låter användaren spara identitetsuppgifter och attribut rörande t.ex. kvalifikationer samt attribut som är kopplade till användarens identitet. Enligt förslaget ska medlemsstaterna utfärda plånböckerna till fysiska och juridiska personer. De kan också utfärdas på uppdrag av medlemsstaterna eller självständigt, och erkännas av medlemsstaterna.

De föreslagna plånböckerna ska accepteras av medlemsstaterna för åtkomst till nättjänster som tillhandahålls av myndigheter. Privata förlitande parter inom vissa utpekade sektorer ska också acceptera dem för åtkomst till sina digitala tjänster, under förutsättning att tjänsten omfattas av krav på att använda stark autentisering. Enligt skäl 9 i förordningsförslagets ingress föreslås plånböckerna kunna användas för institutionella behov hos bl.a. offentliga förvaltningar och internationella organisationer.

Vid sidan av den digitala identitetsplånboken föreslog EU-kommissionen även ändringar kopplade till anmälan av system för elektronisk identifiering.

Rådets kompromissförslag antogs den 6 december 2022 och utgör medlemsländernas utgångspunkt i trilogen. En av de ändringar som rådet föreslog är att alla medlemsstater ska anmäla minst ett system för elektronisk identifiering som omfattar minst ett medel för identifiering på tillitsnivå hög.[4]

[3] COM(2021) 281 final.
[4] Ständiga representanternas kommitté (Coreper I), 25 november 2022, Förslag till Europaparlamentets och rådets förordning om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av en ram för europeisk digital identitet – Allmän riktlinje.

Europaparlamentet presenterade därefter sina ståndpunkter i mars 2023.

Den 29 juni 2023 presenterade Europaparlamentet och rådet en preliminär politisk överenskommelse om de viktigaste elementen i förslaget som utgör inriktningen i de avslutande trilogerna under hösten 2023.[5]

4.3 Tillitsramverket för Svensk e-legitimation

Myndigheten för digital förvaltning (Digg) utvecklar och förvaltar tillitsramverket för Svensk e-legitimation med stöd av regleringen i lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering samt 3 § förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning där det framgår att Digg ska främja användningen av elektronisk identifiering. Ramverket syftar till att etablera gemensamma krav för utfärdare av kvalitetsmärkta svenska e-legitimationer. Ramverket togs ursprungligen fram av E-legitimationsnämnden, vars uppgifter övertogs av Digg i september 2018 i samband med inrättandet av myndigheten.

Utredningen om effektiv styrning av nationella digitala tjänster föreslog att det i lag skulle regleras att ramverket skulle vara en del av infrastrukturen för elektronisk identifiering och att kvalitetsmärket skulle regleras i samma lag. Förslaget bereds inom Regeringskansliet.[6]

Ramverket bygger på den internationella standarden ISO/IEC 29115, ISO/IEC 27000-serien och andra internationella ramverk, men vissa nationella anpassningar har gjorts.

I ramverket fastställs krav som riktar sig mot utfärdare av e-legitimationer. Kraven avser bl.a. utfärdarens kontroller av att en person som tilldelas en e-legitimation verkligen är den som denne utger sig för att vara.

Kraven är indelade i tre olika tillitsnivåer; 2, 3 och 4.

Tillitsnivå 1 definieras i ISO/IEC 29115 men har ingen motsvarighet i tillitsramverket eller i eIDAS-förordningens tillitsnivåer. Denna nivå kräver ingen legitimering, utan det räcker med att exempelvis ange namn och e-postadress.

[5] www.consilium.europa.eu/en/press/press-releases/2023/06/29/council-and-parliament-strike-a-deal-on-a-european-digital-identity-eid/ (hämtad 2023-09-22).
[6] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 31 ff.

Tillitsnivåerna 2–4 innebär minst tvåfaktorsautentisering, men graden av säker grundidentifiering och övrig skyddsnivå vid autentisering skiljer sig åt (se mer om detta nedan). Det är i normalfallet upp till förlitande part att avgöra vilken lägsta tillitsnivå som ska krävas för tillgång till en digital tjänst. Till stöd för denna bedömning finns vägledningar från bl.a. Digg och Myndigheten för samhällsskydd och beredskap.[7] Grunden är informationsklassning i kombination med bedömning av vilken skada en felaktig identifiering skulle kunna leda till. Vissa författningar och tillsynsbeslut ger också vägledning vad avser sådana bedömningar.

4.3.1 Övergripande krav som avser utfärdares verksamhet

Övergripande krav på den verksamhet som utfärdare av e-legitimationer bedriver är bl.a. att de ska teckna och vidmakthålla för verksamheten erforderliga försäkringar samt ha förmåga att bära risken för skadeståndsskyldighet. Utfärdare ska för de delar av verksamheten som berörs i tillitsramverket ha ett ledningssystem för informationssäkerhet (LIS) som i tillämpliga delar baseras på ISO/IEC 27001 eller motsvarande likvärdiga principer för ledning och styrning av informationssäkerhetsarbetet. Kravet rörande ledningssystemets mognadsgrad ökar för högre tillitsnivåer. Ramverket innehåller också bl.a. krav på bakgrundskontroll innan personer antar vissa roller som är av särskild betydelse för säkerheten. Ett exempel på skillnader i krav för de olika nivåerna är att för nivå 3 och 4 ska utfärdare genom hela kedjan i utfärdandeprocessen säkerställa att separation av arbetsuppgifter tilllämpas på ett sådant sätt att ingen på egen hand har möjlighet att tillskansa sig en e-legitimation i en annan persons namn. Kraven är mindre krävande för nivå 2.

Ramverket innehåller även krav som avser teknisk säkerhet, exempelvis att elektroniska kommunikationsvägar som nyttjas i verksamheten för överföring av känsliga uppgifter ska skyddas mot insyn, manipulation och återuppspelning.

[7] Myndigheten för digital förvaltning, *Vägledning till uppfyllande av tillitsramverkets krav för kvalitetsmärket Svensk e-legitimation* och Myndigheten för samhällsskydd och beredskap, *Vägledning – säkerhetsåtgärder i informationssystem för statliga myndigheter* (MSB2032).

4.3.2 Krav kopplade till ansökan och utfärdande

Ramverket innehåller ett antal krav som avser ansökan om en e-legitimation och själva utfärdandet av e-legitimationen. Utfärdare ska föra register över anslutna användare och de tilldelade e-legitimationerna. De ska också tillhandahålla en spärrtjänst där användaren kan spärra sin e-legitimation.

Utfärdare ska kontrollera att uppgifter knutna till en ansökan om utfärdande av e-legitimation är fullständiga och stämmer överens med uppgifter som finns registrerade i ett officiellt register. Utfärdaren kan identifiera en sökande på distans med exempelvis en befintlig godkänd Svensk e-legitimation på minst samma tillitsnivå som den som ska ges ut, om avtalsvillkoren för den e-legitimationen tillåter det. Nivå 4 ställer ytterligare krav på e-legitimationens giltighetstid, för att bibehålla tillitsnivåns princip att personlig inställelse ska ske vart femte år. Distansidentifiering kan också göras på tillitsnivå 2 och 3 genom jämförelse av en giltig fullgod identitetshandling med sökandens ansiktsbild, där nivå 2 tillåter bildupptagning av identitetshandlingen medan nivå 3 kräver att handlingens äkthet och dess innehåll kan avläsas maskinellt och verifieras på kryptografisk väg. Digg har sammanfattat tillitsnivå 2–4 på följande sätt.

Tillitsnivå 2

- Användarens identitet verifieras genom att bevisa innehav av en tillhörighet som bara användaren kan antas förfoga över. Exempel kan vara kod som skickats i kodkuvert till sökandes folkbokföringsadress.
- Användaren identifieras genom exempelvis engångslösenord från dosa eller mobiltelefon.
- Det finns en viss tillit till identiteten, och krav på tvåfaktorsautentisering.

Tillitsnivå 3

- Användarens identitet verifieras på likvärdigt sätt som vid utgivning av en fullgod svensk legitimationshandling. E-legitimationen kan utfärdas på distans om utfärdaren redan har identifierat mottagaren, t.ex. i samband med öppnandet av ett bankkonto eller vid en anställning.
- Användaren identifieras genom exempelvis en skyddad app i en smarttelefon.
- Det finns en hög tillit till identiteten, och krav på tvåfaktorsautentisering.

Tillitsnivå 4

- Användarens identitet verifieras vid personligt besök genom en fullgod svensk legitimationshandling, både första gången och vid förnyelse vart femte år.
- Användaren identifieras genom en e-legitimation som skyddas i ett särskilt chip, som kan finnas på t.ex. ett plastkort, en mobiltelefon eller en USB-enhet. Det finns en mycket hög tillit till identiteten, och krav på tvåfaktorsautentisering.

4.3.3 Kvalitetsmärket Svensk e-legitimation

Utfärdare som har godkänts enligt tillitsramverket på tillitsnivå 3 eller 4 har möjlighet att teckna licensavtalet för Kvalitetsmärket Svensk e-legitimation. Syftet med märket är att offentliga och privata aktörer med digitala tjänster som kräver e-legitimation ska kunna lita på e-legitimationer som har märket och att användare ska kunna känna sig trygga med att det är en säker identitetshandling. En utfärdare som vill använda märket ansöker om det hos Digg som gör en granskning utifrån tillitsramverket och beslutar om utfärdaren lever upp till kraven. Beslutet avser vilken nivå den aktuella e-legitimationslösningen lever upp till och publiceras på Diggs webbplats. Digg följer även upp de e-legitimationer som godkänts för att säkerställa efterlevnad över tid.

4.4 E-legitimationer på den svenska marknaden

4.4.1 Inledning

Nedan redogörs för de utfärdare av e-legitimationer som i dagsläget finns på den svenska marknaden. E-tjänstelegitimationer omfattas inte av redogörelsen nedan.

4.4.2 AB Svenska Pass

Skatteverkets identitetskort för folkbokförda i Sverige innehåller en e-legitimation som från och med september 2017 utfärdas av AB Svenska Pass (härefter Svenska Pass). Bolaget har avtal med Skatteverket om att förse det fysiska id-kortet med en e-legitimation. Det innebär att det är Svenska Pass och inte Skatteverket som har det juridiska ansvaret gentemot både innehavaren av e-legitimationen och de förlitande aktörer som ingått avtal med Svenska Pass. Svenska Pass e-legitimation kan endast användas för identifiering gentemot Skatteverket och för att kunna använda e-legitimationen krävs en dator och en kortläsare.[8]

För att skaffa e-legitimationen måste den sökande vara folkbokförd i Sverige, ha fyllt 13 år och kunna legitimera sig. Om den sökande är under 18 år måste denne ha tillstånd av sin vårdnadshavare. Svenska Pass e-legitimation är godkänd enligt Diggs tillitsramverk på tillitsnivå 4.[9] E-legitimationen ingår inte i något valfrihetssystem och är inte heller anmäld för gränsöverskridande användning inom ramen för eIDAS-förordningen.

4.4.3 BankID

BankID ägs, förvaltas och vidareutvecklas av Finansiell ID-Teknik BID AB (härefter Finansiell ID-Teknik). Finansiell ID-Teknik bildades år 2002 och ägs av Danske Bank, Handelsbanken, Ikano Bank, Länsförsäkringar Bank, SEB, Skandiabanken och Swedbank. Innan företaget bildades hade de stora bankerna i Sverige inlett ett arbete i ett bankkonsortium. Syftet med det arbetet var att ta fram en generell

[8] www.skatteverket.se/privat/folkbokforing/idkort/elegitimationpaidkortet.4.3810a01c150939e893f8169.html (hämtad 2023-09-19).
[9] Äldre versioner av Svenska pass e-legitimation är endast godkända på tillitsnivå 3.

infrastruktur för elektroniska identitetshandlingar, som skulle uppfylla krav från myndigheter och banker samt kunna accepteras av allmänhet och företag.

Bolagets kunder är de flesta av de stora svenska bankerna, som i sin tur säljer och förmedlar BankID. I dagsläget är det tio banker som utfärdar BankID.[10] Det finns tre olika varianter av BankID, Mobilt BankID, BankID på fil och BankID på kort. Mobilt BankID innebär att användaren har sin e-legitimation i en mobiltelefon eller surfplatta. För att kunna hämta och använda Mobilt BankID krävs att användaren har installerat BankID-appen.

BankID på fil är en e-legitimation i en dator. För att kunna hämta och använda BankID på fil krävs att användaren har installerat BankID-programmet.

BankID på kort är en e-legitimation som är lagrad på ett smartkort. Förutom kortet och BankID-programmet krävs även att användaren har en kortläsare för att använda denna lösning.

Vilka lösningar som de olika bankerna erbjuder sina kunder skiljer sig åt. Mobilt BankID och BankID på fil är kostnadsfria för användaren. Vissa banker tar betalt för BankID på kort, exempelvis Swedbank där kortet kostar 400 kronor och den tillhörande kortläsaren 100 kronor.[11]

I nuläget har 8,4 miljoner personer någon variant av BankID och under år 2022 användes BankID för att genomföra 6,7 miljarder transaktioner. Av dessa transaktioner sker endast cirka 8 procent inom offentlig sektor.[12] BankID kan användas i över 6 000 digitala tjänster.[13]

För att kunna skaffa ett BankID måste en person ha ett svenskt personnummer och vara kund i någon av de banker som ger ut BankID. Respektive bank bestämmer själva vilken åldersgräns som krävs för att inneha ett BankID som de utfärdar. Om den sökande är under 18 år måste denne dock alltid ha tillstånd av vårdnadshavare. BankID på fil, BankID på kort och Mobilt BankID är godkända på tillitsnivå 3 enligt Diggs tillitsramverk. BankID är även granskad för gränsöverskridande användning inom ramen för eIDAS-förordningen på nivå väsentlig.

[10] www.bankid.com/privat/skaffa-bankid (hämtad 2023-09-19).
[11] www.swedbank.se/privat/rantor-priser-och-kurser/legitimationbankid.html (hämtad 2023-09-19).
[12] www.bankid.com/om-oss/statistik (hämtad 2023-09-19).
[13] Ibid.

4.4.4 Freja+

Freja+ är en mobil e-legitimation som ägs, förvaltas och utvecklas av Freja eID Group AB (härefter Freja). Det är kostnadsfritt för användare att skaffa Freja+.

Den 30 juni 2023 hade Freja cirka 900 000 registrerade användare, vilket var en ökning med 35 procent jämfört med föregående år. Under samma period utfördes cirka 5,4 miljoner transaktioner.[14] Freja+ kan i dagsläget användas i cirka 600 digitala tjänster.[15]

För att skaffa Freja+ krävs för närvarande att sökanden förekommer i folkbokföringsregistret och kan legitimera sig med en svensk ID-handling. Freja har emellertid nyligen aviserat att de under hösten 2023 kommer att utfärda Freja+ till personer med samordningsnummer med styrkt identitet förutsatt att dessa har ett hemlandspass som är utfärdat inom EU eller EES.[16] För att få Freja+ måste användaren vara minst 8 år och barn upp t.o.m. 12 år måste ha vårdnadshavarens godkännande.

Freja+ är godkänd enligt Diggs tillitsramverk på tillitsnivå 3 och är därtill godkänd för gränsöverskridande användning inom ramen för eIDAS-förordningen på nivå väsentlig.

4.5 Intäktsmodeller för e-legitimationsutfärdare

Det finns i dagsläget tre huvudsakliga intäktsmodeller för e-legitimationsutfärdare, en där ersättning utgår från den som anskaffar e-legitimationen och två där ersättning utgår från förlitande part. Om ersättning utgår från förlitande part kan ersättningen utgå per användningstillfälle eller enligt en fast avgift för en viss tidsperiod. Vi väljer därmed att kalla den första varianten för den transaktionsbaserade modellen och den andra för abonnemangsmodellen. Den modell där ersättning utgår från den som anskaffar e-legitimationen kallar vi anskaffningsmodellen.

Som framgått innebär den transaktionsbaserade modellen vanligen att en kostnad uppstår (ofta benämnd tickkostnad) varje gång e-legiti-

[14] Freja eID Group AB, Delårsrapport 1 april – 30 juni 2023, s. 11 f.
[15] Freja eID Group AB, Pressmeddelande *Nya regler möjliggör fler användare och kunder för Freja*, 2023-08-31.
[16] Ibid.

mationen används. Exempelvis är tickkostnaden inom valfrihetssystemen 17 öre per transaktion.

Den grundläggande principen bakom denna modell är att den som får nyttan av användningen, dvs. gynnas av den säkra autentisering som användningen av en e-legitimation innebär, också ska betala för den. Samma princip gäller även för abonnemangsmodellen.

Den anskaffningsbaserade modellen grundar sig som framgått på att den som anskaffar e-legitimationen också betalar för den. Denna modell är den som vanligen används av utfärdare av e-tjänstelegitimationer och här är det vanligast med en fast avgift per tidsintervall eller en avgift per användare med begränsning i tid.[17]

Det som tydligast skiljer den anskaffningsbaserade modellen och övriga modeller åt är vem som betalar. Vad som prissätts och vad som utgör basen för betalningen kan emellertid variera och kombineras på olika sätt. Det går således även att inom ramen för den anskaffningsbaserade modellen låta kostnaden helt eller delvis styras av antalet transaktioner. BankID är ett exempel på en e-legitimation som huvudsakligen använt sig av den transaktionsbaserade modellen. Av våra kontakter med Finansiell ID-Teknik har dock framgått att det råder fri konkurrens mellan de banker som utfärdar BankID och att andra ersättningsformer kan förhandlas fram.

4.6 Anskaffning av tjänster för elektronisk identifiering

En myndighet som vill erbjuda möjligheten att logga in med e-legitimation kan anskaffa tjänster för elektronisk identifiering genom valfrihetssystem, egen upphandling eller avrop från ramavtal.

I Sverige har inriktningen de senaste tio åren varit att aktörer inom förvaltningen bör använda sig av valfrihetssystem för e-legitimationer. Förfarandet regleras i lagen om valfrihetssystem i fråga om tjänster för elektronisk identifiering. Enligt 2 § avses med valfrihetssystem ett förfarande där den enskilde har rätt att välja den leverantör som ska utföra tjänsten och som en upphandlande myndighet har godkänt och tecknat avtal med. Det finns två valfrihetssystem för e-legitimationer: Valfrihetssystem 2017 respektive Valfrihetssystem 2018. Dessa administreras av Digg som också tillhandahåller anslutnings-

[17] *Användning av e-legitimation i tjänsten i den offentliga förvaltningen* (SOU 2021:62), s. 90.

avtal mellan leverantör av elektronisk identifiering direkt kopplad till vald e-legitimation och förlitande part. En myndighet som vill erbjuda sina användare att använda olika e-legitimationer är förlitande part och kan ansluta sig till valfrihetssystemen genom att ingå respektive avtal. I dagsläget är 94 aktörer anslutna till ett eller båda valfrihetssystemen i egenskap av förlitande parter.

I en nyligen lämnad proposition föreslås att valfrihetssystemen ska ersättas av auktorisationssystem.[18] I promemorian som delvis ligger till grund för förslagen i propositionen föreslås också att det ska införas förordningsbestämmelser om att statliga myndigheter som har behov av tjänster för elektronisk identifiering ska använda de tjänster som tillhandahålls genom auktorisationssystemen.[19] Konsekvensen av detta är att statliga myndigheter inte kan välja andra anskaffningsformer, exempelvis egen upphandling av tjänsterna eller avrop på ramavtal.

I Kammarkollegiets ramavtalsområden inom Programvaror och Tjänster finns t.ex. krav på att tjänster inom elektronisk identifiering ska kunna levereras.[20] Avtal kan ingås direkt med e-legitimationsutfärdare eller med en aktör som fungerar som mellanhand och erbjuder en tjänst som gör det möjligt för användarna att logga in med e-legitimationer från olika utfärdare.

4.7 Tidigare förslag rörande införandet av en statlig e-legitimation

4.7.1 Regeringsuppdrag till Verva

Den numera nedlagda myndigheten Verket för förvaltningsutveckling (Verva) fick i november 2006 av regeringen i uppdrag att leda och samordna statsförvaltningens utvecklingsarbete avseende säkert elektroniskt informationsutbyte och säker hantering av elektroniska handlingar.[21] Uppdraget preciserades därefter till att även omfatta förslag till en modell för en långsiktig hantering av e-legitimationer.[22]

[18] Prop. 2023/24:6.
[19] *Auktorisationssystem för elektronisk identifiering och för digital post*, s. 41 ff.
[20] Kammarkollegiet, *Vägledning för avrop av tjänster för elektronisk identifiering och elektronisk underskrift från ramavtalsområden inom Programvaror och Tjänster 2019* (Version 2.0).
[21] Fi2006/6773, delvis, Fi2006/967.
[22] *Elektronisk identifiering och underskrift i Sverige* Särtryck ur 2008:12, Verva, s. 7.

Verva bedömde att det fanns fyra möjliga vägval för den fortsatta utvecklingen av e-legitimationer. Dessa vägval baserades på olika grader av statligt ansvar och åtagande.[23]

Det alternativ som Verva betecknade som ”Ett helstatligt alternativ” innefattade att staten helt och hållet tog hand om att utfärda alla e-legitimationer som kunde användas i offentliga digitala tjänster. Utmärkande för detta alternativ var att det endast fanns en utfärdare av e-legitimationer för offentliga e-tjänster.

Fördelen med detta alternativ var enligt Verva var att staten kunde sätta en de facto-standard och slippa ta hänsyn till de skillnader som fanns inom området och som fördyrade utbyggnaden av digitala tjänster inom förvaltningen. Med endast en utfärdare hade e-legitimationerna enligt Verva alla förutsättningar att etableras som ett tydligt och välkänt begrepp och varumärke. Utfärdandet kunde ske under specifikationer och regler som gäller alla offentliga tjänster och e-legitimationen fick därmed hög tillit och acceptans.

Som negativa aspekter av en sådan lösning lyfte Verva fram att ett helstatligt alternativ kan föra med sig att marknadens förutsättningar begränsas när inga andra utfärdare kommer att finnas för e-legitimationer till offentliga digitala tjänster. Efter en första upphandling där en leverantör fått uppdraget, begränsas konkurrenternas intresse för att tillgodose den offentliga förvaltningens behov. Samtidigt kan staten hamna i en beroendeställning till en leverantör.

Verva förordade emellertid inte detta alternativ utan föreslog i stället att regeringen skulle säkerställa att det fanns en reglerad ordning för e-legitimationer. Förslaget innefattade även att det nationella identitetskortet skulle kunna användas som bärare av en svensk e-legitimation. Så som förslaget utformades skulle alla e-legitimationer som fick statusen ”svensk e-legitimation” kunna utfärdas med det nationella identitetskortet som bärare.[24]

4.7.2 Utredningen om effektiv styrning av nationella digitala tjänster

Utredningen om effektiv styrning av nationella digitala tjänster hade i uppdrag att bl.a. lämna förslag på långsiktig utformning av det offentliga åtagandet när det gäller ansvarsfördelningen mellan offentlig och

[23] A.a, s. 23 ff.
[24] A.a. s. 27 ff.

privat sektor i processen för grundidentifiering och utfärdande av e-legitimationer så att tillgången till enkla och säkra e-legitimationer för alla säkerställs. Utredningen skulle även analysera och lämna förslag på hur konkurrens och innovation på den privata marknaden för utfärdande av e-legitimationer kunde främjas på lång sikt.[25]

Utredningen bedömde att det bör vara ett statligt åtagande att det finns en tillförlitlig process för grundidentifiering. Utredningen föreslog även att staten skulle utfärda en e-legitimation för att på det viset säkerställa att medborgare och folkbokförda kan få en sådan. Den statliga e-legitimationen skulle enligt förslaget utfärdas samtidigt med en statlig fysisk identitetshandling. Den statliga elektroniska identitetshandlingen skulle kunna användas för identifiering hos myndigheter, men också kunna växlas till en mobil elektronisk identitetshandling. Därmed skulle den statliga elektroniska identitetshandlingen kunna fungera som en backup om t.ex. mobiltelefonen blir obrukbar.[26]

4.7.3 2017-års ID-kortsutredning

Som en del av uppdraget för 2017-års ID-kortsutredning ingick att analysera och ta ställning till om fysiska identitetshandlingar bör innehålla en e-legitimation på högsta tillitsnivå.[27]

Utredningen föreslog att en statlig e-legitimation på högsta tillitsnivå skulle finnas på det statliga identitetskortet. E-legitimationen skulle även kunna användas för att skapa en elektronisk underskrift.[28]

Den statliga e-legitimationen föreslogs kunna utfärdas till personer som har fyllt 13 år och som är svenska medborgare eller folkbokförda i landet. Utfärdandet skulle följa processen för utfärdande av id-kortet. Härigenom ansåg utredningen att samma höga nivå av säkerhet kunde uppnås för den föreslagna e-legitimationen som för statliga fysiska identitetshandlingar.

Utredningen föreslog vidare att Polismyndigheten skulle utfärda de statliga identitetshandlingarna, inklusive den statliga e-legitimationen.[29]

[25] Dir. 2016:39.
[26] *reboot – omstart för den digitala förvaltningen* (2017:114), s. 24.
[27] Dir. 2017:90.
[28] *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14), s. 319 ff.
[29] A.a. s. 326 ff.

4.7.4 Regeringsuppdrag till Myndigheten för digital förvaltning

I juni 2022 fick Digg ett regeringsuppdrag om att analysera möjligheterna för, och lämna förslag om, framtagandet och driften av en statlig e-legitimation.[30] I uppdraget ingick att säkerställa att e-legitimationen utformas på ett sådant sätt att så många som möjligt kan använda den samt att överväga alternativ som kan sänka kostnaden och tidsåtgången för införandet. I januari 2023 överlämnade Digg sin slutrapport till regeringen.[31]

Diggs förslag innebär att den statliga e-legitimationen ska utfärdas på ett kontaktlöst aktivt kort samt att utvecklingsarbetet i ett nästa steg inriktas mot att undersöka hur e-legitimationen även kan tillhandahållas via de nationella identitetskorten.[32]

Det kontaktlösa aktiva kortet ska enligt Diggs förslag lämnas ut av en identitetskontrollerande myndighet efter kontroll av giltig id-handling. Den statliga e-legitimationen ska ges ut på den högsta tillitsnivån. Digg föreslog också att den statliga e-legitimationen ska kunna ges ut till personer som har tilldelats ett samordningsnummer och kan styrka sin identitet.[33]

Den statliga e-legitimationen föreslogs vara ett komplement till de lösningar som marknaden erbjuder och ska erbjudas på samma villkor. Digg föreslog vidare att den statliga e-legitimationen ska erbjudas offentliga aktörer via valfrihetssystem och att privata aktörer ska få tillgång till en statlig identifieringstjänst för att sedan kunna utfärda identitetsintyg till digitala tjänster.[34] Närmare redogörelser för olika delar av Diggs förslag återfinns i kapitel 7.

[30] *Uppdrag att föreslå hur en statlig e-legitimation kan utformas* (I2022/01335).
[31] Myndigheten för digital förvaltning, *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*.
[32] A.a. s. 31 ff.
[33] A.a. s. 35, 38 f. och 42 ff.
[34] A.a. s. 50.

5 Internationell utblick

5.1 Inledning

Sverige är ett av få EU-länder som i dagsläget inte har en anmäld e-legitimation för privatpersoner på den högsta tillitsnivån. I många EU-länder är det även staten som utfärdar e-legitimationer till privatpersoner. Den begränsade utredningstiden har inte möjliggjort någon mer utförlig undersökning av de statliga e-legitimationer som andra länder tillhandahåller. Nedan redogörs emellertid översiktligt för ett urval av statliga e-legitimationer som tillhandahålls av andra EU-länder.

5.2 Danmark

I Danmark är det sedan ett antal år tillbaka som huvudregel obligatoriskt för invånare att använda digitala självbetjäningstjänster samt att ta emot digital post från myndigheter.[1] Tidigare var NemID den dominerande e-legitimationslösningen i Danmark. Mellan oktober 2021 och juni 2023 fasades MitID in som den nya lösningen genom att bl.a. föra över befintliga NemID-användare. MitID utvecklades av den danska motsvarigheten till Myndigheten för digital förvaltning (Digg), Digitaliseringsstyrelsen, och Finans Danmark, som är en intresseorganisation för banker och andra aktörer inom finansområdet. Det privata företaget Nets DanID A/S sköter drift och administration av MitID. Digitaliseringsstyrelsen är emellertid personuppgiftsansvarig för hanteringen och Nets DanID A/S agerar som dess personuppgiftsbiträde.[2]

MitID erbjuds som mobil applikation, kod display, audio kodläsare, eller som ett fristående chip.[3] MitID erbjuds både på tillitsnivå väsentlig

[1] en.digst.dk/policy-and-strategy/mandatory-digitisation/self-service/ (hämtad 2023-09-24).
[2] www.mitid.dk/media/jh5nnnty/om-mitid_baggrund_v104.pdf (hämtad 2023-09-24).
[3] www.mitid.dk/en-gb/get-started-with-mitid/mitid-authenticators/ (hämtad 2023-09-24).

och hög. För den högsta tillitsnivån krävs användning av chiplösningen eller av den mobila applikationen med förbättrad säkerhet. Enligt uppgift från Digitaliseringsstyrelsen har ingen certifiering utförts av den mobila applikationen med förbättrad säkerhet.

MitID-appen är gratis för användarna och detsamma gäller användarens tre första kod displayer eller audio kodläsare. MitID chip kostar cirka 144 danska kronor.[4]

Ansökan om MitID kan göras antingen digitalt eller genom att besöka medborgarservicekontor (”Borgerservice”), men för tillitsnivå hög krävs personlig inställelse.[5] MitID utfärdas som huvudregel till personer som är 15 år eller äldre. I vissa situationer kan även personer som är 13 eller 14 år få MitID.[6]

5.3 Estland

I Estland har staten tagit ett helhetsansvar vad gäller digitala identiteter och lösningar för autentisering. Det är obligatoriskt för medborgare i Estland och medborgare från andra EU-länder som bor i Estland permanent att ha ett nationellt ID-kort som tillhandahålls av staten. Kortet är försett med ett chip som innehåller en e-legitimation som kan användas i en stor mängd digitala tjänster, både offentliga och sådana som tillhandahålls av företag eller andra organisationer. Det finns också lösningar för andra bärare, såsom mobiltelefoner. Mobiltelefonlösningen (”Mobile-ID”) innebär att chipet är integrerat i telefonens SIM-kort.[7]

Den estniska polisen (The Estonian Police and Border Guard Board) utfärdar identitetskortet och är även ansvarig för den identifiering som sker i samband med ansökan.[8] Vad gäller mobiltelefonlösningen så upphandlas detta av den estniska motsvarigheten till Digg (The Estonian Information System Authority, RIA).[9]

Mobiltelefonlösningen kan, med vårdnadshavarnas godkännande, utfärdas till minderåriga från 7 års ålder.[10]

[4] www.mitid.dk/en-gb/help/help-universe/prices/ (hämtad 2023-09-24).
[5] www.mitid.dk/en-gb/help/help-universe/mitid-user/raise-ial/ (hämtad 2023-09-24).
[6] www.mitid.dk/en-gb/help/help-universe/13-to-14-years-old/ (hämtad 2023-09-24).
[7] The Estonian Police and Border Guard Board, Estonian eID scheme: Mobile-ID2022 Technical specifications and procedures for assurance level high for electronic identification.
[8] www.id.ee/en/rubriik/introduction/ (hämtad 2023-09-24).
[9] The Estonian Police and Border Guard Board, Estonian eID scheme: Mobile-ID2022 Technical specifications and procedures for assurance level high for electronic identification.
[10] Ibid.

5.4 Finland

Identitetskort kan utfärdas till finska medborgare och utlänningar som vistas i Finland (identitetskort för utlänningar). Identitetskort för utlänningar utfärdas om sökanden har ett giltigt uppehållstillstånd, uppehållskort eller sökandens uppehållsrätt är registrerad, sökanden har hemkommun i Finland och uppgifter om sökanden har registrerats i befolkningsdatasystemet.[11]

På identitetskortet finns ett chip som innehåller ett s.k. medborgarcertifikat, en e-legitimation som utfärdas av Myndigheten för digitalisering och befolkningsdata. I chipet är det också möjligt att lagra de personuppgifter som finns på kortet och, på innehavarens begäran, tekniska tillämpningar och uppgifter. På begäran av en myndighet kan det vidare för myndighetsanställda lagras sådan information som behövs för den anställdes arbetsuppgifter.[12]

Giltighetstiden är som huvudregel fem år. Ansiktsbild och övriga personuppgifter lagras i ett register. Ansökan om pass och id-kort ska göras hos polisen eller, om ansökan rör en finsk medborgare som vistas utomlands, hos en utlandsmyndighet. Till ansökan ska sökandens ansiktsbild fogas. Den utfärdande myndigheten tar inte några fotografier utan dessa överförs till polisens server av den fotograf som sökanden tar bilden hos. Ansökan om medborgarcertifikat är samordnad med ansökan om identitetskort. Identifieringen av sökanden ska ske på ett tillförlitligt sätt. Sökanden ska identifiera sig med ett giltigt finskt pass eller identitetskort utfärdat av polisen. Även främlingspass och resedokument för flykting kan användas under förutsättning att de inte har försetts med anteckning om att identiteten inte har kunnat styrkas. Om sökanden inte kan visa upp en giltig identitetshandling, görs identifieringen av den utfärdande myndigheten. Hur det ska gå till anges inte i lagen eller förordningen. Det kan t.ex. vara fråga om att jämföra sökandens fingeravtryck med de som finns i passregistret eller ställa kontrollfrågor utifrån uppgifter i olika register. Om en person som ansöker om ett identitetskort för utlänningar inte kan visa upp en giltig identitetshandling ska personen visa upp ett giltigt uppehållstillståndskort eller uppehållskort. Den utfärdande myndigheten får då ta sökandens fingeravtryck och jämföra med de avtryck som är lagrade i uppehållstillståndskortet eller uppehållskortet.[13]

[11] *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14), s. 157 f.
[12] Ibid.
[13] Ibid.

Kostnaden för att ansöka om ett identitetskort är 54 euro vid en elektronisk ansökan och 60 euro vid en fysisk ansökan.[14]

5.5 Nederländerna

I Nederländerna tillhandahåller staten e-legitimationen DigiD som erbjuds i formen av en mobil applikation. Det kostar inget att få en DigiD. E-legitimationen förvaltas och utfärdas av myndigheten Logius, som är Diggs nederländska motsvarighet. E-legitimationen är tillgänglig på tillitsnivå låg, väsentlig och hög.[15] För tillitsnivå hög krävs användning av appen i kombination med ett nederländskt körkort (utfärdat efter den 26 maj 2018) eller nationellt identitetskort (utfärdat efter den 1 januari 2021) som innehåller ett särskilt chip som läses av med telefonens NFC-läsare.[16]

Det finns ingen undre åldersgräns för DigiD och för barn som är 13 år eller yngre krävs vårdnadshavarens godkännande.[17] För barn som är 14 år eller äldre ska ansökan göras av barnen själva.[18]

5.6 Tyskland

Det tyska nationella identitetskortet innehåller sedan 2010 en e-legitimation som är integrerat i kortets chip. E-legitimationen är på tillitsnivå hög. E-legitimationsfunktionen är endast tillgänglig för den som är 16 år eller äldre. Om en person som innehar ett nationellt identitetskort fyller 16 år under kortets giltighetstid kan elegitimationsfunktionen då aktiveras utan extra kostnad. För personer under 24 år kostar det nationella identitetskortet cirka 23 euro och det är giltigt i sex år. För personer som är 24 år eller äldre kostar kortet 37 euro och är giltigt i tio år. [19]

[14] poliisi.fi/sv/serviceavgifter (hämtad 2023-09-24).
[15] Netherlands Court of Audit, *Digital Identity Demanding a Lot from DigiD and eHerkenning*, 29 mars 2023, s. 11.
[16] www.logius.nl/actueel/inloggen-met-rijbewijs-mogelijk-digid-app (hämtad 2023-09-24).
[17] www.nederlandwereldwijd.nl/digid-buiten-nederland/digid-kind (hämtad 2023-09-24).
[18] www.digid.nl/en/apply-and-activate/apply-digid (hämtad 2023-09-24).
[19] www.personalausweisportal.de/Webs/PA/EN/citizens/german-id-card/fees-and-validity/fees-and-validity-node.html#doc14627276bodyText1 (hämtad 2023-09-24).

Övriga medborgare i EU- och EES-stater kan få ett separat e-legitimationskort. Kortet kostar 37 euro och är giltigt i tio år. För att få ett e-legitimationskort måste man vara 16 år eller äldre.[20]

På kortet framgår bl.a. innehavarens för- och efternamn, födelsedatum och kortets giltighetstid. Korten utfärdas av lokala myndigheter på delstatsnivå.[21]

[20] www.personalausweisportal.de/Webs/PA/EN/citizens/id-card-for-eu-and-eea/eID-card-for-eu-and-eea-node.html;jsessionid=230FD85A4AF8D4BAE7CC1BAE6F381F02.1_cid340#doc14627306bodyText1 (hämtad 2023-09-24).
[21] Ibid.

6 Varför behövs en statlig e-legitimation?

6.1 Inledning

I utredningens uppdrag ingår att föreslå hur staten kan utfärda en kostnadseffektiv e-legitimation på högsta tillitsnivå. Enligt utredningens direktiv är syftet att stärka samhällets säkerhet och robusthet, motverka bedrägerier som begås med hjälp av e-legitimationer och underlätta för så många som möjligt att kunna få tillgång till en e-legitimation. Trots att uppdraget således är inriktat på hur en statlig e-legitimation på högsta tillitsnivå ska utformas och utfärdas, och inte på om en sådan e-legitimation behövs, anser vi att det är viktigt att tydliggöra behovsbilden. Dels för att förtydliga varför en statlig e-legitimation behövs, dels för att säkerställa att utredningens förslag i möjligaste mån tillgodoser de behov som finns.

Det bör poängteras att behovsbilden nedan inte tar hänsyn till det föreslagna införandet av en europeisk identitetsplånbok i den reviderade eIDAS-förordningen (se avsnitt 4.2.7). Införandet av nämnda identitetsplånbok kan – beroende på dess utformning och påverkan – förändra vissa av de förutsättningar som anges i detta kapitel.

6.2 Avsaknad av en anmäld e-legitimation på högsta tillitsnivån

Ett av förslagen i revisionen av eIDAS-förordningen ställer krav på medlemsstaterna att anmäla en e-legitimation på högsta tillitsnivå enligt ett särskilt anmälningsförfarande (se avsnitt 4.2.7). Detta krav kan uppfyllas genom att anmäla en statligt eller privat utfärdad e-legitimation. Förslaget innebär således inte att varje medlemsstat måste ha en statlig e-legitimation. Eftersom ingen av de e-legitimationer som

utfärdas för privat bruk i Sverige i skrivande stund är anmäld för gränsöverskridande användning på tillitsnivå hög, och eftersom ingen utfärdare heller har aviserat en avsikt att göra det, ankommer det på regeringen att se till att Sverige uppfyller detta krav. Om Sverige inte skulle uppfylla ett sådant kommande krav kan det leda till ett överträdelseärende.[1]

Som framgår av avsnitt 4.2.5 är det vid gränsöverskridande användning den som erbjuder en digital tjänst, t.ex. en myndighet i ett annat EU-land, som avgör vilken tillitsnivå som krävs. Avsaknad av en anmäld svensk e-legitimation på tillitsnivå hög innebär således att invånare i Sverige i nuläget utestängs från vissa digitala tjänster i andra medlemsstater, om de inte har tillgång till en e-legitimation på tillitsnivå hög från något annat land. Det finns därför även ett behov av att anmäla en e-legitimation på tillitsnivå hög för att säkerställa att svenska invånare får tillgång till digitala tjänster med motsvarande krav i andra EU-länder.

6.3 Grundidentifiering är ett statligt åtagande

Det går inte att entydigt säga vad som innefattas i begreppet grundidentifiering. Begreppet kan och brukar användas som benämning för den process som leder fram till att en identitetshandling (se avsnitt 3.2) utfärdas och som inbegriper att en individ ska styrka sin identitet (se avsnitt 3.1). För att kvalificeras som grundidentifiering har det anförts att det fordras att det i processen ingår personlig inställelse vid ansökan om och utlämnade av identitetshandlingen, att individen vid inställelsen styrker sin identitet på ett tillförlitligt sätt och att fysiska kännetecken hos individen i fråga dokumenteras av den utfärdande aktören.[2]

Myndigheten för digital förvaltning (Digg) har använt begreppet grundidentifiering med innebörden ”att kontrollera att en sökandes identitet är styrkt”, och konstaterat att den användningen ansluter väl till nuvarande regler inom området, exempelvis Polismyndighetens föreskrifter för pass och nationellt identitetskort.[3] Myndighetens för-

[1] Ett överträdelseärende initieras av EU-kommissionen om en medlemsstat inte tillämpar EU-lagstiftningen på rätt sätt. Om frågan inte går att lösa kan kommissionen överlämna ärendet till EU-domstolen som har möjlighet att döma medlemsstaten att betala böter eller ett löpande vite.
[2] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 173 ff., se även redovisningen i avsnitt 3.7.
[3] Myndigheten för digital förvaltning, *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, s. 42 f.

slag till utgivningsprocess innehåller krav på personlig inställelse och krav på att den sökande styrker sin identitet enligt de rutiner och krav som den identitetskontrollerande myndigheten föreskrivit. Huruvida förslaget därmed även innefattar dokumentationskrav avseende fysiska kännetecken av sökanden går inte direkt att utläsa, eftersom det lämnas åt den berörda myndigheten att meddela verkställighetsföreskrifter.

I vårt kommittédirektiv framhålls vikten av att grundidentifieringen kan göras på ett noggrant och säkert sätt av en myndighet vid ett personligt besök.[4]

Staten utfärdar som framgått fysiska identitetshandlingar. De identitetshandlingar som finns att tillgå i Sverige – fysiska eller elektroniska – är kopplade till den svenska folkbokföringen, vars hantering är ett ansvar och en uppgift för staten. Mot denna bakgrund är en grundidentifiering av enskildas identitet redan ett statligt åtagande.

Som anges i våra direktiv och som närmare behandlas i avsnitt 6.5 utgör numera e-legitimationer en samhällsviktig infrastruktur och det är allt svårare att klara sig utan tillgång till en sådan legitimation.

Att möjliggöra för fysiska personer att uppfylla identifikationskrav för att få tillgång till samhällets digitala tjänster är i sig en anledning till att staten bör åta sig ett ansvar för grundidentifiering så att medborgare och andra invånare ska kunna identifiera sig elektroniskt, oavsett att det kan var möjligt för en enskild att erhålla e-legitimation på annat sätt. Vidare går det redan av våra direktiv att utläsa att regeringen anser att staten har ett sådant ansvar.

6.4 Bättre förutsättningar för id-växling

Utfärdare av befintliga e-legitimationer använder sig av sina egna identifieringsprocesser. Eftersom dessa både är kostsamma och ställer höga krav på utförandet skapas en hög tröskel för nya aktörer att inträda på marknaden. Detta gäller både marknaden för kommersiella e-legitimationer och e-tjänstelegitimationer.

Flera tidigare utredningar har påtalat behovet av och framhållit fördelar med en statlig e-legitimation, bl.a. för att kunna användas för id-

[4] En del av uppdraget är att analysera vilka kontroller av identiteten som då behöver vidtas och om omfattningen av kontrollen ska vara jämförbar med den kontroll som sker för andra identitetshandlingar, se dir. 2022:142 s. 3.

växling, dvs. att en e-legitimation kan utgöra underlag vid utfärdande av andra e-legitimationer.[5]

Varje e-legitimationsutfärdare avgör huruvida id-växling ska tillåtas. I dagsläget finns endast begränsade möjligheter för svenska användare att genomföra id-växling. Exempelvis tillåter inte BankID detta enligt sina användarvillkor för förlitande parter.[6]

Det har anförts av bl.a. Sveriges Riksbank och Konkurrensverket att en statlig e-legitimation på högsta tillitsnivå som dels kan användas för att få tillgång till olika digitala tjänster, dels kan möjliggöra id-växling till andra e-legitimationer på lägre tillitsnivå, skulle kunna stärka konkurrensen på e-legitimationsmarknaden och potentiellt öppna för fler valmöjligheter för enskilda.[7]

Om staten ansvarar för grundidentifieringen kan en e-legitimation på den högsta tillitsnivån användas för att skaffa andra e-legitimationer och betrodda tjänster utan att en e-legitimationsutfärdare som erbjuder dessa behöver utföra en lika omfattande identifieringsprocess av en ny användare. Det kan handla om att det inte behövs ett fysiskt besök eller samma dokumentationskrav när en person redan har en statlig e-legitimation.

Även om detta i sig inte är ett skäl för att införa en statlig e-legitimation skulle en mer diversifierad marknad för e-legitimationer även bidra till att göra systemet mer robust och mindre sårbart för antagonistiska angrepp (se mer om detta i avsnitt 6.5). Syftet med att staten ansvarar för grundidentifieringen är att verka som en garant för ett säkert system för elektronisk identifiering. Andra utfärdare kan med stöd av id-växling från en statlig e-legitimation erbjuda sina användare ett helt elektroniskt ansökningsförfarande. På så vis kan andra utfärdare dra nytta av det statliga åtagandet att ansvara för grundidentifieringen.

[5] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114) s. 202 f., *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14) s. 321 f., *Användning av e-legitimation i tjänsten i den offentliga förvaltningen* (SOU 2021:62) s. 181 f. och *Staten och betalningarna* (SOU 2023:16) s. 372 f. Även Digg framhåller betydelsen av id-växling, *En säker och tillgänglig statlig e-legitimation,* s. 12 f.

[6] Detta anges bero på att BankID ges ut kostnadsfritt till användarna och kostnaderna för infrastrukturen finansieras av de förlitande parter som använder BankID i sina tjänster, se www.bankid.com/foretag/anslut-foeretag (hämtad 2023-09-07).

[7] Sveriges Riksbank, *Betalningsrapport 2022.,* s. 32. Konkurrensverket efterfrågade redan 2017 att en statlig e-legitimation skulle införas i Sverige. Detta eftersom kundautentisering är en mycket viktig del av betaltjänstmarknadens funktionssätt överlag och för tredjepartsaktörernas möjligheter att verka på marknaden, Konkurrensverket, *Betaltjänstmarknaden i Sverige*, Konkurrensverkets rapportserie 2017:7 (2017), s. 63 f.

6.5 Stärkt beredskap och ökad redundans

6.5.1 Risker med den ökade användningen av e-legitimationer

Den utbredda användningen av e-legitimationer inom många samhällsområden medför stora möjligheter och nyttor, men också risker. Regeringen har slagit fast att e-legitimationer är en samhällskritisk infrastruktur. [8] E-legitimationer och e-legitimationsutfärdare är därmed ett naturligt mål för brottslighet och antagonister som kan vilja komma åt enskilda personer eller samhället i stort. De mest kvalificerade antagonistiska hoten utgörs i första hand av angrepp utförda av statliga eller statsunderstödda aktörer. Effekterna av ett sådant angrepp kan få lika stora konsekvenser för samhällsviktiga funktioner och kritiska IT-system som ett konventionellt väpnat angrepp.[9]

Det försämrade omvärldsläget har också stor påverkan på riskbilden. Av Säkerhetspolisens (Säpo) lägesbild för 2022/2023 framgår att Rysslands anfallskrig mot Ukraina – i kombination med att även andra auktoritära stater agerar mer aggressivt – medför risker för Sveriges säkerhet. Detta ökar enligt Säpo betydelsen av samhällets motståndskraft och ett fungerande totalförsvar.[10] I takt med att olika samhällsfunktioner, ekonomiska värden och ytterst människors liv och hälsa knyts till sammankopplade system, bedömer Säpo att cyberangrepp riskerar att få allt värre konsekvenser.[11]

Digitaliseringen medför att de risker som finns behöver mötas av samhället och av den verksamhet som förlitar sig på dessa tjänster. Under 00-talet var i stor utsträckning digitala tjänster ett komplement till det vanliga pappersflödet. Då gick det även att gå tillbaka till ett pappersbaserat sätt att arbeta. Detta är i många fall inte möjligt i dag och andra former av kontinuitetslösningar krävs därmed.

Som ett steg i att hantera de risker som digitaliseringen medför tog regeringen under 2017 fram en nationell strategi för samhällets informations- och cybersäkerhet. Av strategin framgår bl.a. att varje aktör som bedriver skyddsvärd eller samhällsviktig verksamhet har ett ansvar att utifrån relevanta riskanalyser utveckla beredskaps- och kontinui-

[8] *För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi* (N2017/03643/D).
[9] Prop. 2020/21:30 s. 151.
[10] Säkerhetspolisen, *Säkerhetspolisens lägesbild 2022/2023*, s. 4 f.
[11] A.a. s. 36.

tetsplaner för att kunna hantera allvarliga cyberattacker eller andra IT-incidenter.[12]

6.5.2 Risker med den svenska marknaden för e-legitimationer

Som bl.a. framgår av avsnitt 4.4 har BankID en klart dominerande ställning på den svenska marknaden och den dominansen är än större när det gäller privata digitala tjänster i allmänhet och betalningsmarknaden i synnerhet.

Flera utredningar och rapporter har påpekat den sårbarhet och brist på konkurrens som finns inom e-legitimationsområdet genom att vi har gjort oss så beroende av BankID.[13] Ofta lyfts det fram att BankID fungerar bra, har nöjda kunder och har varit kostnadseffektivt, men samtidigt påpekas att den bristande konkurrensen medför risker.[14] Det är oklart om den föreslagna europeiska identitetsplånboken kommer att påverka konkurrensen på den nationella e-legitimationsmarknaden. Utifrån det läge som nu råder är det emellertid utan tvekan så att BankID:s dominans på den svenska marknaden medför risker. Vid sidan av risken för utanförskap för de individer som av någon anledning inte kan få eller klarar av att använda ett BankID drabbas av (se mer om detta i avsnitt 6.6), är bristen på redundans den största risken för samhället som helhet. Risken är kopplad till att såväl de som använder BankID som de som tillhandahåller digitala tjänster i hög utsträckning saknar alternativ för det fall BankID är otillgängligt eller av andra anledningar inte fungerar. Tillgängligheten till tjänsten kan t.ex. påverkas av en överbelastningsattack där någon angriper systemet genom att skicka så mycket trafik till en resurs att den blir otillgänglig. Något som är vanligt förekommande vad gäller både webbplatser och digitala tjänster. BankID:s tillgänglighet har vid ett flertal tillfällen påverkats av sådana attacker.[15]

Vi bedömer sammantaget att BankID:s dominanta position gör infrastrukturen till ett attraktivt mål för antagonistiska krafter, i synnerhet eftersom samhället i stort påverkas av avbrott om flera samhällssektorer drabbas samtidigt till följd av att BankID inte fungerar. Sårbarheten gäller inte minst betalningar och finansiella tjänster, men även

[12] *Nationell strategi för samhällets informations- och cybersäkerhet* (Skr. 2016/17:213), s. 22.
[13] *Vem kan man lita på*? (SOU 2021:9) s. 231 och *Staten och betalningarna* (SOU 2023:16) s. 375.
[14] Se exempelvis Riksrevisions rapport *E-legitimation – en underutnyttjad resurs* (RiR 2009:19).
[15] Se t.ex. www.svt.se/nyheter/inrikes/bank-id-ligger-nere-1 (hämtad 2023-04-02).

offentliga och kommersiella e-tjänster. Beroendet av BankID för samhällets funktionalitet medför också att tillhandahållandet av BankID är en verksamhet som kan behöva upprätthållas under höjd beredskap och krig.

6.5.3 En statlig e-legitimation leder till bättre beredskap och en ökad redundans

Som ovan framgått har problematiken med bristande konkurrens inom e-legitimationsområdet tidigare påtalats i såväl statliga utredningar som i myndighetsrapporter. Vissa lösningsförslag har också lagts fram genom åren. Exempelvis föreslog *E-delegationen* i sin strategi för myndigheternas arbete med e-förvaltning att det svenska systemet för e-legitimationer skulle baseras på federationslösningar för användning av befintlig och ny teknik i e-legitimationerna.[16] Vidare föreslog *Utredningen om bildande av en e-legitimationsnämnd* att det skulle införas en federerad e-legitimationslösning. Ett av skälen till den valda modellen var enligt utredningen att konkurrensen på marknaden och förutsättningarna för nya tjänster skulle öka.[17]

De förslag som har koppling till införandet av en statlig e-legitimation redovisas närmare i avsnitt 4.7. *Utredningen om effektiv styrning av nationella digitala tjänster* påtalade att en säker grundidentifieringsprocess genom en statlig e-legitimation kan användas av andra aktörer för att öka konkurrensen på marknaden. *2017 års ID-kortsutredning* framförde att det finns behov av alternativa e-legitimationslösningar utifrån flera perspektiv, särskilt när det gäller säkerhet, robusthet och tillgänglighet. Givet avsaknaden av ett reellt alternativ – om de privat utfärdade e-legitimationerna av någon anledning inte skulle fungera – ansåg utredningen att det behövdes en statlig e-legitimation.[18]

Betalningsutredningen bedömde att det är synnerligen angeläget att en statlig e-legitimation på högsta säkerhetsnivå införs så snart det är möjligt.[19] Utredningen konstaterade bl.a. att en statlig e-legitimation skulle stärka den civila beredskapen om den kan användas för att legitimera sig för att använda olika e-tjänster, inklusive betalningar. En statlig e-legitimation kan potentiellt också underlätta för andra

[16] *Strategi för myndigheternas arbete med e-förvaltning* (SOU 2009:86), s. 87.
[17] *E-legitimationsnämnden och Svensk e-legitimation* (SOU 2010:104), s. 150.
[18] *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14), s. 319 f.
[19] *Staten och betalningarna* (SOU 2023:16), s. 371.

aktörer att erbjuda e-legitimationer och betrodda tjänster, vilket också kan stärka beredskapen.[20] Utredningen poängterade emellertid även att hur utbredd en statlig e-legitimation blir delvis är upp till individerna och vilken nytta de ser med att skaffa en sådan.[21]

Det anförda motiverar bedömningen att det finns ett behov av alternativ till BankID. Den marknadsdominans som BankID har, i kombination med den låga andel av befolkningen som har två e-legitimationer medför i praktiken att aktörer som förlitar sig på e-legitimationer får anses sakna alternativ för att hantera risker och för att upprätthålla en fungerande kontinuitetsplan.

Förutsättningarna för att hantera de risker som framgår ovan skulle således öka om minst ett alternativ, med stor spridning i samhället och motsvarande användningsområden som BankID har, fanns tillgängligt. Detta kan uppnås antingen genom att befintliga alternativ får större spridning eller genom att ytterligare leverantörer etablerar sig på marknaden och tar betydande marknadsandelar.

En ökad etablering kan uppnås genom att staten utför grundidentifiering, vilket underlättar för marknaden som i sin tur kan använda uppgifterna för att utfärda e-legitimationer. Alternativt kan det uppnås genom att staten tillhandahåller en e-legitimation som, vid sidan av kommersiella e-legitimationer, får en hög användningsvolym. Slutligen kan en ökad spridning uppnås om befintliga tjänster accepterar olika e-legitimationer, inte minst inom finansiella- och betaltjänster där BankID har en än mer dominerande ställning. För att en statlig eller annan privat e-legitimation ska kunna bli ett reellt alternativ krävs under alla förhållanden att staten skapar vissa förutsättningar för att så ska kunna ske (se mer om detta i avsnitt 7.13).

Det finns i sammanhanget också skäl att betona att de kommersiella alternativen självfallet drivs av ett underliggande vinstintresse. De ekonomiska förutsättningarna på marknaden styr således om och hur många privata aktörer som tillhandahåller e-legitimationer. Ett syfte för staten med att tillhandahålla en e-legitimation kan således sägas vara att stå som garant för att det finns ett alternativ att tillgå om det skulle ske förändringar på den svenska e-legitimationsmarknaden till följd av exempelvis ändrade kommersiella villkor.

Sammanfattningsvis utgör införandet av en statlig e-legitimation inte ensamt lösningen på de risker som presenteras ovan. Det finns

[20] A.a. s. 376.
[21] A.a. s. 374.

emellertid behov av en statlig e-legitimation som en del i att bättre kunna hantera dessa risker och för att garantera att det finns en svensk e-legitimation som utfärdas till privatpersoner utan beaktande av rådande kommersiella villkor.

6.6 Ökad tillgänglighet

6.6.1 Tillgång till e-legitimation är en förutsättning för delaktighet

Den rådande samhällsutvecklingen drivs i flera avseenden av digitaliseringen och det blir allt viktigare att kunna legitimera sig elektroniskt för att ta del av samhällets alla funktioner. Tillgång till en e-legitimation erbjuder inte bara åtkomst till digitala tjänster hos exempelvis statliga myndigheter, kommuner och banker. Den kan också skapa förutsättningar för att förenkla vardagen, eller till och med vara nödvändig, vid köp av buss- eller tågbiljetter samt vid inköp på fysiska eller internetbaserade marknadsplatser. Vidare krävs inte sällan en e-legitimation för att kunna delta i det sociala samspelet på internet. Att stå helt utanför eller begränsas i sin användning på olika sätt innebär således konsekvenser för enskilda människors vardagliga liv och ekonomi samt därmed också för jämlikheten i samhället.

Det finns ingen legaldefinition av vad som avses med tillgänglighet. Betydelsen av tillgänglighet i vardagligt språkbruk är förhållandevis klar och den mer specifika innebörden framgår, när det finns behov, av den lagstiftning där begreppet förekommer. För vår del finns det dock – på ett mer generellt plan – anledning att påpeka att målsättningen med ökad tillgänglighet till en e-legitimation inte bara inbegriper möjligheten att skaffa en sådan utan också att det ska vara möjligt för alla att använda den.

6.6.2 Alla har inte förutsättningar och möjlighet att delta

En majoritet av befolkningen är delaktiga och aktiva i det digitala samhället. I en studie som Internetstiftelsen årligen genomför redovisas för 2022 att 94 procent av befolkningen 16 år eller äldre använder internet och att 91 procent i samma grupp använder e-legitimation.[22] I allt

[22] Internetstiftelsen, *Svenskarna och internet 2022*, s. 12 ff.

väsentligt motsvarande statistik finns att läsa på Statistiska centralbyråns webbplats.[23] Den digitala närvaron och användandet av e-legitimation är alltså betydande. Statistiken innebär emellertid också att ett stort antal människor ännu inte har tillgång till en e-legitimation, vilket orsakar ett betydande utanförskap.

Något förenklat kan sägas att äldre personer, personer med funktionsnedsättning och personer utan svenskt personnummer inte har tillgång till en e-legitimation i samma utsträckning som den övriga befolkningen.

I gruppen äldre personer uppger 3 av 10 pensionärer att de inte använt e-legitimation det senaste året och för 1920- och 30-talisterna är siffran 6 av 10.[24] När det gäller personer med funktionsnedsättning svarar endast 57 procent att de känner sig delaktiga i det digitala samhället, 33 procent att de känner sig delaktiga till viss del, 8 procent att de inte känner sig delaktiga alls och 2 procent att de inte vet. I samma grupp uppger 80 procent att de använder Mobilt BankID och 16 procent att de använder en e-legitimation som inte är Mobilt BankID.[25] I förhållande till befolkningen i övrigt är således utanförskapet för dessa grupper betydande.

Enskilda personer som inte är folkbokförda eller har varit folkbokförda i Sverige tilldelas inte personnummer, men kan under vissa förutsättningar tilldelas ett samordningsnummer. Detta gäller exempelvis personer som arbetar eller studerar tillfälligt i Sverige eller söker asyl i landet. Formellt sett finns det inget som hindrar att en person med samordningsnummer får tillgång till en e-legitimation, men för det fall e-legitimationen omfattas av det svenska tillitsramverket måste utfärdaren kunna visa för Digg att personen har identifierats på ett säkert sätt vid ansökan. I tillitsramverket ställs krav på att en svensk e-legitimation endast får ges ut till personer med samordningsnummer som har styrkt sin identitet eller gjort identiteten sannolik. Till följd av svårigheter med att identifiera personer med samordningsnummer krävs det för närvarande i praktiken oftast ett personnummer. Under hösten 2023 kommer emellertid Freja+ att börja utfärdas till

[23] www.scb.se/hitta-statistik/statistik-efter-amne/levnadsforhallanden/levnadsforhallanden/befolkningens-it-anvandning/pong/statistiknyhet/befolkningens-it-anvandning-2022/ (hämtad 2023-10-02).
[24] Internetstiftelsen, *Svenskarna och internet 2022*, s. 18.
[25] www.datavisning.se/#/stats/Anv%C3%A4ndning%20av%20internet%20SMFOI%202021 (hämtad 2023-10-02).

personer med samordningsnummer med styrkt identitet förutsatt att dessa har ett hemlandspass som är utfärdat inom EU eller EES.[26]

Någon tillförlitlig statistik på hur många personer med samordningsnummer som använder en svensk e-legitimation finns såvitt känt för utredningen inte – sannolikt eftersom det inte förekommer i någon nämnvärd utsträckning.[27] Bilden av ett digitalt utanförskap för exempelvis asylsökande och andra nyanlända bekräftas dock bl.a. i länsstyrelsernas rapporter och Betalningsutredningens betänkande.[28]

Avsaknad av personnummer kan skapa utanförskap även för unionsmedlemmar som exempelvis arbetar eller studerar i Sverige. Sverige har återkommande fått kritik för de hinder för den fria rörligheten som de ofta förekommande kraven på personnummer skapar.[29] Mot bakgrund av klagomålen startade EU-kommissionen ett s.k. EU-pilotärende och ställde ett antal frågor till svenska myndigheter.[30] Efter att ha avslutat ärendet i mars 2021 konstaterade kommissionen att problemen ännu är olösta och att den avser återkomma om vidare hantering av frågan.[31] Inom ramen för ett annat EU-pilotärende har kommissionen även ställt liknande frågor rörande tredjelandsmedborgare.[32]

Utöver det som redovisats ovan indikerar resultatet av en pilotstudie genomförd av Linköpings universitet att tillgång till e-legitimation kan vara begränsad i vissa områden. Pilotstudien genomfördes i förorten Skäggetorp under november månad 2019 med intervjuförfarande vid dörrknackning samt på verksamheter och offentliga platser. Motivet till studien var att invånare i förorter i lägre utsträckning deltar i enkätstudier, särskilt sådana som genomförs digitalt. Enligt studien uppgav 87 procent av respondenterna att de använder internet (jämfört med 94 procent i undersökningen Svenskarna och Internet 2019[33]) och 86 procent av dessa att de även använder BankID någon

[26] Freja eID Group AB, Pressmeddelande *Nya regler möjliggör fler användare och kunder för Freja*, 2023-08-31.
[27] Problematiken beskrivs i prop. 2021/22:276, s. 28 f. där det också framhålls att det för närvarande saknas möjlighet att koppla en utländsk e-legitimation till ett svenskt samordningsnummer.
[28] Länsstyrelserna, *Bevakning av grundläggande betaltjänster 2022*, se exempelvis s. 5, 68 f. och s. 126 och *Staten och betalningarna* (SOU 2023:16), s. 180 f. och 186.
[29] Se bl.a. Europaparlamentet, Generaldirektoratet för intern politik, Hinder för rätten att fritt röra sig och att fritt uppehålla sig för unionsmedborgare och deras familjer: Landsrapport för Sverige, juni 2016, s. 15 ff. och Skatteverket, Regler och rutiner i folkbokföringsärenden(dnr 2 04 319440-17/113, 26 februari 2018, s. 8 f.
[30] Fi2016/03726/S3.
[31] EUP[2016]8967.
[32] Fi2019/03178/S3.
[33] Internetstiftelsen, *Svenskarna och internet 2019*, ibid.

gång.[34] Andelen respondenter som använder BankID sammanfaller alltså med andelen som använder internet varför utanförskapet när det gäller e-legitimation synes vara förknippat med avsaknad av tillgång till internet.

6.6.3 Orsakerna till avsaknad av e-legitimation är flera

Det finns flera orsaker till det digitala utanförskapet och vissa gruppers bristande tillgång till e-legitimation. Det kan dels ha att göra med befintliga utfärdares krav för att få en e-legitimation, dels vara kopplat till individens egna förutsättningar. För en del personer, särskilt bland gruppen äldre personer, gäller också att det inte finns någon önskan om att använda digitala hjälpmedel.

I en forskningsöversikt som genomfördes av Linköpings universitet på uppdrag av Digitaliseringsrådet identifierades den samhälleliga styrningen som en grogrund för digital inkludering medan infrastruktur/tillgång, socioekonomisk status, motivation, tillit/självtillit samt kunskaper och färdigheter angavs som bidragande faktorer till digitalt utanförskap kopplade till individen. Dessa faktorer kan i varierande mån gälla för alla grupper som står utan e-legitimation eftersom grupperna inte på något sätt är homogena. Därtill kommer att de undersökningar som genomförs för att ta fram statistik många gånger är utformade på ett sätt som exkluderar vissa grupper, exempelvis på grund av att de förutsätter att respondenten kan använda telefon och dator samt behärskar svenska språket.[35]

I dag finns det som redovisats i avsnitt 4.4 tre statligt godkända e-legitimationer som privatpersoner kan skaffa. BankID som utfärdas av tio olika banker, Freja+ som ges ut av Freja eID Group AB och den e-legitimation som utfärdas av AB Svenska Pass och som finns på Skatteverkets identitetskort. Som beskrivs i avsnitt 4.4 krävs för att kunna få ett BankID ett svenskt personnummer och ett konto i någon av de banker som utfärdar BankID. För Freja+ krävs för närvarande att sökanden förekommer i folkbokföringsregistret och kan legitimera sig med en svensk ID-handling. Freja har emellertid

[34] *Förorten svarar. En enkätmetod för att kartlägga digital delaktighet och hållbarhet i Skäggetorp*, Skill och Kaharevic, Linköping: Linköping University Electronic Press, 2021, s. 108, DINO Rapport 2021:7.
[35] *Digitalt utanförskap – en forskningsöversikt*, Francisco m.fl., Linköping: Linköping University Electronic Press, 2019, s. 51, DINO Rapport 2019:3.

nyligen aviserat att de under hösten 2023 kommer att utfärda Freja+ till personer med samordningsnummer med styrkt identitet förutsatt att dessa har ett hemlandspass som är utfärdat inom EU eller EES. För e-legitimationen på Skatteverkets identitetskort krävs att man är folkbokförd i Sverige, har fyllt 13 år och kan legitimera sig. Detta är krav som i varierande mån inte kan uppfyllas av de grupper som i dag saknar e-legitimation.

Gemensamt för många – men givetvis inte alla – som saknar tillgång till en e-legitimation är att de har behov av hjälp av en god man eller förvaltare. Ställföreträdarutredningen, som redovisade sitt betänkande i april 2021, hade bl.a. som uppdrag att dels ta ställning till vilka ändringar som behövs för att aktörerna på området i så stor utsträckning som möjligt ska kunna använda sig av digitala hjälpmedel, dels överväga om och hur framtidsfullmakter ska kunna upprättas och hanteras elektroniskt.[36]

Ställföreträdarutredningen konstaterade att banker och andra utställare av e-legitimationer inte medger en e-legitimation när en sådan bedöms innebära säkerhetsrisker eller när användaren inte kan ge uttryck för sin vilja eller förstå vad en e-legitimation innebär. Vidare fann utredningen att banker, myndigheter och andra som tillhandahåller digitala tjänster ibland ser säkerhetsrisker med att erbjuda sådana tjänster till huvudmän, såsom en risk att tjänsten används av andra till skada för huvudmannen eller att rättshandlingar som huvudmannen ingår med hjälp av tjänsten inte blir bindande, till skada för tredje man.[37]

Utanförskapet för personer med god man och förvaltare till följd av bristande tillgång på e-legitimation bekräftas av flera av de intresseorganisationer och offentliga aktörer som utredningen har talat med. Därtill kommer att de tjänster som erbjuds inte fullt ut är anpassade för olika behov och inte heller erbjuder någon tillgänglig supportfunktion. Detta är omständigheter som i sig får en avhållande effekt eftersom de bidrar till en osäkerhet i användningsskedet.

Sammanfattningsvis står det klart att de lösningar som erbjuds i dag inte fullt ut tillgodoser behovet av att kunna legitimera sig elektroniskt för alla i samhället.

[36] *Gode män och förvaltare – en översyn* (SOU 2021:36).
[37] A.a. s. 451 ff.

6.6.4 Bestämmelser om tillgänglighet

Utöver att ökad tillgänglighet är ett uttalat syfte i våra direktiv finns det även olika bestämmelser som uppställer krav om tillgänglighet både i allmänhet och mer specifikt vad gäller digitala tjänster. Dessa bestämmelser tar främst sikte på bristande tillgänglighet till följd av funktionsnedsättning.

Regeringsformen

Enligt 1 kap. 2 § första stycket regeringsformen ska den offentliga makten utövas med respekt för alla människors lika värde och för den enskilda människans frihet och värdighet. Vidare ska det allmänna enligt femte stycket samma paragraf dels verka för att alla människor ska kunna uppnå delaktighet och jämlikhet i samhället och för att barns rätt tas till vara, dels motverka diskriminering av människor på grund av kön, hudfärg, nationellt eller etniskt ursprung, språklig eller religiös tillhörighet, funktionshinder, sexuell läggning, ålder eller andra omständigheter som gäller den enskilde som person. Bestämmelserna i paragrafen brukar betraktas som program- och målsättningsstadganden som ger uttryck för vissa särskilt viktiga mål eller riktlinjer för den samhälleliga verksamheten. Den riktar sig till alla som utövar offentlig makt, dvs. både normgivande organ och rättstillämpande myndigheter. Stadgandet ger däremot inte upphov till några rättigheter för den enskilde på samma sätt som t.ex. bestämmelserna om de grundläggande fri- och rättigheterna i 2 kap. regeringsformen.

FN-konventionen om rättigheter för personer med funktionsnedsättning

FN:s konvention om rättigheter för personer med funktionsnedsättning och dess fakultativa protokoll antogs 2006. Sverige ratificerade konventionen och dess fakultativa protokoll 2008. Konventionen skapar inte i sig några nya rättigheter utan tydliggör mänskliga rättigheter i relation till personer med funktionsnedsättning. Dess syfte är att säkerställa att personer med funktionsnedsättning kan åtnjuta sina mänskliga rättigheter.

Enligt artikel 9.1 i konventionen ska konventionsstaterna vidta ändamålsenliga åtgärder för att säkerställa att personer med funktionsnedsättning, på lika villkor som andra, får tillgång till den fysiska miljö, transporter, information och kommunikation, innefattande informations och kommunikationsteknik och system, samt till andra anläggningar och tjänster som är tillgängliga för eller erbjuds allmänheten både i städerna och på landsbygden. Dessa åtgärder, som ska innefatta identifiering och undanröjande av hinder och barriärer mot tillgänglighet, ska bl.a. avse information, kommunikation och annan service, däribland elektronisk service och service i nödsituationer.

Av artikel 9.2 följer att konventionsstaterna även ska vidta ändamålsenliga åtgärder för att bl.a. främja personers med funktionsnedsättning tillgång till ny informations- och kommunikationsteknik och nya system, däribland internet, samt främja utformning, utveckling, tillverkning och distribution av tillgänglig informations- och kommunikationsteknologi och system på ett tidigt stadium, så att dessa blir tillgängliga till lägsta möjliga kostnad.

Förordning om de statliga myndigheternas ansvar för genomförande av funktionshinderspolitiken

Enligt 1 § första stycket förordningen (2001:526) om de statliga myndigheternas ansvar för genomförande av funktionshinderspolitiken ska myndigheter under regeringen utforma och bedriva sin verksamhet med beaktande av de funktionshinderspolitiska målen. Av 1 § andra stycket i förordningen framgår att myndigheterna ska verka för att personer med funktionsnedsättning ges full delaktighet i samhällslivet och jämlikhet i levnadsvillkor. Myndigheterna ska vidare särskilt verka för att deras lokaler, verksamhet och information är tillgängliga för personer med funktionsnedsättning. I detta arbete ska konventionen om rättigheter för personer med funktionsnedsättning vara vägledande. Av 2 § samma förordning följer att myndigheterna ska genomföra inventeringar och utarbeta handlingsplaner i arbetet med att göra myndigheternas lokaler, verksamhet och information mer tillgängliga för personer med funktionsnedsättning.

Diskrimineringslagen

Bristande tillgänglighet är en form av diskriminering enligt diskrimineringslagen (2008:567). Med bristande tillgänglighet avses enligt 1 kap. 4 § 3 diskrimineringslagen att en person med en funktionsnedsättning missgynnas genom att sådana åtgärder för tillgänglighet inte har vidtagits för att den personen ska komma i en jämförbar situation med personer utan denna funktionsnedsättning. Av bestämmelsen framgår att de åtgärder för tillgänglighet ska vidtas som är skäliga utifrån krav på tillgänglighet i lag och annan författning, och med hänsyn till de ekonomiska och praktiska förutsättningarna, varaktigheten och omfattningen av förhållandet eller kontakten mellan verksamhetsutövaren och den enskilde samt andra omständigheter av betydelse.

Förbud mot diskriminering i form av bristande tillgänglighet gäller enligt 2 kap. diskrimineringslagen inom samhällsområdena arbetsliv, utbildning, arbetsmarknadspolitisk verksamhet och arbetsförmedling utan offentligt uppdrag, start eller bedrivande av näringsverksamhet, yrkesbehörighet, medlemskap i vissa organisationer, tillhandahållande av varor och tjänster, allmän sammankomst, offentlig tillställning, hälso- och sjukvård, socialtjänst, socialförsäkring, arbetslöshetsförsäkring, statligt studiestöd, värn- och civilplikt samt offentlig anställning.

Lagen om tillgänglighet till digital offentlig service

Lagen (2018:1937) om tillgänglighet till digital offentlig service innebär att tjänster och information som en offentlig aktör tillhandahåller genom en webbplats eller mobilapplikation ska vara tillgänglig. Enligt lagen ska digital service som tillhandahålls av en offentlig aktör genom en teknisk lösning som står under aktörens kontroll vara tillgänglig i enlighet med tillgänglighetskraven i föreskrifter som har meddelats med stöd av lagen. Därutöver ska även digital service som tillhandahålls av en offentlig aktör genom en teknisk lösning som står under tredje parts kontroll, så långt det är möjligt, uppfylla samma krav. Sådan digital service ska uppfylla kraven att vara möjlig att uppfatta, hanterbar, begriplig och robust. Genom att följa en särskild europeisk standard (EN 301 549 V2.1.2), som i sin tur bygger på WCAG 2.1, kan webbplatser och mobila applikationer leva upp till kraven.

Lagen om vissa produkters och tjänsters tillgänglighet

EU:s tillgänglighetsdirektiv trädde i kraft 2019 och syftar till att skapa gemensamma regler vad gäller tillgänglighetskrav för vissa produkter och tjänster.[38] Produkter och tjänster som släpps på marknaden ska uppfylla direktivets krav senast i juni 2025.[39]

Direktivet genomfördes i Sverige genom lagen (2023:254) om vissa produkters och tjänsters tillgänglighet.[40] Lagen träder i kraft den 28 juni 2025 och innebär att vissa produkter och tjänster ska uppfylla vissa krav på tillgänglighet.

De produkter som omfattas av lagen är datormaskinvarusystem med generella användningsområden, terminalutrustning med interaktiv datorkapacitet som används vid elektronisk kommunikation eller för åtkomst till audiovisuella medietjänster, läsplattor och självbetjäningsautomater. De tjänster som omfattas är tjänster som tillhandahålls konsumenter och avser elektroniska kommunikationstjänster, e-handelstjänster, banktjänster, e-böcker, tjänster som ger åtkomst till audiovisuella medietjänster samt vissa passagerartransporttjänster. Lagen innehåller bestämmelser om CE-märkning, marknadskontroll och tillsyn samt syftar till att undanröja hinder på den inre marknaden genom att öka tillgängligheten till produkter och tjänster, framför allt för personer med funktionsnedsättning.

Flera av de produkter, men framför allt tjänster, som omfattas av bestämmelserna i den nya lagen kan enligt vår bedömning förväntas förutsätta att användaren har tillgång till en e-legitimation. En utökad möjlighet att få tillgång till en e-legitimation kommer således vara en förutsättning för att möta kommande krav.

6.6.5 Förslag under beredning m.m.

I takt med att samhället blir alltmer digitaliserat utkristalliseras nya behov som på sikt kan tänkas förutsätta att det finns en möjlighet att legitimera sig elektroniskt och därigenom, i vart fall i praktiken, kan sägas medföra ett krav på tillgång till en e-legitimation. Nedan redovisas förslag som är under beredning samt utredningsdirektiv som lämnats

[38] Europaparlamentets och rådets direktiv (EU) 2019/882 av den 17 april 2019 om tillgänglighetskrav för produkter och tjänster.
[39] Bilaga 1 till direktivet, avsnitt IV e.
[40] Prop. 2022/23:42.

till en pågående utredning som kan få relevans för ett ökat behov av tillgång till en e-legitimation.

Moderna och rättssäkra regler på ställföreträdarområdet

Ställföreträdarutredningen framhöll i sitt betänkande att den digitalisering som sker i samhället i många fall medför ett utanförskap för personer som har en god man eller förvaltare. Vidare att det är angeläget för huvudmän att de kan få tillgång till digitala tjänster, anpassade efter eventuella inskränkningar i rättshandlingsförmåga, funktionsnedsättningar eller annan problematik för att öka deras möjligheter att delta i samhällslivet. Utredningen ansåg det vara positivt att en statlig e-legitimation införs och konstaterade att anpassade digitala tjänster för de som har en god man eller förvaltare är helt i linje med kraven i EU:s tillgänglighetsdirektiv och FN:s funktionsrättskonvention.[41] Utredningens förslag bereds i Regeringskansliet.

Eventuell skyldighet att använda digital post

Regeringen beslutade i oktober 2020 att ge en särskild utredare i uppdrag att utreda möjliga finansieringsmodeller för den samhällsomfattande posttjänsten.[42] I januari 2023 utvidgades utredarens uppdrag och utredaren ska nu enligt tilläggsdirektiven[43] bl.a.

– utreda förutsättningarna för att införa en skyldighet för privatpersoner, enskilda näringsidkare och juridiska personer att ansluta sig till en digital brevlåda för att kunna ta emot säkra elektroniska försändelser från myndigheter,
– utreda hur ett undantag för privatpersoner som inte har förutsättningar att använda en digital brevlåda kan utformas.

Enligt tilläggsdirektivet ska de tillkommande delarna av uppdraget redovisas den 14 juni 2024. Ett kommande förslag kan således, beroende på utformningen av obligatoriet och eventuella undantag, komma att i sin tur innebära ett krav på att inneha en e-legitimation.

[41] *Gode män och förvaltare – en översyn* (SOU 2021:36), s. 451.
[42] Dir. 2020:101.
[43] Dir. 2023:7.

Digitalisering av rättsligt samarbete mellan EU:s medlemsstater

Den 1 december 2021 presenterade kommissionen ett förslag till förordning om digitalisering av rättsligt samarbete och tillgång till rättslig prövning i gränsöverskridande civilrättsliga, handelsrättsliga och straffrättsliga frågor samt ett direktiv med förslag till vissa följdändringar i rättsakter som omfattas av förordningsförslaget. Förslagen innebär bl.a. att fysiska och juridiska personer ska få möjlighet att dels kommunicera med behöriga myndigheter elektroniskt, dels inleda rättsliga förfaranden digitalt via en europeisk åtkomstpunkt på e-juridikportalen. Förordningen innehåller även bestämmelser om användning av videokonferensteknik, elektroniska dokument, elektroniska underskrifter och elektroniska stämplar samt elektronisk betalning av avgifter.[44] I juni 2023 ingicks en provisorisk överenskommelse gällande förslag till två EU-lagar om digitalisering av rättsligt samarbete mellan EU:s medlemsstater. De nya reglerna förväntas underlätta gränsöverskridande rättsliga förfaranden.

6.7 Bedrägerier och annan identitetsrelaterad brottslighet

Det finns många fördelar med ett alltmer digitaliserat samhälle, men en tydlig baksida är den identitetsrelaterade brottslighet som begås med användning av falska eller olovligt åtkomna identitetshandlingar. Det rör sig främst om olika typer av bedrägeribrottslighet, men i förlängningen även annan ekonomisk brottslighet, såsom exempelvis penningtvätts- och bidragsbrottslighet. Brotten begås till stor del med användande av fysiska identitetshandlingar, men i dag används även digitala identitetshandlingar i stor utsträckning för att begå olika typer av brott.

I en myndighetsgemensam rapport om organiserad brottslighet från 2023 beskrivs BankID som en ”dörröppnare för kriminella aktörer”. Enligt rapporten kan kriminella aktörer som förfogar över och kontrollerar ett större antal BankID med tillhörande konton enkelt och relativt riskfritt begå brott i den utnyttjade identitetens namn och därefter förflytta brottsvinsterna mellan andra utnyttjade identiteter.[45]

[44] Regeringskansliet Faktapromemoria 2021/22:FPM40.
[45] Polismyndigheten, Nationella operativa avdelningen, *Myndighetsgemensam lägesbild, Organiserad brottslighet 2023*, juni 2023,, s. 20.

Äldre personer, personer med funktionsnedsättning och socialt utsatta personer tillhör de grupper som utnyttjas och drabbas av den identitetsrelaterade brottsligheten i särskilt stor omfattning. Utan rätt åtgärder riskerar en ökad tillgång till elektronisk identifiering för dessa grupper att bli en möjliggörare för identitetsrelaterad brottslighet.

6.7.1 Digitaliseringen har skapat nya möjligheter även för brottsligheten

Vid många bedrägerier är det ett centralt moment att utge sig för att vara någon annan. Gärningspersonen kan utge sig för att vara en person som inte existerar alls eller använda någon annans identitetsuppgifter olovligen. Det senare handlandet är sedan 2016 kriminaliserat genom bestämmelsen om olovlig identitetsanvändning i 4 kap. 6 b § brottsbalken. Det förekommer också att en person lånar ut sina identitetsuppgifter och på så sätt fungerar som en s.k. målvakt.

Brottsförebyggande rådet (Brå) framhöll i en rapport från 2016 att det fanns indikationer på att användningen av stulna och falska identiteter ökar i Sverige och att det inte sällan har kopplingar till organiserad brottslighet. Enligt rapporten var bakgrunden till det då ökade missbruket av identiteter den tekniska utvecklingen med ökat internetanvändande, i kombination med att enskildas personuppgifter är lättillgängliga för allmänheten i Sverige. Brå konstaterade vidare att det stora antalet godkända identitetshandlingar i Sverige[46] medför att det är svårare att kontrollera handlingarna och enklare att förfalska dem, samt att det är enkelt att kartlägga en person på internet.

Ytterligare omständigheter som angavs ha betydelse för utvecklingen var ändrade köp- och betalningsvanor som innebär att köp samt beviljande av lån och betalningar ofta sker utan direkt fysisk kontakt.[47]

De brottsbekämpande myndigheter som utredningen talat med har framfört att problematiken kvarstår och att motsvarande gäller även för möjligheten att starta nya bolag, eftersom det inte alltid sker

[46] 2017 års ID-kortsutredning har bedömt att antalet fysiska identitetshandlingar bör begränsas och föreslog i sitt betänkande att ett statligt identitetskort och pass ska vara de enda fysiska identitetshandlingar som staten utfärdar, *Ett säkert statligt ID-kort – med e-legitimation (*SOU 2019:14). Förslagen i betänkandet bereds i Regeringskansliet.
[47] Brå, *Bedrägeribrottsligheten i Sverige, Kartläggning och åtgärdsförslag,* (Rapport 2016:9), mars 2016, s. 148 f.

någon direkt fysisk kontakt eller grundligare identitetskontroll från Bolagsverkets sida.[48]

6.7.2 Olika typer av bedrägeribrottslighet

Brå ger årligen ut en publikation med anvisningar och regler för klassificering av brott. I publikationen redovisar Brå ett antal huvudkategorier av bedrägeribrott nämligen; bedrägeri genom social manipulation, identitetsbedrägeri, fakturabedrägeri och kortbedrägeri, annonsbedrägeri, försäkringsbedrägeri, snyltningsbrott, grovt fordringsbedrägeri och övriga. [49]

Enligt Brå:s bedömning kan någon form av identitetsmissbruk förekomma i samband med samtliga bedrägerikategorier, men enbart vid kreditbedrägerier är identitetsmissbruk mer eller mindre en förutsättning för brottet.[50]

Nedan presenteras de huvudkategorier som enligt utredningens bedömning är mest relevanta i relation till användning av e-legitimation.

Bedrägeri genom social manipulation

Bedrägeri genom social manipulation innefattar bl.a. undergrupperna befogenhetsbedrägeri, investeringsbedrägeri och romansbedrägeri.

Befogenhetsbedrägeri består i att gärningspersonen kontaktar ett tilltänkt brottsoffer och förmår denne att agera eller inte agera genom att utnyttja en förtroenderelation. Gärningspersonen utger sig för att ha vissa befogenheter, till exempel i egenskap av banktjänsteman, och lurar den utsatte att ge ut lösenord eller kontouppgifter alternativt att förmå någon att godkänna överföringar med sin e-legitimation. Till denna grupp hänförs även så kallade VD-Bedrägerier och telefonbedrägeri (s.k. vishing).

Investeringsbedrägeri begås genom att gärningspersonen förmår brottsoffret, under förevändningen att det exempelvis är en investering i ädla metaller eller kryptovalutor, köper något som inte existerar.

[48] Utredningen om bolaget som brottsverktyg (SOU 2023:32) lämnade i juni 2023 förslag som bl.a. syftar till att motverka att bolag används som brottsverktyg, exempelvis förslag om utökade kontroller och möjlighet att förelägga om personlig inställelse.
[49] Brå, *Klassificering av brott, Anvisningar och regler,* version 11, januari 2023, s. 64.
[50] Brå, *Bedrägeribrottsligheten i Sverige, Kartläggning och åtgärdsförslag,* (Rapport 2016:9), mars 2016, s. 152.

Brotten genomförs med hjälp av olika online-baserade hjälpmedel och mobiltelefoner. Som regel är denna typ av brottslighet gränsöverskridande till sin karaktär.

Romansbedrägeri består i att gärningspersonen inleder en kärleksrelation eller liknande relation med en person, genom fysisk kontakt eller via internet, i syfte att vilseleda personen till handling som innebär ekonomisk vinning för gärningspersonen, exempelvis genom att förmå personen att låna ut eller skänka pengar till gärningspersonen.

Identitetsbedrägeri/kreditbedrägeri

Identitetsbedrägeri (identitetsstöld) eller kreditbedrägeri innebär att en obehörig person stjäl eller på annat sätt kommer över någons personliga uppgifter och använder dem för sin egen ekonomiska vinning. Det kan handla om att gärningspersonen olovligen köper en vara eller tjänst eller tar ett lån med den utsattes identitet. Även bolag kan användas som låntagare och sedan försättas i konkurs.

Fakturabedrägeri och kortbedrägeri

Fakturabedrägeri begås genom att gärningspersonen vilseleder en person eller ett företag att betala en faktura för en vara eller en tjänst som personen/företaget inte har beställt. Vid kortbedrägeri använder gärningspersonen någon annans fysiska bank-, betal- eller kreditkort för att olovligen genomföra köp av en vara eller tjänst, alternativt göra uttag av kontanter.

Annonsbedrägeri

Gärningspersonen vilseleder en intresserad köpare genom att via en annons erbjuda en vara eller tjänst till försäljning eller uthyrning. Efter att betalning ägt rum har leveransen uteblivit helt eller så har en falsk/-felaktig vara levererats. Ett annonsbedrägeri kan även ske genom att gärningspersonen agerar som en intresserad köpare till det som erbjuds via annons, i syfte att komma över pengar från säljaren eller det som erbjuds via annonsen utan att erhålla betalning till säljaren.

Kopplingen mellan användning av e-legitimation och denna typ av bedrägeri är inte lika självklar som för övriga redovisade. Marknadsplatser på internet såsom exempelvis Tradera och Blocket kräver dock identifiering via Bank-ID som en säkerhetsåtgärd. I förlängningen kan tillgång till annans eller förfalskad e-legitimation således skapa möjlighet att begå brott även vid annonsbedrägeri.

6.7.3 Äldre och personer med funktionsnedsättning är särskilt utsatta för befogenhetsbedrägerier

Under 2022 anmäldes 195 929 bedrägeribrott, vilket var ett i princip oförändrat antal jämfört med 2021. I förhållande till 2019, det första året som Brå har redovisat statistik enligt aktuell uppdelning av brottskategorier, har det skett en minskning om 20 procent. Det är såklart en försiktigt positiv trend men vad som är mer bekymmersamt är att bedrägeribrottsligheten mot äldre och personer med funktionsnedsättning inte följer den utvecklingen. Visserligen har identitetsbedrägerierna mot dessa minskat med 45 procent sedan 2019 men befogenhetsbedrägerierna har i stället ökat med anmärkningsvärda 314 procent under samma tidsperiod. Mellan 2021 och 2022 skedde nästan en fördubbling av antalet anmälda brott i kategorin.[51]

Tabellen nedan illustrerar förändringen i antalet anmälda brott såvitt avser den bedrägeribrottslighet som har koppling till e-legitimationsområdet. Äldre och personer med funktionsnedsättningar är som tidigare redovisats en grupp som i stor utsträckning saknar e-legitimation. Som framgår av tabellen är dessa grupper redan i dag särskilt utsatta för vissa typer av bedrägeribrottslighet. Det kan således förväntas finnas ett omfattande behov av åtgärder för att dessa grupper ska kunna inkluderas på ett säkert sätt.

[51] bra.se/statistik/kriminalstatistik/anmalda-brott.html (hämtad 2023-10-02).

Tabell 6.1 Bedrägeribrottslighet mellan 2019–2022

Antal anmälda brott

Brottstyp	2019	2020	2021	2022	2019–2022, procentuell förändring
Bedrägerier eller annan oredlighet, totalt	244 696	218 308	195 902	195 929	-20
Romansbedrägeri, totalt	993	1 058	1 162	1 312	+32
Romansbedrägeri, äldre eller funktionsnedsatt	337	257	323	457	+35
Investeringsbedrägeri, totalt	1 642	1 643	1 899	2 566	+56
Investeringsbedrägeri, äldre eller funktionsnedsatt	606	474	495	786	+30
Befogenhetsbedrägeri, totalt	3 600	4 676	6 282	10 722	+197
Befogenhetsbedrägeri, äldre eller funktionsnedsatt	1 970	2 660	4 309	8 153	+314
Identitetsbedrägeri, totalt	27 299	27 901	21 836	15 041	-45
Identitetsbedrägeri, äldre eller funktionsnedsatt	3 593	3 381	3 312	2 432	-32
Kortbedrägeri, totalt	129 087	97 197	66 477	71 559	-45
Kortbedrägeri (fysiskt kort), totalt	22 303	16 665	13 858	13 546	-40
Kortbedrägeri (fysiskt kort), äldre eller funktionsnedsatt	4 018	3 261	3 704	2 813	-30

Källa: Brå.

6.7.4 Bedrägeribrottsligheten och penningtvätt

Polismyndighetens finanspolissektion (Finanspolisen) presenterade 2022 en rapport med syftet att ge en bild av penningtvätt kopplat till olika typer av bedrägerier och bedöma hotet från bedrägerierna ur ett brottsvinstperspektiv.[52] Enligt rapporten ägnar sig multikriminella aktörer åt ifrågavarande brottslighet och risken är stor att bedrägerivinsterna återinvesteras i annan allvarlig brottslighet.

I rapporten beskrivs att moms- och välfärdsbedrägerierna utgör det största hotet ur ett brottsvinstperspektiv. Därefter kommer VD-bedrägerierna samt låne- och telefonbedrägerierna. Lånebedrägerierna eftersom de genererar stora belopp och möjliggör för grovt kriminella att tillgodogöra sig brottsvinster genom ägande av bl.a. fastigheter. Telefonbedrägerierna till följd av att det är den bedrägerityp där störst andel misstankerapporterade personer har samband med annan brottslighet och kriminella nätverk. Enligt Finanspolisens bedömning är telefonbedrägerierna en viktig inkomstkälla för den organiserade brottsligheten i Sverige och det finns tecken på att unga personer i utsatta områden utnyttjas som målvakter.

[52] Polismyndigheten, Finanspolissektionen, *Bedrägerier och penningtvätt – Analys av bedrägerier ur ett brottsvinstperspektiv*, (dnr A697.130/2021), januari 2022.

Finanspolisen menar i rapporten vidare att vissa sårbarhetsreducerande åtgärder bör vidtas dels för att stärka bankers och andra verksamhetsutövares förmåga att upptäcka och förhindra bedrägerierna innan de sker, dels för att skapa ökad kontroll hos utbetalande myndigheter i samband med moms- och välfärdsbedrägerier. De exempel på sårbarhetsreducerande åtgärder som föreslås i rapporten är:

– Systematisk övervakning av transaktioner på skattekonton med avseende på penningtvättsrisker – från både Skatteverkets och bankernas sida.
– Högre grad av kundanpassning i övervakningen av transaktioner på företagskonton.
– Teknisk lösning hos bankerna för att upptäcka och förhindra VD-bedrägerier innan transaktionerna genomförs.
– Stärkt kontroll av identitet och löneunderlag i samband med kreditgivning för att minska risken för lånebedrägerier.

6.7.5 Bedrägeribrottsligheten ger näring till annan organiserad brottslighet

Polismyndighetens Nationella bedrägericentrum (NBC) kom i en rapport från 2021 fram till att sambandet mellan den organiserade brottsligheten som aktör, och bedrägeribrottsligheten som brottsfenomen, ger vid handen att bedrägeribrotten är en bland flera mycket framgångsrika vinstdrivande kriminella aktiviteter som individer och grupper inom organiserade kriminella miljöer engagerar sig i.[53]

I rapporten konstaterade NBC att bedrägeribrottslighet är en typ av brottslighet som varierat över tid och att variationer av antalet anmälda bedrägeribrott som regel kan förklaras med införandet av nya finansiella tjänster som sedan kompletterats med olika säkerhetslösningar. Enligt NBC framgår det klart av brottsstatistiken att digitaliseringen av samhället har förändrat tillfällighetsstrukturerna för en rad olika former av kriminella aktiviteter på ett sätt som gynnar de personer som begår bedrägeribrott.

[53] Polismyndigheten, Nationella operativa avdelningen, Nationellt Bedrägericentrum, *De organiserade bedrägerierna – En rapport om bedrägerier kopplade till organiserade kriminella miljöer* (dnr A354.340/2021), 2021.

Polismyndigheten delar in bedrägeribrottsligheten i sex kategorier, i huvudsak på samma sätt som Brå, inom ramen för sin analysverksamhet. Kategorierna är social manipulation, kortbedrägerier, fakturabedrägerier, snyltning och grova fordringsbedrägerier samt försäkringsbedrägerier, bidragsbedrägerier och övriga.

I en rapport som presenterades i april 2023 analyserade NBC brottsvinsterna för bedrägeribrottsligheten 2022. I rapporten redovisas en ökning av dessa från 4,2 miljarder 2020 till 4,6 miljarder 2021 samt anges att brottsvinsten för bedrägerier uppgick till 5,8 miljarder 2022. Enligt rapporten genererade investeringsbedrägerier den högsta brottsvinsten (1,2 miljarder kronor motsvarande 21 procent av den totala brottsvinsten), därefter telefonbedrägerier (cirka 619 miljoner motsvarande 11 procent av totala brottsvinsten) och romansbedrägerier som genererade cirka 609 miljoner kronor i brottsvinst under 2022 (10 procent av den totala brottsvinsten). Identitetsbedrägerier i dess tre olika varianter (köp, lån och övriga) representerar enligt rapporten 14 procent av den totala brottsvinsten med cirka 820 miljoner kronor.[54]

I en rapport från 2022 – som utgör en del av NBC:s uppdrag att analysera förhållandet mellan bedrägeribrott och annan brottslighet som förknippas med organiserad brottslighet – redovisas bl.a. följande.[55]

> Analysen visar att det föreligger en koppling mellan bedrägeribrottsligheten och det dödliga skjutvapenvåldet. Ett rimligt antagande är att den kriminella ekonomin har förändrats på samma sätt som samhället i övrigt sedan 1990-talet. Ibland används begrepp som ”den nya ekonomin” för att beskriva denna förändringsprocess. Under 1990-talet och under de första åren av det nya seklet genomgick de västerländska samhällena en radikal förändring. Samhället och stora delar av såväl offentlig som privat sektor förändrades genom bland annat digitalisering, privatisering av den offentliga sektorn, förändrade kunskapskrav och en alltmer internationaliserad och globaliserad ekonomi. Denna process har också påverkat den kriminella ekonomin. I många avseenden utgör den kriminella ekonomin en inverterad version av den lagliga ekonomin. Digitaliseringen och avregleringen av olika marknader har skapat nya tillfällighetsstrukturer för olika former av brottslighet som ofta kan vara ytterst lukrativ, exempelvis olika slag av välfärdsbedrägerier. En sådan förändrad tillfällighetsstruktur ställer också nya krav på kunskap och organisationsförmåga, något som innebär att nya aktörer förhållandevis enkelt kan etab-

[54] Polismyndigheten, Nationella operativa avdelningen, Nationellt Bedrägericentrum, *Brottsvinsterna för bedrägeribrottsligheten 2022*, (dnr A232.846/2023), april 2023, s.2.
[55] Polismyndigheten, Nationella operativa avdelningen, Nationellt Bedrägericentrum, *De dödliga bedrägerierna*, *En rapport om bedrägeribrottslighet och skjutvapenvåldet*, (dnr A554.314/2022), 2022, s. 21.

lera sig och begå brott som genererar höga brottsvinster. Denna tendens förstärks genom en ökad internationalisering och globalisering. Det är numera förhållandevis enkelt för kriminella aktörer att etablera sig utomlands och skapa lukrativa samarbeten med utländska aktörer.

6.7.6 Bolag och identiteter som målvakter utgör brottsverktyg

I rapporten *Myndighetsgemensam lägesbild, Organiserad brottslighet 2023* anges att aktiebolag är den bolagsform som kriminella aktörer använder mest frekvent samt har ökat sin kunskap och förståelse för.[56]

Brå genomförde inom ramen för sin rapport *Bedrägeribrottsligheten i Sverige* intervjuer med några centrala gärningspersoner. Vid intervjuerna framkom att identitetsuppgifter utnyttjas i samma syfte som målvakter och medhjälpare, dvs. för att minska exponering och risk för huvudgärningspersonen. Flera intervjuade myndighetspersoner beskrev enligt rapporten EU-migranters identiteter som ”den nya tidens målvakter”.[57]

Enligt rapporten används identiteterna på så sätt att en medborgare från ett annat EU-land folkbokförs i Sverige och placeras i styrelsen på ett kreditvärdigt bolag, som sedan genomför omfattande kreditköp innan det försätts i konkurs. Identiteterna kan tillhöra personer som mot betalning tillfälligt hämtas in för ett snabbt besök i Sverige och folkbokförs som inflyttad arbetskraft. Med hjälp av falska arbetsgivarintyg får de ett personnummer som sedan används i brottsligt syfte av huvudmännen. I rapporten anges vidare att intervjuade myndighetsrepresentanter uppgett att personerna vid behov hämtas tillbaka till Sverige och ställer upp vid en eventuell identitetskontroll. Ett annat alternativ är att identiteter tillhörande EU-migranter som redan befinner sig i Sverige utnyttjas i liknande syfte.[58]

Problematiken som Brå redovisade i rapporten redan 2016 beskrivs fortfarande på samma sätt av de myndighetsrepresentanter utredningen har talat med. Ekobrottsmyndigheten har till utredningen framfört att det finns ett omfattande problem bestående i möjligheten att skaffa flertalet olika e-legitimationer hos olika banker och att dessa, till följd av banksekretessen, kan användas samtidigt och

[56] Polismyndigheten, Nationella operativa avdelningen, Myndighetsgemensam lägesbild, Organiserad brottslighet 2023, juni 2023, s. 11 f.
[57] Brå, Bedrägeribrottsligheten i Sverige, Kartläggning och åtgärdsförslag, Rapport 2016:9, mars 2016, s. 143.
[58] A.a. s. 157.

utan någon informationsöverföring mellan banker och myndigheter. Enligt myndigheten har den i sina brottsutredningar sett exempel på att en och samma person innehaft så många som 27 BankID samtidigt och att personen för egen del endast använde två eller tre. Resterande BankID användes av andra personer på telefoner som de hade i sin besittning. Allt eftersom bankerna spärrade e-legitimationerna skapade personerna nya mobila BankID.

6.7.7 Även bidragsbrottsligheten kan involvera användning av oriktiga identitetsuppgifter

Vid bidragsbrott vilseleder gärningspersonen ofta med hjälp av andra uppgifter än identitetsuppgifter. Enligt Brå förekommer dock missbruk av identiteter även vid bidragsbrott. Det handlar om att enskilda personer har flera olika identiteter, vilket möjliggör för samma person att kombinera arbete och bidrag eller ansöka om bidrag ur olika system parallellt och på så sätt få ut ersättning felaktigt.[59]

Utredningen om organiserad och systematisk ekonomisk brottslighet mot välfärden konstaterade i sitt betänkande att det förekommer att identitets- och bosättningsuppgifter på grundval av förfalskade eller manipulerade identitetshandlingar registreras i folkbokföringsdatabasen, vilka därefter används för att begå brott. Den utredningen kunde inte bedöma i hur stor omfattning oriktiga identiteter förekommer vid kvalificerad välfärdsbrottslighet men menade att redan det faktum *att* sådana förekommer, vilket i sig kan skapa möjligheter att begå brott mot välfärdssystemen, gjorde förekomsten särskilt angelägen att motverka. [60]

6.7.8 Säkrare grundidentifiering tillsammans med andra åtgärder kan minska utrymmet för brottslighet

Genom det ovan redovisade framgår tydligt att det finns ett samband mellan ökad digitalisering och identitetsrelaterad brottslighet som i sin tur är sammankopplad med den grova organiserade brottsligheten. Vid införandet av en statlig e-legitimation behöver åtgärder

[59] Brå, Bedrägeribrottsligheten i Sverige, Kartläggning och åtgärdsförslag, Rapport 2016:9, mars 2016, s. 159.
[60] *Kvalificerad välfärdsbrottslighet – förebygga, förhindra, upptäcka och beivra* (SOU 2017:37), s. 267.

vidtas för att förhindra att grupper som redan i dag är utsatta för angiven brottslighet blir än mer sårbara. Som beskrivs i avsnitt 6.3 framhålls i vårt kommittédirektiv vikten av att grundidentifieringen görs på ett noggrant och säkert sätt av en myndighet vid ett personligt besök. I dagsläget finns det ingen enligt eIDAS-förordningen anmäld svensk e-legitimationsutfärdare som genomför grundidentifiering som når upp till kravet för tillitsnivå hög enligt eIDAS-förordningen eller motsvarande tillitsnivå 4 enligt det svenska tillitsramverket. Ett sådant högre krav innebär bl.a. att användarens identitet ska verifieras vid ett personligt besök (se mer om tillitsnivåer i avsnitt 4.2.4). Således skulle en statlig e-legitimation utfärdad på en sådan högre tillitsnivå innebära en säkrare grundidentifiering med ökade möjligheter att säkerställa att en viss digital identitet representerar en viss fysisk person.

Våra bedömningar i angivna avseenden får stöd av en rapport som gavs ut av Brå i september 2023. Rapporten innehåller en omfattande genomgång av problematiken med bedrägeribrottslighet och redovisar brottsförebyggande åtgärder med syfte att, dels minska tekniska och strukturella sårbarheter, dels stärka potentiella brottsoffers motståndskraft. Vidare redovisas bedrägeriförebyggande åtgärder, dels utifrån identifierade tekniska och strukturella sårbarheter, dels identifierade sårbarheter hos potentiella brottsoffer.

En, bland ett flertal andra, rekommendationer från Brå är att en statlig e-legitimation införs och på sikt utvecklas. Enligt Brå skulle införandet av en statlig e-legitimation ha en brottsförebyggande effekt i och med en säkrare grundidentifiering.

Brå konstaterade emellertid också i rapporten att det är uppenbart att den brottsförebyggande verksamhet som bedrivs inte är i närheten av tillräcklig för att komma till rätta med brottsproblemet bedrägerier mot privatpersoner. Enligt Brå krävs åtgärder utformade med praktiska inslag och med syfte att göra brottsoffer mer svårlurade. Vidare menar Brå att ett tydligare helhetsperspektiv i det bedrägeriförebyggande arbetet, där teknik och information används tillsammans för att bättre möta bedragarnas snabba anpassningar, är nödvändigt. Brå rekommenderar bl.a. *att* Polismyndigheten bör ta en ledande roll i det bedrägeriförebyggande arbetet, *att* Polismyndigheten samverkar med andra myndigheter för att utveckla och systematisera riktade informationsinsatser till barn och unga som riskerar att användas som penningmålvakter, *att* Bolagsverket utökar sina kontroller av företrädare för företag, *att* offentliga aktörer på alla nivåer bör utöka sitt

stöd till personer som behöver hjälp med att genomföra digitala tjänster, såsom digitala bankärenden, digitala samhällstjänster och digital handel samt att uppföljning och utvärdering av vidtagna åtgärder sker.[61]

Våra förslag i kapitel 7 syftar, inom ramen för vad vår uppdragsbeskrivning medger, bl.a. till att motverka den identitetsrelaterade brottsligheten. En säker grundidentifiering kan bidra till att uppfylla detta syfte. Som också Brå konstaterar kommer emellertid även andra brottsförebyggande och säkerhetshöjande åtgärder vara av avgörande betydelse för att det ska finnas en reell möjlighet att motverka den identitetsrelaterade brottsligheten.

[61] Brå, *Bedrägerier mot privatpersoner – De brottsförebyggande åtgärdernas träffsäkerhet,* Rapport 2023:11, september 2023, s. 65 ff.

7 Utredningens överväganden och förslag

7.1 Författningsreglering

Utredningens förslag: Den lagreglering som är nödvändig med anledning av införandet av en statlig e-legitimation ska samlas i en ny lag, benämnd lagen om elektronisk identifiering.

Övriga bestämmelser, bl.a. sådana som behövs för verkställigheten av lagen meddelas på annan nivå än lag.

Lagen ska innehålla upplysning om att bestämmelser om elektronisk identifiering även finns i andra författningar. I lagen tas också in bestämmelser som definierar vissa ord och uttryck som används i lagen.

Skälen för utredningens förslag

I vårt uppdrag ingår att utarbeta de författningsförslag som behövs för att genomföra våra övriga förslag. Som framgår av det följande lämnar vi förslag om bl.a. förutsättningar för att tillhandahålla respektive att tillhandahållas en statlig e-legitimation.

Den uppgifts- och ansvarsfördelning som aktualiseras mellan berörda myndigheter i den gemensamma utgivningsprocessen bör författningsregleras, även om delar av det praktiska arbetet, som Myndigheten för digital förvaltning (Digg) anför, kan hanteras genom överenskommelser och myndighetssamverkan.[1] Likaså kräver den statliga e-legitimationen behandling av personuppgifter hos samtliga be-

[1] Myndigheten för digital förvaltning, *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, s. 59 f.

rörda myndigheter, vilket också måste framgå av författningsbestämmelser.

En första fråga är huruvida den statliga e-legitimationen bör särregleras eller om bestämmelser kan föras in i en befintlig författning. Också normgivningsnivå för en reglering behöver analyseras, utifrån dess innehåll och konsekvenser.

Utredningen om effektiv styrning av nationella digitala tjänster och 2017 års ID-kortsutredning, vilka båda föreslog att den statliga e-legitimationen skulle ha det nationella identitetskortet som fysisk bärare, lämnade två disparata förslag vad gäller författningsregleringen. Medan den förstnämnda utredningen ansåg att den statliga e-legitimationen borde regleras i en egen lag, föreslog 2017 års ID-kortsutredning att den fysiska och den elektroniska identitetshandlingen skulle regleras i en ny gemensam lag.[2]

Enligt vår tolkning av utredningsdirektiven är det i vart fall inte inledningsvis aktuellt att använda det nationella identitetskortet eller identitetskortet för folkbokförda i Sverige som bärare för den nu föreslagna e-legitimationen (se avsnitt 7.2.2). I frånvaro av en sådan direkt koppling anser vi att e-legitimationen, som är att anse som en urkund i sig, bör omfattas av en särreglering. Frågan är då om regleringen ska ske i lag, eller om den kan införas i en förordning, såsom Digg har föreslagit.[3]

Till stöd för sin bedömning har Digg anfört att en reglering på annan nivå än lag framstår som ändamålsenligt med beaktande av den snäva tidsram som angetts som målsättning för att ta funktioner för statlig e-legitimation i drift. Ett ytterligare anfört argument är att det varken vid utfärdande eller användning av den statliga e-legitimationen förekommer några sådana betydande intrång i den personliga integriteten som avses i 2 kap. 6 § andra stycket regeringsformen och som kräver reglering i lagform. Digg har bedömt att förslaget inte heller innebär sådana skyldigheter för enskilda eller ingrepp i enskildas personliga eller ekonomiska förhållanden som avses i 8 kap. 2 § första stycket 2 regeringsformen. Slutligen har Digg konstaterat att lagkrav inte behövs enligt Europeiska konventionen om skydd för de mänskliga rättigheterna eller av annat skäl.[4]

---

[2] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114) s. 194, respektive *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14), s. 331 ff.
[3] Myndigheten för digital förvaltning, *En säker och tillgänglig statlig e-legitimation –Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, s. 57 ff.
[4] Ibid.

Våra förslag om bl.a. utformningen av den statliga e-legitimationen föranleder en annan bedömning.

Enligt 2 kap. 6 § andra stycket regeringsformen är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Inskränkningar kan endast göras genom lag och bara under vissa förutsättningar (2 kap. 20 och 21 §§ regeringsformen).

I den databas över statliga e-legitimationer och i samband med ansökan om och utgivning av en statlig e-legitimation, liksom vid dess användning, behandlas sådana uppgifter om enskildas personliga förhållanden som avses i bestämmelsen i 2 kap. 6 § regeringsformen. Databasen innehåller uppgifter om bl.a. namn och personnummer alternativt samordningsnummer för personer med styrkt identitet.

Vid ansökan och utgivning kan, enligt våra förslag, även ansiktsbild och fingeravtryck komma att behandlas i identifieringssyfte (se avsnitten 7.5 och 7.11.7). Därmed får, oaktat att syftet med behandlingen av personuppgifterna är ett annat, personuppgiftsbehandlingen anses innefatta en sådan kartläggning av enskildas personliga förhållanden som avses i 2 kap. 6 § andra stycket regeringsformen.

I databasen och i samband med e-legitimationernas användning behandlas även en förhållandevis stor mängd personuppgifter. Detta är omständigheter som kan tala för att intrånget i den enskildes personliga integritet ska anses vara betydande. Uppgifterna i databasen behandlas främst för ändamålen att den statliga e-legitimationen ska kunna utfärdas och för att verifiera innehavarens identitet vid användandet av digitala tjänster. Verksamheten i sig kan inte betraktas som särskilt integritetskänslig. De flesta av de personuppgifter som behandlas är inte av känslig karaktär. Vidare har den enskilde kännedom om att personuppgifterna behandlas, eftersom hon eller han har ansökt om e-legitimationen och därvid lämnat sina uppgifter. Behandlingen av personuppgifter får mot denna bakgrund anses innebära ett visst intrång i den enskildes personliga integritet, men inte så betydande att det omfattas av grundlagsskyddet i 2 kap. 6 § andra stycket regeringsformen. Det innebär att behandlingen av personuppgifter i databasen inte på grund av den bestämmelsen nödvändigtvis måste regleras i lag.

Eftersom databasen kan komma att innehålla uppgifter om ett potentiellt stort antal personer, och vissa av uppgifterna är av mer integritetskänsligt slag, framstår det ändå som lämpligt att i huvud-

sak ta in bestämmelserna om behandling av personuppgifter i lag. Både riksdagen och regeringen har uttalat att myndighetsregister som innehåller ett stort antal registrerade och har ett särskilt känsligt innehåll bör regleras i lag.[5] Även de mest centrala kriterierna för att utfärda en e-legitimation, liksom vissa krav i samband med ansökan och grunder för återkallelse, är av samma skäl lämpliga att reglera i lag.[6]

Dessutom föreslår vi att det ska uppställas krav om att bl.a. den statliga e-legitimationen ska godkännas av offentliga aktörer (se avsnitt 7.13). Förslaget omfattar åligganden för t.ex. kommunerna. Också av det skälet krävs att vissa bestämmelser tas in i en lag och inte i en förordning.

Frågan är då om lagbestämmelserna bör infogas i en redan gällande lag eller samlas i en särskild författning. Som redan angetts föreslår vi att den statliga e-legitimationen inte ska ha någon befintlig, statlig identitetshandling som fysisk bärare, och att en särreglering är att föredra. Detta eftersom det saknas direkt koppling till gällande regleringar på området, såsom lagen (2015:899) om identitetskort för folkbokförda i Sverige samt passlagen (1978:302) och förordningen (2005:661) om nationellt identitetskort.

I nationell lagstiftning finns endast en lag som direkt berör e-legitimationer och det är lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering. Sett till den lagens syfte och de bestämmelser den innehåller kan det emellertid inte anses lämpligt att däri föra in de aktuella bestämmelserna.

Vi bedömer således att det inte finns någon befintlig lag där nödvändig reglering passar in. De nya lagbestämmelserna ska därför samlas i en särskild författning. Därigenom underlättas även möjligheterna att hitta de nya bestämmelserna.

För det fall att det i framtiden bedöms finnas förutsättningar att, som 2017 års ID-kortsutredning föreslagit, använda det nationella identitetskortet som bärare av den statliga e-legitimationen, bör det övervägas om bestämmelser som rör både det fysiska identitetskortet och den statliga e-legitimationen ska regleras i samma författning.

[5] Bet. 1990/91:KU11 s. 33 ff. och prop. 1990/91:60 s. 58.

[6] Jfr prop. 2015/16:28 s. 57 f. Lagstiftningsärendet gällde bl.a. en översyn av regleringen av identitetskort för folkbokförda i Sverige, som gjordes mot bakgrund av införandet av bestämmelsen i 2 kap. 6 § andra stycket regeringsformen. Regleringen fanns i en förordning och syftet var att bedöma om bestämmelserna måste eller borde tas in i lag. Översynen resulterade i att delar av förordningen infördes i lagen (2015:899) om identitetskort för folkbokförda i Sverige.

Den föreslagna lagen bör kompletteras med verkställighetsföreskrifter, vilket vi i förekommande fall behandlar i anslutning till våra förslag i sak. Regleringsformen kommer därmed motsvara vad som gäller för t.ex. pass och identitetskort för folkbokförda i Sverige.

De lagbestämmelser vi föreslår rör i huvudsak den statliga e-legitimationen. Vi föreslår emellertid även en lagbestämmelse om krav för vissa aktörer att godta andra e-legitimationer (se avsnitt 7.13). Som framgått finns – utöver tidigare nämnda lag med kompletterande bestämmelser till eIDAS-förordningen – inga svenska författningar som direkt reglerar e-legitimationer. Det har tidigare bedömts att e-legitimationsområdet är underreglerat och vi ser därför att det framöver kan finnas behov av ytterligare nationell lagreglering.[7] Den nya lagen bör därmed benämnas på ett sätt som avspeglar dess föreslagna innehåll och tillämpningsområde, men som samtidigt är så pass allmänt hållet att lagen framöver kan kompletteras med andra bestämmelser rörande e-legitimationer. Lagen bör därmed ges ett namn som inte endast indikerar att den innehåller bestämmelser om den statliga e-legitimationen. Begreppet e-legitimation förekommer inte i nu gällande författningar. I stället används begreppen elektronisk identifiering och medel för elektronisk identifiering (se avsnitt 3.5). Vi föreslår därför att lagen benämns lag om elektronisk identifiering.

Elektronisk identifiering är även det begrepp som används i eIDAS-förordningen. Första gången en EU-rättsakt nämns i en svensk grundförfattning skriver man ut rättsaktens fullständiga namn. I omfattande författningar kan man behöva skriva ut rättsaktens fullständiga namn flera gånger, t.ex. i början av varje kapitel. Vid upprepade hänvisningar kan ett förkortat namn av EU-rättsakten användas. Det förkortade namnet för eIDAS-förordningen i svenska författningar är EU:s förordning om elektronisk identifiering. Därtill finns den ovan nämnda lagen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering. Det finns därför en viss förväxlingsrisk mellan namnet på vår föreslagna lag och kortformen för eIDAS-förordningen i svenska författningar.

För att motverka denna risk och samtidigt underlätta för personer som läser lagen att identifiera andra författningar som rör elektronisk identifiering föreslår vi att en bestämmelse tas in i lagen som lämnar upplysningar om att bestämmelser om elektronisk identifiering även finns i andra författningar. Vidare tas i lagen in bestämmelser med

[7] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 170.

definitioner av vissa ord och uttryck i lagen, t.ex. medel för elektronisk identifiering som utgörande den författningsrättsliga benämningen för e-legitimation.

7.2 Utformning av den statliga e-legitimationen

7.2.1 Utgångspunkter för utformningen

I våra direktiv anges bl.a. att syftet med att införa en statlig e-legitimation är att stärka samhällets säkerhet och robusthet, motverka bedrägerier som begås med hjälp av e-legitimationer samt underlätta för så många som möjligt att kunna få tillgång till en e-legitimation.

Under arbetets gång har det blivit allt tydligare att dessa syften i vissa avseenden dels är svåra att förena med varandra om man eftersträvar maximal uppfyllelse av respektive syfte, dels inte kan åstadkommas fullt ut inom ramen för vårt uppdrag. En e-legitimation omgärdad av så höga säkerhetsanordningar att bedrägeribrottslighet helt förhindras skulle sannolikt bli svåranvänd för många och innebära omotiverade integritetsintrång. Därtill kommer att utformningen av e-legitimationen i sig inte helt kan undanröja de risker som finns vid användningen av den. Således är de förslag vi lämnar avsedda att tillgodose angivna syften i så stor utsträckning som möjligt. Vi bedömer att våra förslag bidrar till att uppnå de syften som anges ovan även om ytterligare åtgärder kommer att vara nödvändiga.

7.2.2 Den statliga e-legitimationen ska tillhandahållas på ett kontaktlöst kort

Utredningens förslag: Den statliga e-legitimationen ska finnas på ett kontaktlöst aktivt kort. E-legitimationens utformning ska regleras på förordningsnivå.

Utredningens bedömning: Den statliga e-legitimationen bör så snart som möjligt tillhandahållas på en fysisk identitetshandling utfärdad av staten.

Skälen för utredningens förslag och bedömning

Enligt utredningsdirektiven ska den statliga e-legitimationen utfärdas på den högsta tillitsnivån (se även avsnitt 7.4.1). Kraven på e-legitimationer på nivå hög framgår av eIDAS-förordningen. Enligt artikel 8.2 c framgår att tillitsnivå hög ska avse ett medel för elektronisk identifiering som ger en högre grad av tillförlitlighet avseende en persons påstådda eller styrkta identitet än tillitsnivån väsentlig, och definieras med hänvisning till tekniska specifikationer, standarder och förfaranden som avser detta, inbegripet tekniska kontroller, vilkas syfte är att förhindra risken för missbruk eller ändring av identiteten.

Detaljerna avseende kraven på nivå hög utvecklas i Kommissionens genomförandeförordning (EU) 2015/1502 av den 8september 2015 om fastställande av tekniska minimispecifikationer och förfaranden för tillitsnivåer för medel för elektronisk identifiering i enlighet med artikel 8.3 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden, härefter genomförandeförordningen (EU) 2015/1502. Genomförandeförordningen innehåller specifikationer och procedurer m.m. De bestämmelser som påverkar utformningen av en e-legitimation återfinns i bilagan (Avsnitt 2.2 Hantering av medel för elektronisk identifiering) till genomförandeförordningen och består av krav på hantering av medlet för elektronisk identifiering, dvs. en e-legitimation.

Kravet på nivå hög medför att medlet för elektronisk identifiering ska möjliggöra åtminstone tvåfaktorsautentisering, dvs. en kombination av två av faktorerna: något personen vet, kan eller har. Vidare ska medlet vara utformat på ett sådant sätt att det bara kan användas under innehavarens egen kontroll. Därutöver ska medlet för elektronisk identifiering skyddas mot kopiering, förvanskning och annan manipulation, liksom mot möjlig användning av annan än användaren.

Utöver dessa krav finns det ett s.k. ”cooperation network” som är den gruppering som bildats i enlighet med artikel 12 stycke 6 i eIDAS-förordningen.[8] Denna grupp har skapat en vägledning för reglerna i den nämnda genomförandeförordningen.[9] Vägledningen

[8] Gruppen utbyter information, erfarenheter och praxis på området elektronisk identifiering men gör också sakkunnigbedömning av system för elektronisk identifiering för de system som notifierats från medlemsländerna.
[9] Guidance for the application of the levels of assurance which support the eIDAS regulation.

innehåller inte krav rörande själva utformningen av medlet för elektronisk identifiering.

Enligt Digg, som är svensk deltagare i cooperation network, har det genom andra medlemsländers e-legitimationssystem utvecklats en praxis i vissa länder som innebär att kravet på manipulerings- och kopieringsskydd på nivå hög ska styrkas genom certifiering utförd av oberoende part.[10] Något sådant krav framkommer dock inte av eIDAS-förordningen, genomförandeförordningen eller den tillhörande vägledningen. Vi bedömer emellertid att certifiering bör genomföras för att säkerställa en hög nivå av säkerhet.

Kan den statliga e-legitimationen tillhandahållas som en mobil applikation?

De vanligast förekommande e-legitimationerna för privat bruk på den svenska marknaden, Mobilt BankID och Freja+, nås via mobila applikationer (appar). Det innebär att appar är vad merparten av användarna av e-legitimationer är mest vana vid att använda och troligen också vill ha. Certifiering på nivå hög är dock svårt att genomföra för mobiltelefonbaserade lösningar eftersom det i dagsläget saknas telefoner som innehåller certifierade säkra chip, (s.k. ”secure element”). Det beror i sin tur på att certifieringen är tid- och resurskrävande, och det gäller särskilt för en så pass komplex blandning av hård- och mjukvara som en mobiltelefon utgör.

Vanligtvis är det aktiva kort som certifieras, och även en sådan granskning är tidskrävande och dyr, trots att det är en betydligt enklare produkt med mindre komplex mjuk- och hårdvara. Tiden och kostnaden beror på produkten och hur omfattande granskning som krävs, s.k. assuransnivå. Assuransnivån avgör hur omfattande utvärderingar och tester som görs av den produkt som ska certifieras.

I de delar av eIDAS-förordningen där det ställs krav på certifierade produkter gäller det för HSM-moduler och anordningar för skapande av kvalificerade elektroniska underskrifter och för dessa har assuransnivån varit 4 eller 4+. Det innebär att certifiering av säkra chip med tillhörande mjukvara i mobiltelefoner kommer att vara både kostsamt och tidskrävande. Certifiering av säkra chip i mobiltelefoner kommer därför troligen enbart att vara aktuellt för vissa nyare

[10] Myndigheten för digital förvaltning, *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, s. 35.

telefonmodeller, men det finns då problem gällande hur certifieringen kan upprätthållas i samband med uppdatering av chipen i mobiltelefonerna. Detta skulle även innebära att det kommer att finnas en stor mängd mobiltelefoner som inte har certifierade chip och som därmed inte kan användas som bärare av den statliga e-legitimationen på den högsta tillitsnivån.

Effekterna av svårigheterna med att certifiera mobiltelefonbaserade lösningar medför att vi bedömer att sådana i dagsläget inte är lämpliga bärare av en statlig e-legitimation på tillitsnivå hög. Om en mobiltelefonbaserad lösning eftersträvas för statlig e-legitimation på tillitsnivå hög så kommer den sannolikt att ta tid utveckla och få en begränsad spridning.

Frågan om en statlig e-legitimation bör tillhandahållas på en lägre tillitsnivå, där det inte behövs certifiering av bäraren, är en fråga som ligger utanför ramen för vårt uppdrag. Vi vill dock lyfta fram att de flesta som har tillgång till en mobiltelefon redan har, eller kan få, en kommersiell e-legitimation.

Även om vissa skulle uppleva att det medför högre användarvänlighet ser vi därför att behovet av en statlig mobil e-legitimation är begränsat. Vissa gruppers behov från ett tillgänglighetsperspektiv skulle även inte kunna tillgodoses enbart genom en mobilbaserad lösning.

Vilken fysisk bärare är lämpligast?

Som konstateras ovan ska den statliga e-legitimationen vara baserad på en hårdvara. Det finns flera tänkbara lösningar för hur en sådan hårdvara kan utformas, till exempel aktiva kort med kontaktchip, kontaktlösa aktiva kort, eller USB-dongel. Digg utvärderade i sin rapport flera möjliga bärare och föreslog att den statliga e-legitimationen ska ges ut som ett kontaktlöst aktivt kort.[11] Digg angav som skäl för sitt förslag bl.a. att det redan finns flera mobila e-legitimationer och att ytterligare en inte bidrar till mer tillgänglighet samt att ett kontaktlöst aktivt kort kan läsas via s.k. NFC av surfplattor och mobiltelefoner men även av kortläsare till datorer.[12] Vi ansluter oss till Diggs bedöm-

[11] Myndigheten för digital förvaltning, *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, s. 32.
[12] Near Field Communication är en standard för överföring av data kontaktlöst över korta sträckor som standardiseras av NFC-forum.

ning och anser att ett kontaktlöst aktivt kort är en lämplig bärare av den statliga e-legitimationen.

De närmare bestämmelser som är nödvändiga beträffande e-legitimationens tekniska utformning meddelas lämpligen på lägre nivå än lag. En upplysningsbestämmelse om rätt att meddela sådana verkställighetsföreskrifter tas därför in i den föreslagna nya lagen om elektronisk identifiering.

Digg har vidare föreslagit att den statliga e-legitimationen baseras på de amerikanska PIV-specifikationerna.[13] Enligt vår bedömning är det i och för sig möjligt att basera den statliga e-legitimationen på dessa standarder, men ytterligare harmoniseringskrav på området via EU-regelverk kommer troligen referera till europeiska standarder från the European Committee for Standardization (CEN) och The European Telecommunications Standards Institute (ETSI). Vi bedömer därför att korten bör baseras på öppna standarder och europeisk standard när sådan finns.

Vid utredningens kontakter med experter, den privata sektorn och myndigheter har den absoluta merparten framfört att det – för att den statliga e-legitimationen ska bli en framgång och nå större volymer – krävs att den tillhandahålls på en statligt utgiven fysisk id-handling, till exempel det nationella identitetskortet, och inte på ett blankt kort. Utöver att placeringen på ett fysiskt id-kort kan förväntas bidra till ett större intresse har bedömningen motiverats med att användarna i högre utsträckning kommer att uppfatta den statliga e-legitimationen som en värdehandling om den finns på en fysisk id-handling.

Även om Digg föreslog att den statliga e-legitimationen skulle tillhandahållas på ett kontaktlöst aktivt kort bedömde myndigheten att det nationella identitetskortet på sikt skulle kunna bli en kompletterande bärare. Utöver argumentet att vissa målgrupper inte kan få ett nationellt identitetskort anförde Digg att processen att skaffa ett sådant kort är förhållandevis lång och att priset kan ha en avhållande effekt.[14] Digg föreslog slutligen att myndigheten skulle ges i uppdrag att ytterligare undersöka hur den statliga e-legitimationen kan tillhandahållas via det nationella identitetskortet.[15]

Vi menar att övervägande skäl talar för att den statliga e-legitimationen som utgångspunkt, och så snart det bedöms möjligt, bör till-

[13] Personal Identity Verification som standardiserats av NIST.
[14] Myndigheten för digital förvaltning, *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, s. 34.
[15] A.a. s. 92.

handahållas på en statligt utfärdad fysisk id-handling. Ett viktigt skäl för detta är att det tydligt signalerar att det rör sig om en värdehandling.

För att tillgodose behovet för icke svenska medborgare och personer med samordningsnummer, som alltså inte kan få ett nationellt identitetskort eller ett identitetskort för folkbokförda i Sverige, kan det emellertid fortsatt finnas behov av en annan bärare även om den statliga e-legitimationen tillhandahålls på en statligt utfärdad fysisk id-handling.

7.2.3 Den statliga e-legitimationen ska innehålla namn och identitetsbeteckning

Utredningens förslag: Den statliga e-legitimationen ska innehålla efternamn, förnamn, namn som visas för användaren och identitetsbeteckning.

Skälen för utredningens förslag

Digg tillhandahåller statens nationella identitetsfederation Sweden Connect och i dess tekniska ramverk finns en attributsspecifikation av attribut som används vid e-legitimering för det svenska ramverket för elektronisk identifiering som tillhandahålls för Sweden Connect av Digg.[16] Dessa format är de som de kommersiella tillhandahållarna använder och som främst förekommer på den svenska marknaden. Den statliga e-legitimationen bör innehålla och tillhandahålla samma attribut.[17] De attribut som ska tillhandahållas är då efternamn, förnamn, namn som visas för användaren samt identitetsbeckning. Se avsnitt 7.4.2 avseende de identitetsbeteckningar som omfattas.

[16] *Attribute Specification for the Swedish eID Framework*, *Version 1.7* docs.swedenconnect.se/technical-framework/latest/04_Attribute_Specification_for_the_Swedish_eID_Framework.html (hämtad 2023-05-31).
[17] A.a. avsnitt 2.3.

7.2.4 Den statliga e-legitimationen ska utformas för att tillåta anpassningar och innehålla personlig prägel

Utredningens bedömning: Utformningen av den statliga e-legitimationen kan inte utan andra anpassningar skapa användarbarhet för alla. Regelverket bör därför utformas på ett sätt som möjliggör anpassningar i utformningen av den fysiska bäraren och kompletteras med andra åtgärder.

Det kontaktlösa kortet bör utformas med en personlig prägel.

Skälen för utredningens bedömning

Som beskrivits i avsnitt 6.6 finns det vissa författningskrav som kan påverka utformningen av den statliga e-legitimationen. EU:s tillgänglighetsdirektiv anger exempelvis beträffande banktjänster för konsumenter att identifieringsmetoder, elektroniska signaturer och betaltjänster ska vara uppfattningsbara, hanterbara, begripliga och robusta. Även FN:s funktionsrättskonvention syftar till att säkerställa att personer med funktionsnedsättning har tillgång till bl.a. tjänster på lika villkor som andra.

Vid utredningens kontakter med representanter för organisationer som samlar personer med olika funktionsnedsättningar eller andra hjälpbehov har flertalet aspekter som är viktiga för utformningen framkommit. Åsikten att utformningen ska vara sådan att den erbjuder valmöjligheter, och inte särlösningar, har varit återkommande.

Synskadades riksförbund har i samtal med utredningen särskilt framfört ett behov av taktila kännetecken på kortet och att utformningen ska vara möjlig att använda tillsammans med ett skärmläsarprogram som omvandlar innehåll på skärmen till tal eller punktskrift. Digg föreslog i sin rapport att kortet ska utformas utan personlig prägel men framhöll att särskilt fokus i ett framtida arbete skulle läggas på mer utförliga tester av tillgängligheten. Enligt Digg skulle dessa sannolikt leda till kompletteringar i form av anpassningar för att möta olika gruppers behov.[18] Vi anser, liksom Digg, att det av såväl tillgänglighets- som säkerhetsskäl bör vara prioriterat att genomföra konkreta användarundersökningar med de grupper som berörs. Ett sådant omfattande

[18] Myndigheten för digital förvaltning, *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, s. 93 och Bilaga 1, s. 4.

arbete har inte varit möjligt att genomföra inom ramen för vårt uppdrag och lämpar sig därtill bättre i ett senare skede när en produkt finns på plats att utvärdera löpande. Enligt vår bedömning finns det emellertid, mot bakgrund av det som Synskadades riksförbund framhållit, skäl att redan från början tillse att kortet har någon form av prägel eftersom det utgör en förutsättning för synskadades möjlighet att särskilja e-legitimationen från andra kort. Vi anser således att kortet bör utformas med en personlig prägel.

Dyslexiförbundet har framhållit att det kan vara svårt för personer med kognitiva svårigheter att minnas koder, varför en möjlighet till inloggning med ansiktsigenkänning eller fingeravtryck skulle vara värdefull. Andra organisationer har påpekat att det finns personer som till följd av olika sjukdomstillstånd inte kan lämna fingeravtryck eller använda ansiktsigenkänning. Även dessa synpunkter behöver tas om hand i ett framtida arbete med tester.

Vi bedömer emellertid att anpassningar i utformningen av den statliga e-legitimationen inte ensamt kan leda till uppfyllelse av målet att inkludera alla som står utanför – det behövs även andra åtgärder. Ställföreträdarutredningen bedömde exempelvis att ett nationellt register över förordnade förmyndare, gode män och förvaltare samt de som har en sådan ställföreträdare, var nödvändigt för att huvudmän ska kunna få tillgång till e-legitimation och digitala tjänster i större utsträckning än i dag. Vi ansluter oss till den bedömningen och kan därutöver konstatera att i stort sett samtliga intresseorganisationer som vi talat med har fört fram att det finns ett stort behov av supportinsatser i användningsskedet. Detta är också något som Digg anförde i sin slutrapport vari Digg föreslog att stödet t.ex. lämnas via offentliga aktörer såsom Statens servicecenter, kommunala DigiDel-center och bibliotek.[19]

Utöver att minnas koder kan en utmaning för personer med kognitiva svårigheter förväntas vara att minnas hur den statliga e-legitimationen rent praktiskt fungerar. *Autism Sverige* och *Riksförbundet FUB* har exempelvis påtalat att många av deras medlemmar sannolikt kommer att behöva hjälp vid varje enskilt användningstillfälle. För att en anpassad utformning ska kunna leda till ökad tillgänglighet krävs således en väl utvecklad supportfunktion och möjligheter för ställföreträdare att bistå sina huvudmän.

[19] A.a. s. 93 f.

För att tillgodose behovet av att över tid tillhandahålla en tillgänglig statlig e-legitimation kommer anpassningar till ny teknik ständigt behövas. Det kan ha att göra med ny teknik för e-legitimationen som sådan eller att nya hjälpmedel för personer med funktionsnedsättning erbjuds. Den utfärdande myndigheten behöver således ges utrymme att anpassa utformningen av den statliga e-legitimationen efter vilka alternativ för läsning som vid ett visst tillfälle behöver finnas tillgängliga. Utvecklingen av olika praktiska hjälpmedel som krävs bör lämpligen ske i samarbete med berörda organisationer.

7.2.5 Säker utformning av den statliga e-legitimationen

Utredningens bedömning: Bäraren av den statliga e-legitimationen ska ha skydd mot obehörig användning, läsning och kopiering av uppgifter på bäraren.

Den statliga e-legitimationen bör använda krypteringsalgoritmer enligt nationella eller europeiska rekommendationer. Den statliga e-legitimationen bör ha stöd för två olika krypteringsalgoritmer samtidigt.

Placering av den statliga e-legitimationen på fysiskt identitetskort bidrar till ökad säkerhet.

Kontinuiteteten i försörjningskedjan till den statliga e-legitimationen behöver säkerställas.

Skälen för utredningens bedömning

I likhet med Digg anser vi att den statliga e-legitimationen behöver ha flera lager av skydd och använda beprövad och testad teknik, standarder och implementationer.[20] Den statliga e-legitimationen behöver särskilt skyddas mot obehörig läsning, kopiering och användning och tillhörande uppgifter som krypteringsnycklar och biometrisk information om innehavaren. Det sker genom olika tekniska skyddsåtgärder, användning av säkra standarder, implementationer, protokoll, kryptering samt underskrifter och stämplar. Den utfärdande myndigheten behöver genomföra återkommande riskanalyser och identifiera

[20] Myndigheten för digital förvaltning, *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, s. 20.

lämpliga skyddsåtgärder, samt följa upp dessa för att långsiktigt upprätthålla säkerheten i den statliga e-legitimationen. I det arbetet kan den utfärdande myndigheten söka råd och stöd från andra myndigheter med ansvar och kompetens på området.

Den statliga e-legitimationen behöver använda krypteringsalgoritmer och implementationer som är säkra. Det kan ske genom att det kommer nationella rekommendationer i enlighet med förslaget till en strategi och åtgärdsplan för kryptografiska funktioner från den s.k. NISU-utredningen.[21] I avsaknad av sådana rekommendationer kan europeiska rekommendationer användas. Den statliga e-legitimationen behöver vidare byggas så pass robust att sårbarheter i en enskild standard, algoritm eller implementation inte gör den obrukbar på det sätt som skedde för vissa nationella id-kort i samband med den s.k. ROCA-sårbarheten[22].

Utredningen delar Diggs bedömning avseende behovet av stöd för fler än en uppsättning krypteringsalgoritmer.[23] Den statliga e-legitimationen kommer att vara beroende av olika leverantörer och försörjningskedjan behöver därmed vara säker och det behöver därtill finnas en leveransförmåga även under perioder av svåra påfrestningar, kris och ytterst krig. Det innebär att aktörer som ingår i leveranskedjan behöver granskas och kan behöva vara föremål för en riskanalys. Detta kan begränsa antalet möjliga leverantörer som kan leverera bäraren och andra tillhörande system och komponenter som behövs för utformningen av e-legitimationen. Vidare behöver leveransförmågan och lager av kortämnen och andra kritiska komponenter säkerställas. Den statliga e-legitimationen kommer sannolikt omfattas av säkerhetsskyddslagens (2018:585) bestämmelser och de olika leverantörerna kommer troligen behöva teckna säkerhetsskyddsavtal.

[21] *Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten* (SOU 2015:23), s. 303.
[22] Se mer om ROCA-sårbarheten i *Vem kan man lita på? – Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen* (SOU 2021:9), s. 229 ff.
[23] *Ett säkert statligt Id-kort – med e-legitimation* (SOU 2019:14), s. 37.

7.2.6 Den statliga e-legitimationen ska innehålla vissa biometriska uppgifter om innehavaren

Utredningens förslag: Den statliga e-legitimationen ska i ett lagringsmedium på bäraren innehålla ansiktsbild och fingeravtryck.

En innehavare av en statlig e-legitimation ska ha rätt att kontrollera den information som har sparats i lagringsmediet på e-legitimationens bärare.

Utredningens bedömning: Särskilda åtgärder bör vidtas för att skydda de biometriska uppgifterna i lagringsmediet på bäraren.

Skälen för utredningens förslag och bedömning

Hur biometriska uppgifter ska få användas av myndigheter är föremål för ständigt pågående diskussioner. För såväl pass som nationella identitetskort gäller – såvitt avser vad som får lagras i bäraren – att ansiktsbilder och fingeravtryck får lagras i ett chip. Frågan uppkommer därmed om även den statliga e-legitimationen ska ha motsvarande innehåll som kan användas för biometriska jämförelser.

Biometriutredningen definierade i sitt betänkande vad biometri är, eftersom legaldefinitioner av begreppet saknas. Utredningens definition ser ut enligt följande.[24]

> Biometri är ett begrepp som förekommer i olika sammanhang men som inte har en helt entydig innebörd. Det finns ingen definition i lag av begreppet. I förarbetena till brottsdatalagen anges att biometri är ett samlingsnamn för sådan automatiserad teknik som syftar till att identifiera en person eller avgöra om en påstådd identitet är riktig (prop. 2017/18:232 s. 86). Det innebär att tekniken är baserad på fysiska karaktärsdrag hos den som ska identifieras.
>
> Inom brottsbekämpningen syftar biometri i regel på metoder för att identifiera en person eller avgöra om en antagen eller ifrågasatt identitet är riktig, t.ex. utifrån personens fysiska karaktärsdrag. Det kan handla om att göra datorstödda jämförelser av fingeravtryck, dna-profiler, ansiktsbilder eller röstprov. Begreppet biometri syftar alltså på den automatiserade metod eller teknik som används för att jämföra individuella kännetecken i identifieringssyfte. Det innebär att det finns olika slags biometrier, t.ex. fingeravtrycksanalys, dna-analys, ansiktsigenkänning, röstigenkänning och handstilsanalys. (…) När vi i detta betänkande använder oss av begreppet biometri avser vi begreppet med denna innebörd. Vi åsyftar alltså

[24] *Biometri – för en effektivare brottsbekämpning* (SOU 2023:32), s. 246.

den teknik och metod som används för automatiserade jämförelser av olika slags individuella kännetecken.

I sin rapport har Digg konstaterat att en säkrare grundidentifiering skulle kunna genomföras om den identitetskontrollerande myndigheten vid handläggningen av ett ansökningsärende hade tillgång till, och fick behandla, biometriska uppgifter. Myndigheten har därför föreslagit att förutsättningarna för sådan behandling ska utredas vidare.[25] I en till rapporten kompletterande bilaga har Digg utvecklat sin syn på de tekniska och praktiska hinder som biometriverifiering på distans kan medföra och som i förlängningen kan försvåra eller förhindra användning av e-legitimationer.

Digg har i bilagan anfört att kontroller som jämför biometriska uppgifter, som används vid exempelvis gränskontroller, inte fungerar på distans i en elektronisk miljö. Vidare har Digg påtalat att de biometriska sensorer som finns i dagens smarttelefoner inte är åtkomliga för tredjepartstillämpningar och att det inte är möjligt att läsa ut de biometriska uppgifterna som användaren registrerat i telefonen eller att tillföra biometriska uppgifter från annat håll. Således är det inte möjligt att använda en telefons biometriska sensorer för att stärka säkerheten i elektronisk identifiering på distans. Enligt Digg skulle eventuella manipulationer, såsom avgjutningar av fingeravtryck, inte heller kunna upptäckas, eftersom avläsning av de biometriska avtrycken sker oövervakat. Vidare skulle en metod med användning av ansiktsjämförelser enligt Digg ställa krav på telefonen och omgivningen samt fodra tillförlitliga kontroller och således kräva en fungerande kompletterande handläggning.[26]

Den statliga e-legitimationen, i likhet med de kommersiella e-legitimationerna, riskerar att missbrukas. Det är svårt att förhindra alla dessa risker, eller helt eliminera dem; däremot kan riskerna till viss mån reduceras. En vanlig risk och ett säkerhetsproblem i dag är att personer lånar ut sin e-legitimation medvetet eller omedvetet, alternativt att den används utan innehavarens kännedom (se mer om detta i avsnitt 6.7).

Polismyndigheten har framfört att en av svagheterna i Diggs tekniska lösning är att det saknas biometrisk autentisering, och efterfrågat

[25] Myndigheten för digital förvaltning, *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, s. 95.
[26] A.a. bilaga 4 s. 3.

att den statliga e-legitimationen bör innehålla biometriska uppgifter.[27] Enligt Polismyndigheten räcker det inte att säkerställa att e-legitimationen utfärdas till rätt individ. En innehavare kan t.ex. överlåta e-legitimationen till någon annan, som använder den utan att det kan upptäckas. En sådan överlåten e-legitimation kan också komma att användas för id-växling.

Vi gör ingen annan bedömning än Digg såvitt avser nu rådande förutsättningar. Även om frågan på intet sätt kan anses okomplicerad ser vi emellertid, mot bakgrund av det ökande problem som den identitetsrelaterade brottsligheten innebär (se avsnitt 6.7), ett behov av att möjliggöra användning av alla medel som kan bidra till att motverka missbruk av den statliga e-legitimationen. Den tekniska utvecklingen sker snabbt och även om det alltså för närvarande finns vissa svårigheter förknippade med den praktiska och tekniska användningen bör förfarandet redan nu ges stöd i lag.

Vi menar sammantaget att de nu förekommande svårigheterna inte hindrar att e-legitimationen innehåller ansiktsbild och fingeravtryck som kan användas för biometriska jämförelser. I likhet med vad som gäller för pass och nationella identitetskort ska därför den ansiktsbild och de fingeravtryck som lämnas vid ansökan om en statlig e-legitimation, lagras i chipet på bäraren av den statliga e-legitimationen. Uppgifterna kan därmed vid behov användas för att se att det är den person som den statliga e-legitimationen utfärdats till som också använder den. Att förekomsten av uppgifterna är motiverad också för att säkerställa en innehavares identitet i samband med identitetskontrollen och ur ett integritetsskyddsperspektiv utvecklas närmare i avsnitten 7.5 och 7.11.7. Att uppgifterna behöver skyddas genom tekniska säkerhetsåtgärder framgår av avsnitt 7.4.4.

En innehavare av en statlig e-legitimation ska, i likhet med det som gäller i fråga om pass och nationellt identitetskort, ha rätt att hos den identitetskotrollerande myndigheten (se avsnitt 7.6.2) kontrollera den information som har sparats i lagringsmediet (jfr 22 a § passförordningen (1979:664) respektive 20 § förordningen om nationellt identitetskort).

[27] A.a. s. 2.

7.3 Den statliga e-legitimationen bör kunna användas för att skapa kvalificerade elektroniska underskrifter

Utredningens bedömning: Den statliga e-legitimationen bör kunna användas för att skapa kvalificerade elektroniska underskrifter.

Utredningens förslag: Den statliga e-legitimationen ska finnas på en bärare som antingen är certifierad eller kan certifieras som en anordning för skapande av kvalificerade elektroniska underskrifter.

Skälen för utredningens bedömning och förslag

Den statliga e-legitimationen bör kunna användas för att framställa kvalificerade elektroniska underskrifter

Utredningen ska enligt direktiven analysera om den statliga e-legitimationen ska kunna användas för att framställa kvalificerade elektroniska underskrifter (se mer om kvalificerade elektroniska underskrifter i avsnitt 4.2.6). För att en kvalificerad elektronisk underskrift ska kunna skapas krävs ett kvalificerat certifikat och en anordning för skapande av kvalificerade elektroniska underskrifter.

2017 års ID-kortsutredning föreslog ett krav om att den av utredningen föreslagna statliga e-legitimationen skulle kunna användas för att skapa en avancerad elektronisk underskrift. Att de inte valde att föreslå att den skulle kunna användas för att skapa kvalificerade elektroniska underskrifter motiverades med att den dåvarande behovsbilden – när det gällde elektroniska underskrifter i svenska digitala tjänster – gjorde det svårt att motivera den ökade komplexitet och kostnad som följer av kraven på särskilda tekniska och säkerhetsmässiga egenskaper i e-legitimationen.[28]

Utredningen om betrodda tjänster hade i uppdrag att bl.a. tydliggöra när avancerade respektive kvalificerade elektroniska underskrifter skulle användas i den offentliga förvaltningen.[29] Utredningen konstaterade att användningen av avancerade elektroniska underskrifter i den offent-

[28] *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14), s. 336 ff.
[29] *Vem kan man lita* på? *– Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen* (SOU 2021:9).

liga förvaltningen är utbredd, medan användningen av kvalificerade elektroniska underskrifter endast förekom i begränsad omfattning.[30]

Utredningen bedömde att tre faktorer bidragit till den begränsade användningen av kvalificerade elektroniska underskrifter. Den första faktorn var att det saknades nationella författningsbestämmelser som kräver eller främjar användning av kvalificerade elektroniska underskrifter. Den andra faktorn var att den offentliga förvaltningen i stort bedömde att kraven som eIDAS-förordningen ställer på avancerade elektroniska underskrifter oftast tillgodosåg deras behov. Den sista faktorn var det begränsade utbudet och att aktörer inom förvaltningen som övervägt att använda kvalificerade elektroniska underskrifter upplevt svårigheter med att införskaffa dem.[31] Fram till oktober 2020 fanns det endast en tillhandahållare av kvalificerade betrodda tjänster i Sverige. I dagsläget finns det två.[32]

Användningen av kvalificerade elektroniska underskrifter i Sverige har inte ökat i nämnvärd omfattning sedan Utredningen om betrodda tjänster genomförde sin analys. Det går emellertid att på EU-nivå se en tydlig utveckling genom att EU-kommissionen i flera lagstiftningsförslag föreslår krav som innebär att kvalificerade elektroniska underskrifter ska användas. I förslaget till revidering av eIDAS-förordningen föreslås även att identitetsplånboken ska kunna användas för att skapa kvalificerade elektroniska underskrifter och stämplar. Det kan även noteras att bristen på tillhandahållare av kvalificerade elektroniska underskrifter har skapat problem för svenska företag när de vill lämna anbud i andra länder och det uppställs krav om att anbuden ska skrivas under med kvalificerad elektronisk underskrift. Sammantaget ser vi mot bakgrund av den nu rådande utvecklingen att behovet av användning av kvalificerade elektroniska underskrifter kommer att öka. Vi bedömer mot denna bakgrund att den statliga e-legitimationen bör kunna användas för att skapa kvalificerade elektroniska underskrifter.

[30] A.a. s. 145.
[31] A.a. s. 145ff
[32] pts.se/sv/bransch/internet/betrodda-tjanster/Lista-over-kvalificerade-tillhandahallare/ (hämtad 2023-09-23).

Hur ska en statlig e-legitimation användas för att framställa kvalificerade elektroniska underskrifter?

En statlig e-legitimation på tillitsnivå hög kan användas för att ge innehavaren möjlighet att skapa kvalificerade elektroniska underskrifter. I det följande beskrivs de tre olika sätt på vilka kvalificerade elektroniska underskrifter kan skapas med en statlig e-legitimation.

Den statliga e-legitimationen används för identifiering i en kommersiell tjänst för kvalificerade elektroniska underskrifter

Om den statliga e-legitimationen används som ett sätt att elektroniskt identifiera innehavaren för att få ett kvalificerat certifikat påverkas inte utformningen av bäraren av e-legitimationen. Det gäller under förutsättning att den kvalificerade tillhandahållaren förser den som identifierat sig med en egen anordning för framställande av kvalificerade underskrifter. Det kan ske antingen genom att användaren får ett smartkort eller genom att den kvalificerade tillhandahållaren lagrar användarens krypteringsnyckel på en server eller att denne genererar certifikat och krypteringsnycklar vid varje användningstillfälle.[33]

Detta scenario förutsätter att kommersiella aktörer ges tillgång till identifieringsinformationen och id-växlar eller använder dem vid varje tillfälle för att identifiera personen till en fristående underskriftstjänst. Scenariot påverkar inte den tekniska utformningen av den statliga e-legitimationen i någon större utsträckning, men kan påverka på vilket sätt förlitande parter ansluts och hur ersättning till den som tillhandahåller underskriftstjänsten ska se ut. Det kan vara fall där en kvalificerad tillhandahållare av betrodda tjänster använder den statliga e-legitimationen i en annan medlemsstat för att utfärda ett kvalificerat certifikat för kvalificerade elektroniska underskrifter till någon som är folkbokförd i Sverige eller som är svensk medborgare.

[33] *Vem kan man lita på? – Enkel och ändamålsenlig användning av betrodda tjänster i den offentliga förvaltningen* (SOU 2021:9) s. 72 f.

Den statliga e-legitimationen är även en anordning för att kunna skapa kvalificerade elektroniska underskrifter

Om den statliga e-legitimation även ska vara en anordning för att kunna skapa kvalificerade elektroniska underskrifter påverkas den tekniska utformningen samt den aktör som ska tillhandahålla den kvalificerade betrodda tjänsten. För att skapa kvalificerade elektroniska underskrifter behöver den som tillhandahåller tjänsten anmäla sig till tillsynsmyndigheten och genomgå en bedömning av överensstämmelse med de krav som uppställs. Tillhandahållare av tjänsten kan vara den som utfärdar den statliga e-legitimationen, en annan myndighet eller en upphandlad leverantör av tjänsten.

För att framställa en kvalificerad elektronisk underskrift krävs en anordning för skapande av kvalificerade elektroniska underskrifter. Det krävs då att bäraren av den statliga e-legitimationen antingen certifieras i enlighet med bestämmelserna i artikel 30 i eIDAS-förordningen med tillhörande genomförandebeslut[34] eller att den redan har granskats och finns i förteckningen[35] över sådana anordningar. Att granska en ny anordning tar normalt lång tid och är kostsamt, vilket gör att det går fortare att använda en redan certifierad anordning för kvalificerade elektroniska underskrifter och stämplar. De standarder som ska användas för certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter som pekas ut i genomförandeförordningen tar främst sikte på aktiva kort med kontaktchip. Den estniska informationssystemsmyndigheten RIA har emellertid efter en genomförd studie kommit fram till att ett aktivt kort – som fungerar som en anordning för att framställa kvalificerade elektroniska underskrifter – kan vara kontaktlöst. Vi menar mot den bakgrunden att den föreslagna ordningen är möjlig.[36]

Om en statlig tjänst för att skapa kvalificerade elektroniska underskrifter skulle inrättas hade det medfört krav på certifiering av såväl verksamhet som tjänst, vilket i sin tur kräver ett omfattande merarbete

[34] KOMMISSIONENS GENOMFÖRANDEBESLUT (EU) 2016/650 av den 25 april 2016 om fastställande av standarder för säkerhetsbedömning av kvalificerade anordningar för skapande av elektroniska underskrifter och stämplar enligt artiklarna 30.3 och 39.2 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

[35] Förteckningen finns här eidas.ec.europa.eu/efda/notification-tool/#/screen/browse/list/QSCD_SSCD (hämtad 2023-09-21).

[36] Analysis of the Possibility to Use ID1 Card´s NFC Interface for Authentication and Electronic Signing, Analysis Version 1.1 11th October 2022 Doc. D-26-7, www.ria.ee/media/1350/download (hämtad 2023-09-21).

som är både tidskrävande och kostsamt. Att förbereda en verksamhet för certifiering skulle troligen kräva cirka tre års förberedelsetid och därefter sex månader för certifiering. Denna kostnad bedöms vara i storleksordningen 25 miljoner kronor för anpassning av verksamheten och efterföljande certifiering. Därutöver kommer omcertifiering att behöva ske åtminstone vartannat år med en beräknad kostnad om 1,5 miljoner kronor per tillfälle.

Den statliga e-legitimationen används för att identifiera användare till en fristående kvalificerad statlig underskriftstjänst

Detta scenario liknar i stort ovanstående scenario eftersom det kräver att en kvalificerad betrodd tjänst etableras, men med skillnaden att den statliga e-legitimationen i sig inte behöver vara en anordning för skapande av kvalificerade elektroniska underskrifter. Det innebär att det utifrån detta scenario inte ställs några särskilda krav på bäraren av den statliga e-legitimationen. Däremot behöver tillhandahållaren av den fristående underskriftstjänsten anskaffa eller certifiera en anordning för skapande av kvalificerade elektroniska underskrifter.

Utformning av bäraren

Vi bedömer att den statliga e-legitimationen bör kunna användas för att framställa en kvalificerad elektronisk underskrift och att utformningen ska möjliggöra att detta kan ske på alla de sätt som finns med i redogörelsen ovan. Detta med anledning av att vi ser ett behov av att skapa förutsättningar för så stor flexibilitet som möjligt. Detta innebär att den statliga e-legitimationen ska finnas på en bärare som antingen är eller kan certifieras som en anordning för skapande av kvalificerade elektroniska underskrifter.

7.4 Tillhandahållande av den statliga e-legitimationen

7.4.1 Utgångspunkter

Utredningens förslag: En statlig myndighet ska tillhandahålla en e-legitimation på tillitsnivå hög enligt eIDAS-förordningen.

Skälen för utredningens förslag

Förslagen i revisionen av eIDAS-förordningen ställer, som redan framgått, krav på medlemsstaterna att anmäla en e-legitimation på högsta tillitsnivå enligt ett särskilt anmälningsförfarande. En anmäld e-legitimation kan därefter användas i digitala tjänster i andra EU-länder (gränsöverskridande användning).

Varken dessa förslag eller den gällande förordningen innehåller dock krav på att anmälan av e-legitimationssystem för gränsöverskridande användning ska omfatta en e-legitimation utfärdad av den anmälande medlemsstaten. Det är tillåtet att även anmäla e-legitimationer som utfärdas av privata aktörer (se avsnitt 4.2.3). I utredningsdirektiven anges emellertid att utgångspunkten är att utfärdande av e-legitimationer på den högsta tillitsnivån enligt eIDAS-förordningen bör ske av en statlig myndighet.[37] Det bör vidare beaktas att om det inte finns privata e-legitimationsalternativ som uppfyller de satta kraven, måste staten säkerställa att Sverige uppfyller sina förpliktelser (se avsnitt 6.2).

I kapitel 6 har vi redovisat brister och problem med den nuvarande situationen samt övriga behov av att staten säkerställer tillgången till en säker och tillgänglig lösning för elektronisk identifiering.

Med beaktande av problem- och behovsbilden och de redovisade utgångspunkterna för vårt uppdrag föreslås att en statlig myndighet ska tillhandahålla en e-legitimation. I enlighet med vårt uppdrag föreslås att den statliga e-legitimationen ska utfärdas på tillitsnivå hög enligt eIDAS-förordningen.

Att en statlig myndighet tillhandahåller och utformar den föreslagna e-legitimationen innebär dessutom att myndigheten har det juridiska ansvaret gentemot både innehavaren och de förlitande parterna för e-legitimationen under hela dess livslängd. Det statliga ansvaret om-

[37] Jfr uttalandet av 2017 års ID-kortsutredning: ”[b]edömningen om en viss e-legitimation bör anmälas blir enklare när det gäller en handling som utfärdas av staten”, *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14), s. 320.

fattar inte bara att säkerställa att e-legitimationen utfärdas på rätt sätt utan också den identitetskontroll som görs vid utfärdandet och vid varje användningstillfälle. Det innebär dock inte, som konstaterats av 2017 års ID-kortsutredning, att myndigheten också måste utveckla den eller hantera alla andra aspekter av den löpande förvaltningen av e-legitimationen, exempelvis användarsupport. Myndigheten kan upphandla själva handhavandet av e-legitimationen från en leverantör.[38]

Frågan om vilken myndighet som bör ges i uppdrag att utfärda en statlig e-legitimation återkommer vi till i avsnitt 7.6.

7.4.2 Till vilka och på vilket sätt ska den statliga e-legitimationen tillhandahållas?

Utredningens förslag: Den statliga e-legitimationen får tillhandahållas efter ansökan.

Personkretsen omfattar sökanden som

- antingen har ett svenskt personnummer, eller har tilldelats ett samordningsnummer för personer med styrkt identitet, som inte är förklarat vilande, och
- innevarande kalenderår är eller ska fylla nio år.

För barn under arton år krävs att barnets vårdnadshavare har lämnat skriftligt medgivande, om det inte finns synnerliga skäl att ändå utfärda ett statligt medel för elektronisk identifiering. I fråga om barn som är under arton år ska en handling som styrker uppgift om vem som är vårdnadshavare uppvisas, om denna uppgift inte framgår av den identitetskontrollerande myndighetens tillgängliga uppgifter.

Vid bifall till en ansökan ska e-legitimationen skyndsamt lämnas ut till sökanden.

En ansökan om statlig e-legitimation ska avslås, om sökanden inte uppfyller dessa krav och inte har styrkt sin identitet på föreskrivet sätt.

I lagen tas in bestämmelser om besluts överklagbarhet och verkställighet.

[38] A.a. s. 327.

Utredningens bedömning: I samband med att en ansökan om statlig e-legitimation görs, måste behov av nödvändig tillgänglighet och support tillgodoses. Vidare behövs en funktion för användarsupport i den utfärdande myndighetens verksamhet.

Skälen för utredningens förslag och bedömning

Utgångspunkter för överväganden om personkretsen för den föreslagna statliga e-legitimationen

I utredningsdirektiven anges att vi ska analysera hur en e-legitimation kan utformas så att så många som möjligt kan få tillgång till den, exempelvis personer från andra länder som arbetar eller studerar i Sverige och svenska medborgare som bor utomlands. Med beaktande härav samt behovs- och problembilden som redovisats i kapitel 6 är vår utgångspunkt att kretsen som får tillhandahållas en statlig e-legitimation bör inkludera så många som möjligt utan att kraven på en säker identifiering förbigås. Det gäller särskilt i fråga om de personer som i dagsläget har svårt att få tillgång till befintliga e-legitimationer.

Denna utgångspunkt motsvarar i stort Diggs. Enligt myndighetens förslag ska den statliga e-legitimationen tillhandahållas personer över 13 år som har personnummer eller sådant samordningsnummer där det inte råder osäkerhet om personens identitet. För den som är 16 år har föreslagits krav på godkännande av personens vårdnadshavare.[39]

Diggs förslag innebär en utvidgning av personkretsen i förhållande till förslaget från Utredningen om effektiv styrning av nationella tjänster. Den utredningens förslag omfattade svenska medborgare och de personer som är folkbokförda i Sverige.[40] Den personkretsen överensstämmer även med förslaget från 2017 års ID-kortsutredning med tillägget att den som kan tilldelas en e-legitimation ska vara minst 13 år.[41]

[39] Myndigheten för digital förvaltning, *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, s. 42–46, samt bilaga 4. Det kan för tydlighets skull tilläggas att myndighetens förslag lämnades innan lagen (2022:1697) om samordningsnummer trädde i kraft. Lydelsen av myndighetens författningsförslag (3 §) torde ha utgått från tidigare formuleringar avseende samordningsnummer i lagen (2001:182) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet, se t.ex. 2 kap. 3 § tredje stycket i dess tidigare lydelse.
[40] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 195 f. Se även avsnitt 4.7.2.
[41] *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14), s. 325 f., 333 f. och 340–342. Se även avsnitt 4.7.3.

Personnummer och samordningsnummer är de vanligaste personidentifieringsuppgifterna i Sverige för enskilda individer.[42] Det råder inte någon tvekan om att personer som är folkbokförda, och därmed har ett personnummer, ska kunna tillhandahållas en statlig e-legitimation. Med hänsyn till vår uppdragsbeskrivning bör övervägas huruvida även den som tilldelats ett samordningsnummer ska omfattas av personkretsen för den statliga e-legitimationen.

I det följande redovisar vi först översiktligt viss reglering av dessa identitetsbeteckningar och våra ställningstaganden i frågan om personkretsens avgränsning i förhållande till dessa. Därefter redovisar vi våra överväganden beträffande behov av en åldersgräns.

Personnummer

Ett personnummer är avsett att utgöra en unik identitetsbeteckning (se avsnitt 3.3). Hur det utformas och att det ska tilldelas den som uppfyller kraven för att bli folkbokförd i Sverige framgår av 18 § folkbokföringslagen (1991:481).[43] För personer som är utländska medborgare krävs, utöver bosättning i landet, som huvudregel uppehållsrätt eller uppehållstillstånd för att få vistas i Sverige (3 och 4 §§ folkbokföringslagen). Barn som föds inom landet eller, under vissa förutsättningar, utomlands, ska också folkbokföras (2 och 2 a §§ folkbokföringslagen).

En person med personnummer behåller det livet ut. När personen avlider avregistreras han eller hon och identiteten avslutas i folkbokföringsdatabasen. Även när en person flyttar från riket sker en avregistrering. Detsamma gäller för konstaterade falska identiteter. I likhet med dödsfall kommer personnumret inte längre att användas, men på samma sätt som för utflyttade individer är personnumret för den avregistrerade falska identiteten sökbar (19–22 §§ folkbokföringslagen). Personnumret och den historiska informationen som är kopplad till detta finns således kvar i folkbokföringsdatabasen.[44]

[42] Personnummer och samordningsnummer är exempel på sådana uppgifter som finns och får behandlas i folkbokföringsdatabasen, 2 kap. 2 § lagen (2021:182) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet, se även 1 kap. 2 § andra stycket lagen om samordningsnummer. Dessa identitetsbeteckningar får också ingå i det statliga personadressregistret (SPAR), om personerna har styrkt sin identitet eller gjort identiteten sannolik, 4 § lagen (1998:527) om det statliga personadressregistret, se även prop. 2007/08:58 s. 11 ff.

[43] Personnummer kan även tilldelas personer som inte ska folkbokföras. Det gäller dock bara för personer som har diplomatisk immunitet och vistas i Sverige under minst ett år, till exempel anställda vid en utländsk ambassad eller vissa internationella organisationer. Personnummer tilldelas i dessa fall på begäran av Regeringskansliet.

[44] Prop. 2017/18:145 s. 107 f.

Den som tilldelas ett personnummer har därmed en mycket stark anknytning till Sverige. Genom koppling till personnummer, i stället för att i författningen hänvisa till personer som är folkbokförda, kommer bl.a. svenska medborgare som t.ex. utflyttat kunna ansöka om den föreslagna e-legitimationen (se avsnitt 7.6.2).

I förtydligande syfte kan tilläggas att omständigheten att en individ har skyddade personuppgifter inte utgör ett hinder mot att tillhandahållas fysiska identitetshandlingar utfärdade av staten, och inte heller en kommersiell e-legitimation eller den föreslagna statliga. Detsamma gäller för personer med fingerade personuppgifter enligt lagen (2006:939) om kvalificerade skyddsidentiteter.[45]

Samordningsnummer

För att kunna tilldelas ett samordningsnummer efter egen ansökan krävs att personen i fråga har en sådan anknytning till Sverige att hon eller han kan antas behöva en identitetsbeteckning (2 kap. 1 § första stycket 2 lagen [2022:1697] om samordningsnummer). En utlänning som äger en fastighet i Sverige anges som exempel på en person med avsedd anknytning och avsett behov, vilket däremot inte anses bör vara fallet i fråga om en person som enbart har en inskrivning på Arbetsförmedlingen eller en registrerad ansökan om asyl.[46]

Personer som tilldelats ett samordningsnummer behöver således inte nödvändigtvis ha samma anknytning till landet som i Sverige bosatta personer med personnummer, men tillräcklig för att det, som tidigare anförts, bör övervägas om den förstnämnda kategorin ska ingå i personkretsen för den föreslagna statliga e-legitimationen.

På motsvarande sätt som personnummer är samordningsnummer unika. Hur samordningsnummer utformas framgår av 2 kap. 8 § lagen om samordningsnummer. Om en person med ett samordningsnummer senare blir folkbokförd ersätts samordningsnumret med ett personnummer. Individens koppling till samordningsnumret finns emellertid kvar i registret.

[45] Prop. 2005/06:149 s. 53 f.
[46] Prop. 2020/21:160 s. 54 f. Vidare anges att i regel kan inte heller den som har ett gällande avvisnings- eller utvisningsbeslut anses ha en sådan anknytning till Sverige att hon eller han kan antas ha ett behov av ett samordningsnummer. Det krävs att den enskilde kan visa på objektiva omständigheter om sin anknytning till landet som gör att det kan antas finnas ett faktiskt behov av en identitetsbeteckning vid prövningstillfället (a.a. s. 98).

Som konstaterats av bl.a. Digg, är det inte minst för personer med samordningsnummer som behovet är som störst att tillhandahålla en statlig e-legitimation (se även i avsnitt 6.6).[47] Det ska inte vara svårare för en person med samordningsnummer att tillgodogöra sig olika tjänster än för den som är folkbokförd och har personnummer.[48] En förutsättning för att tillhandahållas en statlig e-legitimation är dock, enligt vår bedömning att det är fråga om ett sådant samordningsnummer som tilldelats efter att personen i fråga har styrkt sin identitet. Därutöver bör uppställas som krav att ett sådant samordningsnummer inte får vara vilandeförklarat (3 kap. 2 § lagen om samordningsnummer).

Lagen om samordningsnummer syftar till att stärka systemet med samordningsnummer. Huvudregeln är att den som ska tilldelas ett samordningsnummer ska styrka sin identitet vid personlig inställelse hos Skatteverket genom att överlämna vissa angivna, giltiga identitetshandlingar. Verket har även rätt att kontrollera biometriska uppgifter som finns lagrade i de överlämnade handlingarna (2 kap. 2–4 §§ lagen om samordningsnummer).

Samordningsnummer ska enligt den nya lagen tilldelas i tre nivåer beroende på vilken identitetskontroll som har föregått tilldelningen. Nivåerna benämns ”styrkt identitet”, ”sannolik identitet” respektive ”osäker identitet”. Den som tar emot uppgifter om samordningsnummer ska få tydlig information om vilken bedömning av identiteten som har gjorts.

I lagens förarbeten har anförts bl.a. att den högsta nivån kommer att tilldelas efter en fullgod identitetskontroll som resulterat i att identiteten har styrkts. Identitetskontrollen kommer att motsvara den som gäller för folkbokföring efter inflyttning till landet och således utgöra ett säkert nummer.[49]

Vi bedömer av säkerhetsmässiga skäl och med beaktande av behovet av ökad tillgänglighet att det är rimligt och lämpligt att personer vilka tilldelats samordningsnummer med styrkt identitet ska kunna tillhandahållas den föreslagna e-legitimationen. Härigenom inkluderas förvisso inte alla personer som i dagsläget inte kan få en e-legitimation, men det bidrar till att minska det digitala utanförskapet. Vi anser att det vore en alltför stor säkerhetsrisk att ge en möjlighet att få en statlig

[47] Myndigheten för digital förvaltning, *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, s. 12 och 38.
[48] Prop. 2021/22:276 s. 39.
[49] A.a. s. 88.

e-legitimation till personer som har samordningsnummer tilldelat på en lägre nivå än styrkt identitet.

Invändningar mot att inkludera även personer som tilldelats samordningsnummer med styrkt identitet i personkretsen för en statlig e-legitimation har framförts av bl.a. Polismyndigheten. Det har anförts att det finns personer med samordningsnummer som medvetet kan tänkas lämna ifrån sig kontrollen över sin e-legitimation till någon som avser att använda innehavarens identitet i brottslig verksamhet. Detta förekommer redan i dag beträffande befintliga e-legitimationer. Genom att inkludera personer med samordningsnummer och svag anknytning till landet finns enligt Polismyndigheten en risk för att antalet som kan utnyttjas för detta syfte kommer att öka mångdubbelt. Risken för missbruk ligger enligt myndigheten i att personer med svag anknytning till Sverige får e-legitimationer utfärdade samtidigt som det i allt väsentligt saknas förebyggande åtgärder för att förhindra missbruk.[50]

Den nya lagen om samordningsnummer utgör en av flera vidtagna åtgärder i syfte att höja kvaliteten i Skatteverkets folkbokföringsverksamhet.[51] Skatteverket har bl.a. getts bättre förutsättningar för t.ex. identitetskontroller i samband med att samordningsnummer tilldelas. Regeringen har uttalat att en stärkt identitetskontroll där personlig inställelse är ett krav kan förväntas leda till att andelen fel i folkbokföringsdatabasen minskar och att det blir svårare att skapa och använda en falsk identitet. En stärkt kontroll förväntas också innebära en stärkt tilltro till samordningsnumret och därmed öka dess användbarhet i samhället.[52]

Det är därutöver av vikt att säkerställa att den föreslagna e-legitimationen inte bara är korrekt utfärdad för en hög tillitsnivå. Även vid dess användning bör det finnas kontrollmöjligheter. Vår bedömning är att förutsättningarna ökar för sådan kontroll genom vårt förslag att den statliga e-legitimationen ska innehålla ansiktsbild och fingeravtryck (se avsnitt 7.2.6). Sammantaget bedömer vi att samordningsnummer

[50] Myndigheten för digital förvaltning, *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, bilaga 2.
[51] Den statliga utredning som föregick genomförda reformer hade i uppdrag att bl.a. föreslå regelverk som ökar förutsättningarna för att folkbokföringen är tillförlitlig och ändamålsenlig samt lämna förslag om ett säkrare system för samordningsnummer (dir. 2019:54). Förslagen från Utredningen om folkbokföring och samordningsnummer (SOU 2021:57) har behandlats i regeringens propositioner *Stärkt kontroll och kvalitet i folkbokföringen* (prop. 2021/22:217) och *Stärkt system för samordningsnummer* (prop. 2021/22:276).
[52] Prop. 2021/22:276 s. 130.

för personer med stärkt identitet är en tillräckligt tillförlitlig identitetsbeteckning.

Av den föreslagna författningsregleringen ska således framgå att den statliga e-legitimationen kan tilldelas individer som antingen har personnummer, eller har samordningsnummer för personer med styrkt identitet, givet att det inte är vilandeförklarat (se mer om detta i avsnitt 7.5.

Ålderskrav

Vi instämmer i den bedömning som både 2017 års ID-kortsutredning och Digg gjort vad gäller behov av att uppställa ett ålderskrav.[53] Vid utredningens underhandskontakter och öppna samrådsmöten med berörda myndigheter, organisationer och leverantörer har framkommit att även barn under 13 år har ett behov av att kunna identifiera sig elektroniskt. Också bland remissinstanserna i fråga om förslagen från 2017 års ID-kortsutredning framfördes liknande synpunkter.

Från och med årskurs tre, dvs. när en elev fyller nio år, finns det ett behov av att självständigt kunna identifiera sig för att genomföra digitala nationella prov (DNP). Via en teknisk plattform som tillhandahålls av Skolverket kan både kommunala och privata skolenheter koppla in sitt befintliga inloggningssystem i DNP-systemet. Elever använder indirekt en egen e-legitimation för inloggning i systemet. Vanligtvis görs detta genom en primär inloggning till skolans eget system, vilken sker med elevens e-legitimation. Inloggning till skolans system möjliggör därefter en sekundär inloggning på den tekniska provplattformen, dvs. förfarandet utgör en id-växling. Det är därmed inte nödvändigt för eleven att vid varje provtillfälle ha med sig egen e-legitimation.

Något reellt behov av en e-legitimation tidigare än denna ålder har vi inte kunnat identifiera. Således föreslår vi att den statliga e-legitimationen ska kunna utfärdas från och med det kalenderår en individ fyller nio år. Vi ser inga risker med den föreslagna åldersnivån kopplade till *utfärdandet* av e-legitimationen. I likhet med vad som gäller i fråga om pass, nationellt identitetskort och identitetskort för folkbokförda, bör för sökande som är minderåriga uppställas krav på vårdnadshavarens

[53] *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14), s. 333 f. respektive Myndigheten för digital förvaltning, *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, s. 36 f.

skriftliga medgivande, om det inte finns synnerliga skäl att ändå utfärda en statlig e-legitimation.

De risker som kan finnas vid *användandet* av e-legitimationen kan motverkas av förlitande parter, som i varje tjänst avgör om minderåriga ska ha tillgång till tjänsten eller om vissa ålderskategorier ska sakna tillgång. Möjligheten att utesluta individer över en viss ålder i vissa tjänster har också framhållits som ett skäl för att ge minderåriga tillgång till en e-legitimation, eftersom e-legitimationen då kan användas för att motverka s.k. gromning.[54]

Ansökningsförfarande och utgivningsprocess för den statliga e-legitimationen

De tidigare nämnda utredningarna, liksom Digg, har föreslagit att en statlig e-legitimation ska tillhandahållas efter ansökan. Detta är även ett krav för tillitsnivå hög enligt eIDAS-förordningen och genomförandeförordningen (EU) 2015/1502. För den högsta tillitsnivån krävs också att utgivningsprocessen (ansökan, grundidentifiering, tillhandahållande och aktivering) delas upp i mer än ett steg, eftersom arbetsuppgifter i processen måste separeras. Det är således inte tillåtet att samtliga delar hanteras av samma handläggare; någon del av processen måste ske oberoende av handläggaren. I eIDAS-förordningens regelverk förutsätts det vara aktiveringssteget som ska säkerställa denna separation. Digg har valt att föreslå en lösning med ett sådant aktiveringsförfarande som uttryckligen föreskrivs i genomförandeförordningen.[55]

Digg har föreslagit hur en utgivningsprocess och dess olika steg skulle kunna utformas utifrån samma förutsättning som anges i våra direktiv, nämligen ett delat myndighetsansvar avseende dels utfärdandet av e-legitimationen, dels den föregående identitetskontrollen.

Förslaget innebär sammanfattningsvis följande.[56] Vid ett personligt besök på ett utgivningsställe registrerar den identitetskontrollerande myndigheten en ansökan för individen i Diggs system för e-legitimationsverksamheten samt utför grundidentifieringen och dokumenterar dess resultat. Efter att det, i Diggs tillhandahållna system för

[54] Uttryck som används för vuxna som i sexuellt syfte söker kontakt med barn och unga. Efter engelskans grooming.
[55] Se artikel 8 och avsnitt 2.1.1 i bilagan till genomförandeförordning (EU) 2015/1502.
[56] Myndigheten för digital förvaltning, *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, s. 43 ff.

den statliga e-legitimationen, har intygats att identifieringen är genomförd, prövar Digg ansökan genom ett automatiserat förfarande. Prövningen består bl.a. i att kontrollera att grundidentifieringen genomförts med ett positivt resultat och att den åberopade identiteten finns registrerad i folkbokföringsdatabasen, samt att identiteten inte är markerad som avliden, försvunnen eller falsk. Om inga hinder finns mot att utfärda e-legitimationen bifaller Digg ansökan och den identitetskontrollerande myndigheten kan genast utge e-legitimationen till sökanden, som därefter har att aktivera den.

Aktivering, som måste ske inom viss tid från utlämnandet, kan enligt Diggs förslag göras på tre olika sätt.

För det första, genom elektronisk aktivering i egen utrustning med hjälp av en av Digg tillhandahållen app. Tillvägagångssättet förutsätter en smarttelefon eller motsvarande, och ett giltigt svenskt pass eller giltigt svenskt nationellt identitetskort. För det andra kan e-legitimationen aktiveras elektroniskt i en självserviceterminal som finns i lokalen på utgivningsstället. Detta alternativ är tillgängligt för den som inte har tillgång till en smarttelefon eller motsvarande, men som innehar ett giltigt svenskt pass eller giltigt svenskt nationellt identitetskort.

Om inget av de två alternativen för aktivering skett inom 24 timmar från att kortet tillhandahölls, sänds en aktiveringskod till sökandens folkbokföringsadress eller registrerad utlandsadress, om sådan existerar (se avsnitt 7.11.5). Med koden kan aktivering ske på Diggs webbplats, antingen med hjälp av egen dator, eller via dator exempelvis på ett av Statens servicecenters kontor. Även om en aktiveringskod skickats med post till sökanden, kvarstår de föregående två aktiveringsalternativen.

Vi ansluter oss till Diggs förslag om utgivningsprocess. En fördel med förslaget är att utgivningsprocessen innebär att ansökan, grundidentifiering, utlämnade och, i förekommande fall, aktivering av den statliga e-legitimationen ska ske vid ett och samma tillfälle.

Vid sidan av de föreslagna rekvisiten om ålder och personnummer alternativt samordningsnummer för personer med styrkt identitet, måste sökanden kunna styrka sin identitet på ett tillförlitligt sätt. Det senare kravet redogör vi närmare för i avsnitt 7.5. Ansvaret för att utföra identitetskontrollen behandlas i avsnitt 7.6.

Om sökanden inte uppfyller uppställda krav ska ansökan avslås. Vid bifall ska e-legitimationen snarast lämnas ut på platsen för ansökan.

Behov av tillgänglighetsanpassningar och stöd

Vid utredningens kontakter med olika intresseorganisationer har det framförts att befintliga utgivningsställen för identitetshandlingar inte tillgodoser behov av anpassningar för personer med funktionsnedsättningar. Det har exempelvis påtalats att det redan vid kölappsautomaten saknas punktskrift eller andra hjälpmedel för att hitta fram till rätt plats i lokalen. Således behövs en översyn av de lokaler som avses att användas för ansökan och utlämnade av den statliga e-legitimationen, i syfte att tillse att dessa uppfyller kraven på erforderlig tillgänglighet.

Enligt vår bedömning kommer det största behovet av support att uppkomma i användningsskedet. Sådan support behöver anpassas efter de skilda behov som innehavarna av den statliga e-legitimationen har och kommer sannolikt att kräva telefonsupport såväl som möjligheter att besöka fysiska platser. Behovet av hjälp i den praktiska hanteringen bör utvärderas av den utfärdande myndigheten. Vi bedömer dock att denna hantering delvis kan tillgodoses genom andra åtgärder, exempelvis genom att ställföreträdare får utökade förutsättningar att bistå sina huvudmän (se avsnitt 6.6.5).

Författningsreglering

I likhet med vad som gäller ansökningsförfaranden och utgivningsprocesser hos Polismyndigheten och Skatteverket för pass och nationellt identitetskort respektive identitetskort för folkbokförda bör de centrala bestämmelserna meddelas på lagnivå.[57] Det handlar t.ex. om krav på att sökanden ska styrka sin identitet på föreskrivet sätt och att den identitetskontrollerande myndigheten har möjlighet att kontrollera sökandens uppvisade identitetshandlingar på motsvarande sätt som för bl.a. identitetskort för folkbokförda (se mer om detta i avsnitt 7.5). Sådan ytterligare detaljreglering som bedöms vara nödvändig bör finnas på förordningsnivå och i myndighetsföreskrifter, bl.a. om var ansökan ska göras och krav kopplade till sådana sökanden som är minderåriga.

Av den nya lagen bör vidare framgå att en ansökan ska avslås om rekvisiten för att tillhandahållas en statlig e-legitimation inte är uppfyllda. Vidare tas i lagen in bestämmelser om att beslut enligt lagen ska överklagas till allmän förvaltningsdomstol, att prövningstillstånd ska

[57] Det av Polismyndigheten utfärdade nationella identitetskortet är förordningsreglerat, se avsnitt 7.5.

krävas för överklagande till kammarrätten och att beslut får verkställas omedelbart, om något annat inte anges i beslutet.

Den personuppgiftsbehandling som blir aktuell för de berörda myndigheterna redovisas närmare i avsnitt 7.11. Vissa bestämmelser om personuppgiftsansvar och nödvändig personuppgiftsbehandling bör, som framgår även av avsnitt 7.1, införas i lag och kompletteras genom verkställighetsföreskrifter, såsom bestämmelsen om att vissa behövliga personuppgifter för ansökan får hämtas från Skatteverkets folkbokföringsdatabas (se avsnitt 7.11.5).

Det behov av stöd och support som vi bedömer föreligga under ansökningsförfarandet och utgivningsprocessen samt vid den statliga e-legitimationens användning förutsätter inte särskild reglering. Det finns redan tillämpliga regelverk som myndigheter har att förhålla sig till i tillgänglighetshänseende (se avsnitt 6.6.4).

7.4.3 En e-legitimation för hela samhället

Utredningens bedömning: Den statliga e-legitimationen ska kunna användas både i offentlig och privat sektor. I såväl tekniskt som rättsligt hänseende kan olika lösningar vara att föredra för respektive sektor. Det ankommer därmed på den utfärdande myndigheten att utforma och tillhandahålla nödvändiga och lämpliga tjänster åt förlitande parter och privata tjänsteleverantörer avseende dels kontroll av e-legitimationers giltighet och användare (elektronisk identitetskontroll), dels leverans av identitetsintyg efter en elektronisk identitetskontroll (utställande av identitetsintyg).

Skälen för utredningens bedömning

Enligt Diggs förslag ska den statliga e-legitimationen kunna användas i hela samhället, dvs. både i offentlig och privat sektor. Digg har föreslagit att myndigheten tillhandahåller olika tjänster åt förlitande parter och privata tjänsteleverantörer med avseende på dels kontrollerna av om använd e-legitimation är giltig och vem som har brukat den (elektronisk identitetskontroll), dels leveransen av identitetsintyg efter en elektronisk identitetskontroll (utställande av identitetsintyg).

Förslagen innebär sammanfattningsvis följande.[58]

> [e]n statlig förlitandetjänst inrättas genom vilken Digg tillhandahåller både elektroniska identitetskontroller och identitetsintyg. Utöver detta inrättas det även en statlig identifieringstjänst där Digg endast utför identitetskontroller utan att leverera identitetsintyg.
>
> Som en följd av uppdelningen i två olika tjänster behöver det rättsliga mellanhavandet konstrueras på delvis olika sätt. När den statliga förlitandetjänsten används uppkommer ett rättsförhållande direkt mellan Digg och förlitande aktör. När identitetsintygen i stället tillhandahålls av en privat leverantör av identitetsintyg uppkommer dels ett rättsförhållande mellan Digg och den privata leverantören av identitetsintyg, dels ett rättsförhållande mellan den privata leverantören och den förlitande aktör som den privata leverantören förser med identitetsintyg. För den statliga identifieringstjänsten behöver Digg bara tillhandahålla ett maskinellt gränssnitt, API75, för att verifiera användares identitet.

> [p]rivata leverantörer av identitetsintyg ska få ansluta sig till en statlig identifieringstjänst för att i sin tur ställa ut identitetsintyg i det format och på det sätt som de överenskommer om med sina respektive kundgrupper. Det blir därmed den privata leverantören av identitetsintyg som gentemot de privata förlitande aktörerna får hantera förlitandeavtal, ansvarsfrågor, ersättningar, uppföljningar och sanktioner om en förlitande aktör bryter mot uppsatta regler. Diggs roll begränsas till att kontrollera om den använda e-legitimationen är giltig och vem som har brukat den för att sedan besvara den privata leverantörens fråga om en användares identitet kan verifieras eller inte.

Digg har bedömt att den föreslagna förlitandetjänsten bör kunna omfattas av lagen (2013:311) om valfrihet i fråga om tjänster för elektronisk identifiering. Digg har vidare anfört att den statliga e-legitimationen ska ansöka om att ingå i valfrihetssystem i fråga om tjänster för elektronisk identifiering. På så sätt kan nämnda lag tillämpas för upphandlande myndigheter för att få tillgång till identifieringstjänster för den statliga e-legitimationen.

Regleringen i lagen om valfrihetssystem innebär att det är varje upphandlande myndighet som tillämpar system och tecknar avtal med leverantörerna. Digg agerar ombud och hanterar administration och avtalstecknande med stöd av fullmakter. I förarbetena till lagen om valfrihetssystem i fråga om tjänster för elektronisk identifiering anfördes att E-legitimationsnämnden (vars roll Digg numera övertagit) skulle bistå de upphandlande myndigheterna för att säkerställa att de krav på

[58] Myndigheten för digital förvaltning, *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, s. 50 ff.

leverantörerna som ställs vid anskaffningen av tjänsterna för elektronisk identifiering och de kontrakt som tecknas är förenliga med det regelverk som sätts upp.[59]

Regeringen har föreslagit att den nuvarande ombudsmodellen ska ersättas med en modell där den myndighet som regeringen bestämmer tillhandahåller auktorisationssystem för elektronisk identifiering och för digital post. Regeringen avser att utse Digg till den tillhandahållande myndigheten. I ett auktorisationssystem godkänner den tillhandahållande myndigheten att leverantörer av tjänster för elektronisk identifiering ansluter till systemet och ingår avtal om sådana tjänster med leverantörerna. Det kommer alltså inte längre vara respektive upphandlande myndighet som fattar beslut och ingår avtal med godkända leverantörer. I den tillhandahållande myndighetens uppgift ingår även att ta ut en avgift från de offentliga aktörerna och att betala ut ersättning till de godkända leverantörerna i enlighet med de villkor som ställts upp vid inrättandet av ett auktorisationssystem. Enligt regeringen framstår det som en mer ändamålsenlig och enklare modell att en och samma myndighet utför uppgiften att tillhandahålla system för de övriga statliga myndigheternas, kommunernas och regionernas räkning. Den nya lagen föreslås träda i kraft den 1 januari 2024.[60]

Vi bedömer att det finns ett behov av tjänster avseende elektronisk identitetskontroll och utställande av identitetsintyg som Digg har föreslagit. Det bör ankomma på den utfärdande myndigheten att utforma dessa på lämpligt sätt. Med beaktande av regeringens förslag om auktorisationssystem kan tilläggas att den beskrivna förlitandetjänsten kan komma att omfattas av den nya lagen om auktorisationssystem, i stället för lagen om valfrihetssystem.

[59] E-legitimationsnämnden skulle därmed svara för annonsering och utformning av förfrågningsunderlag, liksom för godkännande av och tecknande av kontrakt med de intresserade leverantörer som uppfyller de krav som ställs (prop. 2012/13:123 s. 36 f.).
[60] Prop. 2023/24:6 s. 23 och 43.

7.4.4 Säkerhetsbehov vid tillhandahållande av den statliga e-legitimationen

Utredningens bedömning: Utfärdandet och infrastrukturen för tillhandahållande av den statliga e-legitimationen kommer att behöva vara robust, uthållig och säker.

Tillhandahållaren av den statliga e-legitimationen behöver ha en väl utvecklad säkerhetskultur som arbetar med ständiga förbättringar, uppföljningar, granskningar och tester av säkerheten så att säkerheten uppdateras i takt med att hot- och risker utvecklas.

Tillhandahållandet behöver kunna ske under normala förhållanden, svåra påfrestningar, höjd beredskap och krig. Verksamheten kommer sannolikt att omfattas av regelverket kring säkerhetsskydd och tillhandahållaren behöver inledningsvis genomföra en säkerhetsskyddsanalys.

Skälen för utredningens bedömning

Av våra direktiv framgår att vi ska analysera eventuella risker för informationssäkerheten. En generell genomgång av riskbilden finns i avsnitt 6.5. I avsnitt 7.2.4 redogörs även för de skyddsåtgärder som vi bedömer krävs för att utformningen av den statliga e-legitimationen ska hantera de risker som kan uppstå. Utöver detta kommer den statliga e-legitimationen att vara en viktig infrastruktur för elektronisk identifiering av personer i Sverige. Det kommer innebära krav på att infrastrukturen och alla ingående komponenter har en hög tillgänglighet och även i övrigt väl utvecklade säkerhetsåtgärder. Det är därför viktigt att utfärdaren av den statliga e-legitimationen upprätthåller en hög nivå av informationssäkerhet med hög tillgänglighet, riktighet och konfidentialitet. Detta kräver även att utfärdaren har den finansiering som fordras för att upprätthålla denna höga nivå. Vi ser därför anledning att tydliggöra vilka åtgärder som vi bedömer att utfärdaren behöver vidta i detta avseende. Kostnaderna för åtgärderna framgår av avsnitt 9.5.

Utfärdaren bör arbeta med ett ledningssystem för informationssäkerhet. Detta är ett stöd för hur informationssäkerhetsarbetet styrs i verksamheter och ger ett systematiskt och riskbaserat arbetssätt. Ledningssystem för informationssäkerhet är svensk och internationell

standard.[61] Enligt en av standarderna i serien SS-EN ISO/IEC 27001 kan en verksamhet certifieras. Vi bedömer att utfärdaren bör sträva efter att certifieras enligt SS-EN ISO/IEC 27001 eftersom det kan medföra ökad tillit och förtroende för utfärdaren av den statliga e-legitimationen.[62]

Utfärdaren behöver utifrån ledningssystemet arbeta med förebyggande säkerhetsarbete, exempelvis riskanalyser för att prioritera och vidta rätt säkerhetsåtgärder. Arbetet behöver kompletteras med omvärldsbevakning och övervakning av tjänsterna för att hantera incidenter. Vidare behöver utfärdaren planera för att hantera mer omfattande störningar som kan inträffa, s.k. kontinuitetshantering.[63] Infrastrukturen behöver byggas robust med en hög uthållighet så att fel i avbrott i enskilda komponenter i infrastrukturen, nätverkstjänster eller system inte leder till avbrott eller störningar i utfärdandet eller möjligheten att använda de statliga e-legitimationerna.

Informationen som lagras i databasen behöver ha ett riktighetsskydd som visar om oönskade förändringar av informationen har skett. Den information som lagras och genereras behöver beakta dataminimeringsprinciper, men även skyddas under lagring, överföring och användning (se även avsnitt 7.11 om skydd av databasen).

Utfärdaren bör samarbeta med andra myndigheter som har särskild kompetens inom området informations- och cybersäkerhet och som kan bidra med råd och stöd i framtagandet av infrastrukturen, vid upphandling av drift, system och komponenter i infrastrukturen samt vid infrastrukturens vidareutveckling och förvaltning. De myndigheter som främst kan komma i fråga är de myndigheter som ingår i det nationella cybersäkerhetscentret.[64] I utfärdarens säkerhetsarbete kopplat till riskanalyser och säkerhetsåtgärder behöver även underleverantörer och deras eventuella underleverantörer ingå, i syfte att upprätthålla nödvändig säkerhet i hela systemet.

[61] Övergripande består ISO 27000-serien av två olika typer av standarder: Ledningssystemstandarder för att stödja ett systematisk arbetssätt. Dessa har likheter med andra ledningssystemstandarder såsom ISO 9001 – Kvalitetsledning, och ISO 14000 – Miljöledning och vägledningsstandarder för säkerhetsåtgärder för att skydda informationen.
[62] Om ISO 27000 och certifiering enligt SS-EN ISO/IEC 27001:2023, www.sis.se/iso27001/dettariso27001/ (hämtad 2023-09-22).
[63] Kontinuitetshantering handlar om att planera för att upprätthålla sin verksamhet på en tolerabel nivå. Oavsett vilken störning den utsätts för. www.msb.se/sv/amnesomraden/krisberedskap-civilt-forsvar/samhallsviktig-verksamhet/kontinuitetshantering/ (hämtad 2023-09-22).
[64] Försvarets radioanstalt, Försvarsmakten, Myndigheten för samhällsskydd och beredskap och Säkerhetspolisen har inrättat ett nationellt cybersäkerhetscenter på uppdrag av regeringen. Arbetet görs i nära samverkan med Post- och telestyrelsen, Polismyndigheten och Försvarets materielverk.

Organisatoriska säkerhetsåtgärder i form av riktlinjer, processer och rutiner behöver införas för dem som arbetar med och i utfärdandet av den statliga e-legitimationen. Syftet är att undvika personberoenden vilket också motiverar att vissa kritiska moment bör utföras av minst två personer tillsammans. Därutöver bör kontroller genomföras, t.ex. i samband med beslutsprocesser inför förändringar i komponenter och system. Detta görs för att undvika risken att en enskild medarbetare av misstag eller illvilja påverkar säkerheten i hela infrastrukturen.

Uppföljning och tester bör ske genom återkommande säkerhetsgranskningar, revisioner och penetrationstester. Sådana granskningar kan ske genom stöd från myndigheter med särskilt kompetens på området, men det kan även upphandlas på marknaden.

Utfärdaren behöver även vidta tekniska säkerhetsåtgärder som kryptering, digitala signaturer, stämplar och andra skydd.

Utfärdaren kommer att behöva hantera säkerhetsskyddsklassificerad information och verksamheten i sig själv kommer sannolikt att omfattas av säkerhetsskyddslagen. Vidare kan förlitande parter tänkas vilja teckna säkerhetsskyddsavtal med utfärdaren.

I samband med anskaffning av driftstjänster kan det även bli aktuellt för den som tillhandahåller e-legitimationen att teckna säkerhetsskyddsavtal. Säkerhetsskyddsanalys och vidare överväganden i enlighet med säkerhetsskyddsregleringen behöver därför göras av utfärdaren av den statliga e-legitimationen.

Den statliga e-legitimationen kan därtill komma att bli viktig ur ett totalförsvarsperspektiv. Det innebär att utfärdaren av den statliga e-legitimationen kan behöva planera för och ta i anspråk anställda för totalförsvarsbehov i händelse av höjd beredskap eller krig samt vidta övriga åtgärder som krävs för att säkerställa ett uthålligt tillhandahållande av den statliga e-legitimationen.

7.5 Grundidentifiering

Utredningens förslag: Innan en statlig e-legitimation får utfärdas krävs att sökanden har styrkt sin identitet.

En sökande som vid identitetskontrollen överlämnar pass, identitetskort eller motsvarande handling som är försedd med innehavarens ansiktsbild, eller som innehåller ett lagringsmedium med

ansiktsbild och fingeravtryck, ska vara skyldig att på begäran låta den myndighet som utför identitetskontrollen ta hans eller hennes fingeravtryck och en ansiktsbild i digitalt format för kontroll av att dessa motsvarar dem som finns på eller är lagrade i handlingen.

Regeringen eller den myndighet som regeringen bestämmer ska ges rätt att meddela föreskrifter om undantag från skyldigheten att låta den myndighet som utför identitetskontrollen ta fingeravtryck och ansiktsbild. I den nya lagen ska införas en upplysningsbestämmelse om att regeringen eller den myndighet regeringen bestämmer får meddela de föreskrifter som behövs för verkställigheten av kontrollen att en sökande har styrkt sin identitet.

Skälen för utredningens förslag

Utgångspunkter för våra överväganden

Enligt kommittédirektiven ska vi analysera vilka kontroller av identiteten som behöver vidtas och om omfattningen av kontrollen ska vara jämförbar med den kontroll som sker för andra identitetshandlingar.

Vi ska för våra överväganden beakta de förslag som Digg har lämnat och de synpunkter som framkommit inom ramen för myndighetens regeringsuppdrag.

Som tidigare redovisats innebär den av Digg föreslagna utgivningsprocessen för en statlig e-legitimation ett delat myndighetsansvar på så vis att grundidentifieringen av sökanden utförs av en annan, identitetskontrollerande myndighet (se avsnitt 7.4.2). Sökanden ska styrka sin identitet i enlighet med de rutiner och krav som den identitetskontrollerande myndigheten enligt förslaget ska få föreskriva.[65] Digg har vidare konstaterat att kraven i avsnitt 2.1.1 (Ansökan och registrering) i bilagan till kommissionens genomförandeförordning (EU) 2015/1502 måste beaktas vid den närmare utformningen av ansökningsprocessen.[66]

Utifrån uppdragsbeskrivningen i våra direktiv och de utgångspunkter som ska beaktas har vi, som framgått, anslutit oss till Diggs förslag om ansökningsförfarande och utgivningsprocess (avsnitt 7.4.2, se även avsnitt 7.6.2 om ansvaret för grundidentifieringen).

[65] Myndigheten för digital förvaltning, *En säker och tillgänglig digital identitet – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, s. 42 ff. samt bilaga 4.
[66] Ibid.

Den hänvisade bilagan till genomförandeförordningen (EU) 2015/1502 innehåller tekniska specifikationer och förfaranden för tillitsnivåerna låg, väsentlig och hög avseende de medel för elektronisk identifiering (dvs. en e-legitimation) som utfärdats inom ramen för ett anmält system för elektronisk identifiering.

I avsnitt 2.1.1 i bilagan uppställs, för samtliga tillitsnivåer, krav på att (i) säkerställa att den sökande är medveten om villkoren förenade med användningen av medlet för elektronisk identifiering, (ii) säkerställa att den sökande är medveten om rekommenderade säkerhetsåtgärder kopplade till medlet för elektronisk identifiering, och (iii) samla in de relevanta identitetsuppgifter som krävs för styrkande och kontroll av identitet.

Beträffande relevanta uppgifter för identitetskontrollen föreslår Digg uttryckligen att personnummer alternativt samordningsnummer ska omfattas av kontrollen. Det anges inte i detalj hur grundidentifieringen ska genomföras utan föreslås att sökanden styrker sin identitet i enlighet med de rutiner och krav som föreskrivits av den identitetskontrollerande myndigheten. I anslutning till beskrivningen av utgivningsprocessen uttalas vidare att med grundidentifiering avses i sammanhanget ”att kontrollera att en sökandes identitet är styrkt” och att begreppsanvändningen ”ansluter väl till nuvarande regler inom området, exempelvis Polismyndighetens föreskrifter för pass och nationellt identitetskort”.[67]

Identitetskontroller för vissa befintliga identitetshandlingar samt vid registrering i folkbokföringsdatabasen och ärenden om medborgarskap

För våra överväganden om vilka kontroller av identiteten som behöver vidtas vid utfärdandet av en statlig e-legitimation redovisas här kortfattat de identitetskontroller som görs av Polismyndigheten, Skatteverket och Migrationsverket i fråga om allmänt accepterade identitetshandlingar samt vid prövning av ansökan för medborgarskap. Den identitetskontroll som görs vid tilldelning av samordningsnummer har berörts i avsnitt 7.4.2. För en utförlig redogörelse, som inkluderar exempelvis körkort hänvisas till 2017 års ID-kortsutredning.[68]

[67] Myndigheten för digital förvaltning, *En säker och tillgänglig digital identitet – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, s. 42.
[68] *Ett säkert och statligt ID-kort – med e-legitimation* (SOU 2019:14), s. 107 ff.

Beviskravet styrkt identitet används såväl vid ansökan om pass och nationellt identitetskort som vid ansökan hos Skatteverket om identitetskort för folkbokförda i Sverige och i samband med ansökan hos Migrationsverket om svenskt medborgarskap. Även för den som – oavsett medborgarskap – ska lämna en anmälan om inflyttning från utlandet uppställs krav på personlig inställelse hos Skatteverket för identitetskontroll. Detsamma gäller i fråga om en anmälan enligt samma paragraf av bl.a. den som är avregistrerad som försvunnen och ska folkbokföras (26 och 26 a §§ folkbokföringslagen).[69]

Bestämmelserna om pass och nationellt identitetskort regleras i passlagen och passförordningen respektive förordning om nationellt identitetskort.[70]

Pass och nationellt identitetskort, som utfärdas av Polismyndigheten och enbart till svenska medborgare, är de enda giltiga dokument som styrker både identitet och medborgarskap.[71] I motsats till andra identitetshandlingar gäller pass och nationellt identitetskort som resehandling till alla länder (pass) respektive inom Schengenområdet (nationellt identitetskort). Till skillnad från vissa andra länder uppställs i Sverige inget krav på att vare sig medborgare eller personer som vistas i landet ska ha ett nationellt identitetskort.[72]

Oavsett om det är fråga om en ansökan om pass eller nationellt identitetskort måste alltså sökanden inställa sig personligen. Sökanden måste i samband med ansökan styrka sin identitet, sitt svenska medborgarskap och övriga personuppgifter (6 § passlagen respektive 2 och 3 §§ förordningen om nationellt identitetskort). Identiteten kan styrkas på de sätt som anges i 3 kap. 2 och 3 §§ PMFS 2019:3 FAP 530-1.

Det vanligaste sättet att styrka sin identitet är genom uppvisande av en giltig identitetshandling, vilket för nämnda identitetshandlingar innebär ett giltigt (i) svenskt vanligt eller extra pass, (ii) nationellt identitetskort, (iii) svenskt körkort, (iv) svenskt SIS-märkt identitetskort, eller (v) identitetskort för folkbokförda i Sverige. Om det inte är möj-

[69] Av 26 § andra stycket framgår att kravet på personlig inställelse inte gäller anmälan för barn som ska folkbokföras här i landet enligt 2 a § eller 3 § tredje stycket folkbokföringslagen, se prop. 2021/22:217 s. 37 och Skatteverkets rättsliga vägledning, www4.skatteverket.se/rattsligvagledning/edition/2023.8/330375.html (hämtad 2023-08-04).

[70] Regleringen kompletteras med Polismyndighetens föreskrifter och allmänna råd om pass och nationellt identitetskort PMFS 2021:3 FAP 530–1.

[71] Pass och nationellt identitetskort får utfärdas utom riket av utlandsmyndigheter, se 2 § tredje stycket passlagen och 3 kap. förordningen (2014:115) med instruktion för utrikesrepresentationen.

[72] Se dock 2 kap. 1 och 1 a §§ utlänningslagen (2005:716) samt 2 kap. 1–3 §§ utlänningsförordningen (2006:97).

ligt kan vissa kategorier av anhöriga, vissa företrädare och arbetsgivare skriftligen försäkra att sökandens uppgifter om identiteten är korrekta. Den som lämnar en sådan försäkran måste vara närvarande vid identitetskontrollen och kunna styrka sin egen identitet genom någon av de identitetshandlingar som godtas (3 kap. 5 § nämnda föreskrifter). Om sökanden inte kan styrka sin identitet vare sig genom en identitetshandling eller genom någon annans försäkran, får Polismyndigheten godta att identiteten styrks på något annat tillförlitligt sätt (3 kap. 4 § nämnda föreskrifter). Polismyndigheten ska kontrollera identiteten noggrant (3 kap. 1 § nämnda föreskrifter).

I likhet med vad som gäller för pass och nationella identitetskort ska sökanden av ett identitetskort för folkbokförda i Sverige styrka sin identitet genom att i första hand uppvisa en godtagbar identitetshandling (2 § lagen om identitetskort för folkbokförda i Sverige och 3 § Skatteverkets föreskrifter om identitetskort, SKVFS 2009:14).[73] Om sökanden inte har en godtagbar identitetshandling finns det, på samma sätt som i pass- och id-kortsärenden hos Polismyndigheten, ett intygsförfarande (3 och 5 §§ nämnda föreskrifter). Likaså har Skatteverket möjlighet att göra en sammanvägd bedömning av åberopade handlingar för de fall sökanden inte kan styrka sin identitet och övriga personuppgifter på något av tidigare angivna sätt. Med godtagbar identitetshandling avses, enligt 4 § samma föreskrifter, ett giltigt: (i) identitetskort utfärdat av Skatteverket, (ii) vanligt svenskt pass, (iii) svenskt nationellt identitetskort, (iv) svenskt körkort, (v) svenskt tjänstekort utfärdat av statlig myndighet, (vi) SIS-märkt företagskort, tjänstekort eller identitetskort, (vii) EU-pass utfärdat från och med den 1 september 2006, (viii) pass utfärdat av Island, Liechtenstein, Norge eller Schweiz från och med den 1 september 2006, eller (ix) nationellt identitetskort för EU-medborgare utfärdat från och med den 2 augusti 2021.

Om sökanden har uppehållstillstånd i Sverige ska han eller hon enligt 3 § lagen om identitetskort för folkbokförda i Sverige anses ha styrkt sin identitet om de uppgifter som lämnas i ansökan om identitetskort stämmer överens med vad som har registrerats i fråga om uppehållstillståndet. Identiteten ska dock inte anses styrkt på detta sätt om särskilda skäl talar emot det.

I förarbetena till de nya bestämmelserna i 26 a och 26 b §§ folkbokföringslagen uttalades bl.a. att den identitetskontroll som sker före folkbokföring är av stor betydelse för att motverka att oriktiga

[73] Ändringar i grundförfattningen har gjorts genom SKVFS 2019:5 och SKVFS 2021:9.

uppgifter registreras i folkbokföringsdatabasen. När en person väl har folkbokförts, sprids uppgifterna i samhället. Vidare konstaterades att identitetshandlingar spelar en avgörande roll vid Skatteverkets identitetskontroller, eftersom handlingarna innehåller, om de utfärdats på ett säkert sätt, de uppgifter om en person som behövs för att fastställa hans eller hennes identitet. Genom lagändringen är en enskild skyldig att på begäran överlämna pass, identitetskort eller motsvarande handling.[74] Med motsvarande handling avses framför allt handlingar som används i stället för pass och för vilka det finns särskilda standarder och krav som innebär att handlingen utgör ett säkert verktyg för identifiering, som t.ex. främlingspass och resedokument.[75] Den som har beviljats uppehållstillstånd i Sverige ska på begäran också överlämna sitt uppehållstillståndskort för kontroll.

Även för beslut om medborgarskap efter ansökan (naturalisation) förutsätts att sökanden har styrkt sin identitet (11 § lagen [2001:82] om svenskt medborgarskap).[76]

För att identiteten ska anses vara styrkt krävs att det råder klarhet om sökandens namn, ålder och, som huvudregel, medborgarskap. I förarbetena anfördes bl.a. följande vad gäller identitetskontrollen.[77]

> Utgångspunkten är att sökanden, för att anses ha styrkt sin identitet på ett godtagbart sätt, skall kunna förete ett hemlandspass i original eller en fotoförsedd identitetshandling i original utfärdad av behörig myndighet i hemlandet, allt under förutsättning att äktheten inte kan sättas i fråga. Om sökanden har varit fast bosatt i ett annat land än hemlandet, kan en sådan handling utfärdad i den staten godtas. Som riktmärke gäller att handlingarna skall vara tillförlitliga och utfärdade på ett ur identitetssynpunkt tillfredsställande sätt. Härav följer bl.a. att handlingen inte får vara av alltför enkel beskaffenhet. I princip är kravnivån avseende bevisningen densamma oavsett vilket ursprungsland handlingarna härrör från. Emellertid ställs mindre långtgående krav på den rent tekniska utformningen av en handling som utfärdats i ett utvecklingsland jämfört med vad som gäller för handlingar som utfärdats i t.ex. Västeuropa.
>
> Även om sökanden inte kan förete handlingar som är tillräckliga för att uppfylla beviskravet, kan identiteten till följd av principen om fri bevisprövning anses vara styrkt i vissa fall. Det krävs då att det i ärendet, utöver de åberopade handlingarna, föreligger ytterligare omständigheter som ger ett starkt och otvetydigt stöd för den av sökanden uppgivna identiteten.

[74] Prop. 2021/22:217 s. 37 ff.
[75] A.a. s. 68.
[76] Ärenden om medborgaskap handläggs vid två enheter inom Migrationsverket (i Göteborg och Norrköping), se www.migrationsverket.se/Privatpersoner/Bli-svensk-medborgare/Vanliga-fragor-och-svar-om-svenskt-medborgarskap.html (hämtad 23-05-29).
[77] Prop. 1997/98:178 s. 8.

> En eller flera var för sig otillräckliga handlingar kan sammantagna med övriga omständigheter således anses utgöra tillräcklig bevisning. Även uppgifter från nära anhöriga kan åberopas.

Krav på grundidentifiering enligt tidigare genomförda utredningar

Enligt vad som anförts av Utredningen om effektiv styrning av nationella digitala tjänster är ett förfarande som leder fram till en identitetshandling en process som innefattar grundidentifiering, förutsatt att det i processen ingår *att* sökanden ska inställa sig personligen hos utfärdaren vid ansökan om, såväl som utlämnandet av, identitetshandlingen, *att* sökanden ska styrka sin identitet på ett tillförlitligt sätt, och *att* utfärdaren dokumenterar fysiska kännetecken av sökanden, åtminstone ett fotografi (se även avsnitt 3.7).

Utredningen om effektiv styrning av nationella digitala tjänster konstaterade också att Polismyndigheten och Skatteverket är de myndigheter som vid den aktuella tidpunkten utfärdade identitetshandlingar i enlighet med angivna principer. Som redovisas i avsnitt 4.7.2 lämnade utredningen inget förslag om vilken av dessa myndigheter som borde ges i uppdrag att utfärda en statlig e-legitimation med hänvisning till uppdraget för 2017 års ID-kortsutredning, vars arbete pågick parallellt. Däremot föreslogs att den statliga elektroniska identitetshandlingen borde dela grundidentifieringsprocess med en fysisk identitetshandling och författningsförslagen utarbetades med förlaga från liknande bestämmelser avseende sådana identitetshandlingar.[78]

Också 2017 års ID-kortsutredning föreslog att ansökningsförfarandet för en statlig e-legitimation skulle följa processen för ansökan om ett fysiskt statligt identitetskort, och att Polismyndigheten skulle utses som utfärdare av även e-legitimationen (se mer om detta i avsnitt 4.7.3). I motsats till förslaget som lämnades av Utredningen om effektiv styrning av nationella digitala tjänster föreslog 2017 års ID-kortsutredning inte något absolut krav på personlig inställelse vid ansökan och anförde att identifiering borde kunna ske också genom ombud och med ett intygsförfarande.[79]

Utredningen ansåg nämligen att det svenska tillitsramverkets krav på identitetskontroll vid personligt besök, på likvärdigt sätt som vid utgivning av en fysisk identitetshandling, borde tolkas mot bakgrund

[78] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114) s. 173 ff..
[79] *Ett säkert och statligt ID-kort – med e-legitimation* (SOU 2019:14) s. 326 ff. och s. 340 ff.

av vad som anges i avsnitt 2.1.2 i bilagan till genomförandeförordningen (EU) 2015/1502. Enligt det hänvisade avsnittet är ett möjligt sätt att uppfylla kraven på tillitsnivå hög att tillämpa samma förfaranden som används på nationell nivå i medlemsstaten av den enhet som ansvarar för registreringen för att erhålla ett erkänt fotografiskt eller biometriskt identifieringsbevis. Eftersom ansökan om den statliga e-legitimationen föreslogs ske just enligt samma förfarande som vid utfärdande av en fullgod, fysisk identitetshandling, ansågs en ansökan även genom bud vara förenlig med eIDAS-förordningen.[80]

Omfattningen av identitetskontrollen för en statlig e-legitimation

De redovisade utredningarnas förslag om ansökningsprocess bygger alltså på att den statliga e-legitimationen har det nationella identitetskortet som fysisk bärare och att utfärdandet sker med stöd av samma identifieringsprocess. Som framgår av avsnitt 7.6.1 gör även vi bedömningen att det är en lämplig ordning.

Enligt vad som framgår av avsnitt 7.6.3 föreslår vi dock, utifrån förutsättningarna för vårt uppdrag, ett uppdelat myndighetsansvar, och att det är Digg som ska utfärda den statliga e-legitimationen. I avsnitt 7.6.2 föreslås att den myndighet regeringen bestämmer ska ges i uppdrag att kontrollera att sökanden kan styrka sin identitet (identitetskontrollerande myndighet). Den statliga e-legitimationen kommer som framgått, i vart fall inte inledningsvis, att utfärdas på någon befintlig statlig fysisk identitetshandling (se avsnitt 7.2.2).

Det blir därmed inte aktuellt med en gemensam identifieringsprocess för statliga fysiska och elektroniska identitetshandlingar. Att vår uppdragsbeskrivning inte gör det möjligt att lämna ett sådant förslag medför, enligt vår bedömning, att det är oförenligt med kraven enligt eIDAS-regelverket att tillåta att ansökan om den föreslagna e-legitimationen görs genom ombud. Personlig inställelse är därmed en förutsättning för att ansöka om den statliga e-legitimationen.

I likhet med de tidigare utredningarnas och Diggs förslag bör det krävas att sökanden på ett tillförlitligt sätt styrker sin identitet för att den statliga e-legitimationen ska kunna utfärdas.

Av samma skäl som anfördes av regeringen i bl.a. lagstiftningsärendet för stärkt system för samordningsnummer, och på samma sätt

[80] A.a. s. 342.

som föreskrivs i den nya regleringen av detsamma, bör det vara en skyldighet för en sökande av statlig e-legitimation som inställer sig personligen för identitetskontroll att på begäran överlämna pass, identitetskort eller annan motsvarande handling eller uppehållstillståndskort för kontroll.

Vad gäller pass och identitetskort är det handlingar som i regel är försedda med fotografi av innehavarens ansikte och kan ha ett lagringsmedium (chip) där ansiktsbild eller fingeravtryck finns lagrade.[81] Den identitetskontrollerande myndigheten ska ha möjlighet att kontrollera de biometriska uppgifter som kan hämtas ur ansiktsbilden eller fingeravtrycken som finns lagrade i den uppvisade identitetshandlingen och jämföra dessa med de biometriska uppgifter som kan hämtas från bilden och fingeravtrycken som vi föreslår ska tas av sökanden. Genom en sådan kontroll kan det säkerställas att den handling som visas upp är äkta och att den är utställd på den person som överlämnar den.

Om ett lagringsmedium med sådana uppgifter är förstört bör det, enligt vår uppfattning, också vara tillåtet att göra maskinella jämförelser av fotografiet på uppvisad identitetshandling. Detsamma bör gälla i de fall sökandens identitetshandling saknar ett lagringsmedium och enbart är försedd med ett fotografi. Enligt vad utredningen erfarit är en sådan maskinell jämförelse något som är tekniskt genomförbart. Vad gäller fingeravtryck kan tilläggas att dessa vanligtvis är krypterade på ett sådant sätt att de endast kan kontrolläsas efter avtal med utfärdande land. Till skillnad från svenska resehandlingar, identitetskort och uppehållstillståndskort krävs därmed bilaterala avtal med varje enskilt land. Polismyndigheten, men inte Skatteverket, har ingått sådana avtal.

Den enskilde bör således vara skyldig att på begäran låta myndigheten som utför identitetskontrollen ta fingeravtryck och en ansiktsbild i digitalt format för att myndigheten ska kunna kontrollera att dessa stämmer överens med ansiktsbild eller fingeravtryck som, i förekommande fall, finns på eller lagrade i den uppvisade handlingen. Syftet med denna kontroll är alltså att säkerställa handlingens äkthet och innehavarens identitet.[82]

I tidigare nämnda lagstiftningsärende för stärkt system för samordningsnummer anfördes vidare att det kan finnas anledning att göra vissa undantag från skyldigheten att låta sig fotograferas och lämna

[81] Se t.ex. prop. 2021/22:276 s. 65.
[82] Prop. 2021/22:276 s. 64 f.

fingeravtryck. Det kan t.ex. handla om att barn under en viss ålder och personer som har vissa fysiska hinder inte behöver lämna fingeravtryck.[83]

Sådana undantag bör, i likhet med vad som gäller enligt t.ex. den nya lagen om samordningsnummer, regleras i förordning, med stöd av ett föreskriftsbemyndigande. Beträffande undantag från att lämna fingeravtryck på grund av fysiska hinder och ålder bör regleringen av den statliga e-legitimationen utformas på motsvarande sätt som de för pass och nationella identitetskort. Enligt 2 § passförordningen, som är meddelad med stöd av föreskriftsbemyndigandet i 6 § tredje stycket passlagen, görs undantag för barn under sex år. Detsamma gäller enligt 3 § tredje stycket förordningen om nationellt identitetskort. Eftersom vi föreslår att den statliga e-legitimationen ska tillhandahållas personer från och med det kalenderår de fyller nio år, kan dock en undantagsbestämmelse i förordningsform inte gälla för barn under den åldern.

Även övriga bestämmelser som närmare anger på vilket sätt identiteten ska styrkas bör regleras i förordning eller myndighetsföreskrifter, som lämpligen utformas med befintliga regler om identitetskontroll som förebild (se mer om författningsreglering och normgivningsnivåer även i avsnitt 7.1). Vid utformningen av dessa bestämmelser måste kraven i eIDAS-förordningen beaktas.[84]

Som framgått innebär vårt förslag att en statlig e-legitimation ska kunna utfärdas till den som antingen har svenskt personnummer eller har tilldelats samordningsnummer för personer med styrkt identitet (se avsnitt 7.4.2). Ett påtalat problem vad gäller den sistnämnda identitetsbeteckningen är att det i dagsläget saknas möjlighet för personer med tilldelat samordningsnummer att ansöka och få Skatteverkets identitetskort för folkbokförda i Sverige. För utländska medborgare är det inte heller möjligt att tillhandahållas nationellt identitetskort. Det har, bl.a. av Svenska Bankföreningen, anförts att utan en fysisk identitetshandling som kopplar samman individen med det tilldelade samordningsnumret finns det inget som styrker att just den personen har rätt att använda det ifrågavarande samordningsnumret. Svenska Bankföreningen har hemställt om en ändring i lagen om identitetskort för folkbokförda i syfte att möjliggöra att även personer som tilldelats sam-

[83] A.a. s. 66 f.

[84] Som konstaterats i andra sammanhang ställs högre krav på nivå 4 enligt det svenska tillitsramverket än nivå hög enligt eIDAS-förordningen och genomförandeförordningen (EU) 2015/1502, (t.ex.) vad gäller krav på personlig inställelse vid styrkande och kontroll av identitet. se bl.a. *Användning av e-legitimation i tjänsten i den offentliga förvaltningen* (SOU 2021:62) s. 173 f.

ordningsnummer med styrkt identitet ska kunna få ett sådant identitetskort.[85]

Vi delar uppfattningen att det finns ett behov av att överväga en sådan möjlighet, men det ligger utanför vårt uppdrag. Med anledning av det anförda kan dock tilläggas att det i folkbokföringsdatabasen får behandlas uppgift om på vilken nivå samordningsnumret har tilldelats beroende på vilken identitetskontroll som föregått tilldelningen eller senaste förnyelsen av numret. Detsamma gäller för uppgift om vilandeförklaring. Detta framgår av 2 kap. 3 § första och tredje styckena lagen (2001:182) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet. Myndigheter som hämtar information via Navet kan därmed få de uppgifter om personens identitet som kopplas till numret, inbegripet vilka handlingar som individen har uppvisat vid identitetskontrollen.[86] Skatteverket har möjlighet att medge sådan direktåtkomst till sistnämnda uppgifter om handlingar och grunden för tilldelningsbeslut, för det fall en annan myndighet behöver uppgifterna för att fullgöra sitt uppdrag och får behandla dem (2 kap. 8 § nyss nämnda lag).

För samordningsnummer som vilandeförklarats aviseras visserligen inte identitetsnivån. Som framgått innebär dock vårt förslag inte bara att det ska vara fråga om samordningsnummer som tilldelas personer med styrkt identitet; det krävs därutöver att ett sådant nummer inte får ha förklarats vilande (se avsnitt 7.4.2). Härigenom kan det säkerställas att den identitetskontrollerande myndigheten får information från folkbokföringsdatabasen om vilken bedömning av identiteten som föregått tilldelningen eller senaste förnyelsen av numret samt vilka handlingar som ligger till grund för detta. Myndigheten kan därmed avgöra om den i sin verksamhet behöver vidta ytterligare åtgärder för att kontrollera de uppgifter som angetts. Aktörer får således ett bättre underlag för beslut och åtgärder.

En grundidentifiering som inkluderar personlig inställelse för att ta ansiktsbild, fingeravtryck och göra vederbörliga datorstödda jämförelser med motsvarigheter på sökandens identitetshandling är en avgörande faktor för att skapa förutsättningar för en säker och tillförlitlig

[85] Svenska Bankföreningens framställan 2023-06-19 till Justitiedepartementet och Finansdepartementet (föreningens diarienr 2023-06-006).
[86] Navet utgör ett delsystem i folkbokföringsdatabasen och får i första hand användas för aktualisering, komplettering och kontroll av personuppgifter. Större delen av utlämnandet av uppgifter sker genom utskick (avisering) efter beställningar från statliga myndigheter, kommuner och regioner, se t.ex. prop. 2021/22:276 s. 87.

statlig e-legitimation. Personlig inställelse för sökanden möjliggör dessutom att en utgivningsprocess genom vilken ansökan, utlämnande och, i förekommande fall även, aktivering av e-legitimationen kan ske vid ett och samma tillfälle, oaktat den föreslagna ansvarsuppdelning myndigheterna emellan (se avsnitt 7.6).

Att bäraren för e-legitimationen föreslås innehålla ett lagringsmedium för ansiktsbild och fingeravtryck som tagits (se avsnitt 7.2.6) innebär en dokumentation av fysiska kännetecken hos sökanden. Det föreslagna förfarandet som, förutsatt att ansökan bifalls, leder fram till en identitetshandling utgör således en process som innefattar grundidentifiering i enlighet med de ovan redovisade principer som förordats av Utredningen om effektiv styrning av nationella tjänster.

7.6 Ansvar för grundidentifiering och utfärdande

7.6.1 En sammanhållen grundidentifiering för fysiska och elektroniska identitetshandlingar

Utredningens bedömning: En myndighet bör ha det huvudsakliga ansvaret för grundidentifiering som sker inför utfärdande av såväl en statlig e-legitimation som statliga fysiska identitetshandlingar.

Skälen för utredningens bedömning

Grundidentifiering, som behandlas i avsnitt 7.5, är en avgörande faktor för att skapa förutsättningar för en säker och tillförlitlig statlig e-legitimation.[87]

Utifrån ramarna för vårt uppdrag föreslår vi att den statliga e-legitimationen ska finnas på ett kontaktlöst kort. Samtidigt gör vi bedömningen att e-legitimationen så snart som möjligt ska finnas även på ett statligt utfärdat identitetskort. Att separera den grundidentifiering som sker vid utfärdande av fysiska statliga legitimationshandlingar från den som genomförs innan en e-legitimation utfärdas framstår – särskilt vid en sådan sammanhållen hantering – av såväl praktiska som säkerhetsmässiga skäl, inte lämpligt.

[87] Se även avsnitt 6.7.8 för vidare resonemang kring betydelsen för att motverka identitetsrelaterad brottslighet.

2017 års ID-kortsutredning föreslog en begränsning av dels antalet fysiska identitetshandlingar, dels antalet utfärdare av identitetshandlingar. Enligt utredningen medförde de skilda utfärdandeprocesserna, liksom att olika krav ställdes på ansökan, bakgrundskontroll av sökanden, tillverkning och utlämnande att de identitetshandlingar som fanns var av skiftande kvalitet och såg olika ut. Enligt utredningens bedömning försvårade detta för den som skulle kontrollera handlingarnas giltighet och äkthet vilket i sin tur utgjorde en risk för ökad identitetsrelaterad brottslighet.[88]

Vi instämmer i den bedömningen och anser att motsvarande omständigheter gör sig gällande i fråga om vikten av att en och samma myndighet ansvarar för att utföra grundidentifieringen inför utfärdande av de fysiska identitetshandlingar som tillhandahålls av staten såväl som en statlig e-legitimation. En sådan ordning kan bidra till att skapa enhetliga rutiner, effektiv hantering och tydlighet för befolkningen. Enligt vår uppfattning skulle det också bidra till att tydliggöra att en e-legitimation är en värdehandling att jämställa med fysiska identitetshandlingar.

Vikten av en sammanhållen hantering av grundidentifieringen har påpekats av i princip samtliga de organisationer, myndigheter och leverantörer som utredningen har talat med. Därutöver har såväl Skatteverket som Försäkringskassan, genom sina i utredningen medverkande experter, i särskilda yttranden framhållit behovet av ett samlat grepp för hela identitetskedjan.[89]

7.6.2 Få myndigheter bedöms ha de förutsättningar som krävs

Utredningens förslag: Den myndighet regeringen bestämmer ska utföra grundidentifiering i samband med utfärdande av en statlig e-legitimation.

Den grundidentifiering som ska ske inför utfärdande av en statlig e-legitimation för svenska medborgare utomlands ska utföras av de myndigheter som för dessa medborgare utfärdar pass eller nationellt identitetskort.

[88] *Ett säkert statligt ID-kort – med e-legitimation*, (SOU 2019:14), s. 200 ff.
[89] Yttrandena finns tillfogade detta betänkande.

Utredningens bedömning: De myndigheter som kan komma i fråga för att genomföra grundidentifieringen på ett tillräckligt säkert, effektivt och tillgängligt sätt är Polismyndigheten och Skatteverket. Vi bedömer att Polismyndigheten är den myndighet av dessa två som är bäst lämpad att utföra uppdraget.

Utlandsmyndigheterna har erforderliga förutsättningar att hantera grundidentifiering för en statlig e-legitimation.

Skälen för utredningens förslag och bedömning

Den myndighet som ska genomföra grundidentifieringen behöver ha en gedigen organisation, erforderlig kunskap inom området, resurser och en utbredd närvaro i samhället. Därmed kan endast ett fåtal myndigheter komma i fråga för uppdraget och enligt vår bedömning är det Polismyndigheten eller Skatteverket.

2017 års ID-kortsutredning gjorde sina överväganden i fråga om grundidentifiering i samband med förslagen om vilken myndighet som skulle ansvara för utfärdande av såväl fysiska id-handlingar som en statlig e-legitimation. Det skiljer sig från vårt uppdrag eftersom det framgår av våra direktiv att Digg ska utfärda den statliga e-legitimationen. Det är emellertid vår uppfattning att grundidentifieringen och utfärdandet har sådana beröringspunkter att de skäl 2017 års ID-kortutredning anförde i fråga om lämplig utfärdande myndighet är relevanta även för vår bedömning av vilken myndighet som är lämplig att utföra grundidentifieringen.

Enligt vår bedömning ska personer med svenskt personnummer bosatta utomlands kunna ansöka om en statlig e-legitimation. Pass och id-kort utfärdas av de utlandsmyndigheter som även är passmyndigheter. 2017 års ID-kortsutredning gjorde bedömningen att någon förändring såvitt avsåg hanteringen av pass och id-kort vid dessa myndigheter inte var påkallad.[90] Vi ansluter oss till den bedömningen och anser att uppgiften att utföra grundidentifieringen inför utfärdande av en statlig e-legitimation för svenska medborgare utomlands bör utföras av motsvarande myndigheter.

[90] *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14), s. 212.

2017 års ID-kortsutredning föreslog Polismyndigheten

2017 års ID-kortsutredning föreslog att Polismyndigheten skulle utfärda de statliga fysiska identitetshandlingarna och den statliga e-legitimationen. Utredningen konstaterade vid en jämförelse mellan Polismyndigheten och Skatteverket att Skatteverkets erfarenhet av att utfärda identitetshandlingar inte var i närheten av den som fanns vid Polismyndigheten. Vidare påpekade utredningen att de identitetsjämförelser som Skatteverket gör i folkbokföringsverksamheten är av delvis annat slag och har ett annat syfte än den identitetsbedömning som görs i samband med utfärdande av en identitetshandling. Enligt utredningen var det av stor vikt att beakta möjligheten att bekämpa den ökade bedrägeribrottsligheten där missbruk av identiteter och identitetshandlingar spelar en stor roll. Utredningen anförde följande som skäl för att Polismyndigheten skulle ges uppdraget.[91]

> En viktig omständighet som tillkommit sedan Id-kortsutredningen lämnade sitt förslag, vilket också är anledningen till vårt uppdrag, är den ökade bedrägeribrottsligheten där missbruk av identiteter och identitetshandlingar spelar en stor roll. Polismyndigheten har det huvudsakliga ansvaret för arbetet med att motverka bedrägeribrottsligheten. Sambandet mellan identitetshandlingar och bedrägeribrottslighet talar enligt vår mening starkt för att Polismyndigheten bör tilldelas ansvaret för att utfärda de statliga fysiska identitetshandlingarna. Polismyndighetens erfarenheter från det brottsbekämpande arbetet, där falska eller felaktiga identitetshandlingar används i bedrägligt syfte, är värdefull för att utveckla och säkra utfärdandeprocessen. Kunskapen om och erfarenheterna från utfärdandeverksamheten kan även gagna brottsbekämpningen. Att ge Polismyndigheten ansvaret för utfärdandet kan således förväntas leda till samordningsvinster för båda delarna av verksamheten. En sådan ordning har därför goda förutsättningar att verka i brottsförebyggande riktning.
>
> En annan fördel med att lägga ansvaret hos Polismyndigheten är att myndigheten redan har lanserat en e-tjänst för kontroll av giltigheten när det gäller de identitetshandlingar som utfärdas av myndigheten. E-tjänsten […] kan användas av exempelvis banker eller andra som gör identitetskontroll för att på ett enkelt sätt kontrollera giltigheten av svenska pass och nationella identitetskort. Tjänsten har inneburit att kontrollen av identitetshandlingarnas giltighet har förenklats och effektiviserats avsevärt. Det är av stor vikt att det finns ett effektivt sätt att kontrollera en identitetshandlings giltighet. En enkel kontroll mot utfärdaren minskar risken för missbruk av identitetshandlingar samtidigt som den medför stora effektivitetsvinster. Det finns alltså redan en väl fungerande e-tjänst för kontroll hos Polismyndigheten vilket inte finns hos Skatteverket. E-tjänsten bör kunna användas även för kontroll av id-kort som inte kan användas

[91] Aa. s. 208 ff.

för resa. Om Polismyndigheten blir enda utfärdare möjliggörs dessutom en vidareutveckling av kontrollen så att den på sikt skulle kunna bli helt automatiserad. Exempelvis skulle det vid en avläsning av uppgifter på kortet kunna skickas en automatisk förfrågan till e-tjänsten varvid svar erhålls utan att den som utför kontrollen själv behöver slå in några uppgifter. En sådan lösning försvåras av att det i dag finns flera utfärdare.

Ansökan om de id-kort som utfärdas av Skatteverket kan göras på 27 platser. Därutöver finns det ytterligare 18 kontor där det är möjligt att hämta ut färdiga id-kort. Servicekontorsutredningen har […] föreslagit att dessa ska vara kvar i avvaktan på att vi redovisar våra förslag. Pass och nationellt identitetskort utfärdas av Polismyndigheten på omkring 110 platser. Därutöver finns det ytterligare cirka 40 utlämningsställen. Tillgängligheten för allmänheten är alltså väsentligt bättre hos Polismyndigheten än hos Skatteverket.

Vi föreslår […] att både ansiktsbild och fingeravtryck ska sparas på ett lagringsmedium i de statliga identitetskorten precis som gäller för pass i dag. Hantering av sådana uppgifter är särskilt känslig och kräver särskild säkerhet i processen. Polismyndigheten hanterar redan i dag ansiktsbild och fingeravtryck som sparas i ett lagringsmedium i passen samt ansiktsbild som sparas i de nationella identitetskortens lagringsmedium. Myndigheten har dessutom stor vana vid att hantera sådana uppgifter i den polisiära verksamheten. Polismyndigheten har alltså redan den erfarenhet och kunskap som krävs medan Skatteverket inte har samma vana vid att hantera sådana uppgifter.

Ett annat argument som talar för Polismyndigheten som utfärdare är att myndigheten har goda förutsättningar för att bedriva det informationsarbete som vi ser behov av. En av förklaringarna till de brister som i vissa fall finns i kontrollen av en persons identitet är okunskap om vad man ska titta på och varför. Det är därför av stor vikt att öka kunskapen om hur kontroller ska utföras och förståelsen för varför kontroller behöver göras hos den personal som utför identitetskontroller i olika verksamheter. Inom Polismyndigheten finns en stor kunskap om såväl de bedrägerier som utförs med användning av identitetshandlingar som utfärdandeprocessen. Det är värdefullt för verksamheter som ägnar sig åt identitetskontroller att få del av den kunskapen. Genom att öka kunskapen om hur bedrägerier går till kan risken för att bedrägerier genomförs minskas.

Sammantaget finns det alltså enligt vår uppfattning mycket starka skäl som talar för att Polismyndigheten ska utfärda de statliga fysiska identitetshandlingarna.

Som skäl emot att Polismyndigheten skulle ges uppdraget anfördes i stället följande.[92]

Som skäl emot denna ordning kan anföras att Polismyndighetens verksamhet bör renodlas i syfte att frigöra resurser för att förstärka kärnverksamheten, dvs. att upprätthålla allmän ordning och säkerhet. Detta

[92] A.a. s. 210 ff.

angavs som skäl för beslutet att Skatteverket skulle utfärda identitetskort för folkbokförda i Sverige, trots att Id-kortsutredningen på goda grunder föreslog att ansvaret skulle läggas på Polismyndigheten. Frågan om renodling av polisens verksamhet har genom åren varit föremål för olika utredningar. Polisverksamhetsutredningen gjorde år 2001 den bedömningen att passhanteringen varken krävde polismans befogenheter eller kunskap eller kunde motiveras av polisens uppgift att upprätthålla allmän ordning och säkerhet och att passhanteringen därmed till stor del saknade polisiär relevans. Utredningen kom trots det fram till att polisen fortfarande borde vara passmyndighet. Det huvudsakliga skälet var att ett överförande av passärendena till någon annan myndighet skulle innebära så stora konsekvenser för framför allt poliskontoren i glesbebyggda områden, som skulle kunna tvingas lägga ner, att det skulle få orimliga konsekvenser ur servicesynpunkt.

Det skäl som gjorde att Polisverksamhetsutredningen inte föreslog att passverksamheten skulle föras över till en annan myndighet är alltjämt gällande. Det finns orter där det skulle vara svårt att upprätthålla en receptionsverksamhet om Polismyndigheten inte längre skulle bedriva pass- och id-kortsverksamhet eftersom övrig receptionsverksamhet inte har så stor omfattning. Om verksamheten flyttas från Polismyndigheten finns det därför en risk att ett antal poliskontor skulle behöva stänga. Även om inte avgiftsintäkterna från pass- och id-kortsverksamheten finansierar annan receptionsverksamhet så motiverar verksamheten att det även finns en mottagning för andra ärenden, exempelvis tillståndsärenden. Många medborgare har dessutom bara kontakt med Polismyndigheten i samband med ansökan om pass eller id-kort. Verksamheten blir då en viktig del för att skapa förtroende för myndigheten. Ett bra bemötande och servicemottagande i ett passärende kan öka förtroendet för Polismyndigheten vilket kan bli avgörande för om medborgaren i ett annat sammanhang väljer att göra en anmälan, ställa upp som vittne eller liknande.

Argumentet att en överflyttning av pass- och id-kortshanteringen till Skatteverket skulle medföra en renodling av Polismyndighetens verksamhet och medföra att resurser frigörs till Polismyndighetens övriga verksamhet är inte helt adekvat. Rimligen skulle, som också Polisverksamhetsutredningen konstaterade, resurser som motsvarar pass- och id-kortshanteringen behöva föras över från Polismyndigheten till Skatteverket. Verksamheten är dessutom avgiftsfinansierad. Om verksamheten skulle flytta från Polismyndigheten flyttas även avgiftsintäkterna. Det är således svårt att se att det brottsbekämpande arbetet skulle komma att gynnas av att pass- och id-kortsverksamheten flyttas bort från Polismyndigheten. Tvärtom gör vi, som ovan framgått, snarare bedömningen att det brottsförebyggande arbetet gynnas av att myndigheten har denna verksamhet.

Det kan visserligen hävdas att utfärdande av identitetshandlingar inte tillhör Polismyndighetens kärnverksamhet, men det kan å andra sidan inte heller sägas vara främmande för den verksamheten. Vi menar i stället att den rådande samhällsutvecklingen med en kraftig ökning av bedrägeribrottsligheten och där brott många gånger begås med hjälp av för-

falskade eller felaktiga identitetshandlingar gör att det numera finns starka skäl att verksamheten avseende utfärdande av identitetshandlingar är samordnad med Polismyndighetens brottsbekämpande verksamhet. Polismyndigheten bör genom en sådan ordning få ökade förutsättningar att förebygga bedrägeribrott. Uppgiften att utfärda pass och id-kort kan därför i dag, på ett annat sätt än då Polisverksamhetsutredningen tog ställning i frågan, motiveras av Polismyndighetens kärnuppgift att upprätthålla allmän ordning och säkerhet.

Det finns således enligt vår uppfattning starka skäl för att Polismyndigheten ska ansvara för utfärdande av de statliga fysiska identitetshandlingarna. Vi har funnit få skäl som talar emot en sådan ordning.

Har något förändrats sedan 2017 års ID-kortsutredning gjorde sin bedömning?

Som redovisats i avsnitt 6.7 är den identitetsrelaterade brottsligheten, även om ökningen av sådana brott kopplade till förfalskade fysiska id-handlingar har avstannat något, fortsatt ett omfattande samhällsproblem. Det är alltjämt Polismyndigheten som har det huvudsakliga ansvaret för att motverka den typen av brottslighet vilket – precis som 2017 års ID-kortsutredning konstaterade – med styrka talar för att Polismyndigheten bör ansvara för grundidentifieringen. I princip samtliga företrädare för de organisationer och myndigheter som utredningen talat med har också framfört att Polismyndigheten är bäst lämpad för uppdraget. Flera har påtalat att en inställelse hos Polismyndigheten i sig har en brottsavhållande funktion eftersom det är mindre sannolikt att någon presenterar en förfalskad id-handling för en polistjänsteman än för en handläggare på Skatteverket. I det sammanhanget har också framförts att Skatteverket saknar rätt att omhänderta misstänkt falska identitetshandlingar om sådana presenteras för myndigheten inom ramen för ett ansökningsärende. En konsekvens därav är att Skatteverket i de fallen nekar sökanden begärd åtgärd och sedan återlämnar den förfalskade id-handlingen. Enligt Ekobrottsmyndigheten är detta särskilt ett problem när det gäller bedragare som utnyttjar migranter från andra EU-länder (tillvägagångssättet beskrivs i avsnitt 6.7).

Vi har inte närmare utrett om åtgärden att omhänderta misstänkt förfalskade identitetshandlingar bör omfattas av regelverket kring Skatteverkets brottsbekämpande verksamhet eller inte. Hur saken hanteras i dag indikerar oavsett att myndigheten för närvarande inte har tillräckliga förutsättningar för att motverka identitetsrelaterad brottslighet.

Om Skatteverket skulle ges uppgiften att utföra grundidentifieringen bör ett regelverk som ger handläggare rätt att omhänderta falska id-handlingar utredas vidare.

Vår bedömning är att de skäl som 2017 års ID-kortsutredning anförde i fråga om förutsättningar att motverka bedrägeribrottsligheten gör sig fortsatt gällande. Även vi har alltså uppfattningen att ett mycket tungt vägande skäl för att Polismyndigheten ska ges uppdraget är vikten av att motverka bedrägeribrottsligheten. Till det redan anförda kan även läggas att Polismyndigheten, till skillnad från Skatteverket, har tillgång till internationella register som används i brottsbekämpande syften. Polismyndigheter har dessutom träffat sådana bilaterala avtal med andra länder som är en förutsättning för att avläsa krypterad biometrisk information som finns lagrade i dessa länders rese- och identitetshandlingar.

För närvarande kan ansökan om id-kort som utfärdas av Skatteverket göras på 34 olika servicekontor och på begäran kan uthämtning därutöver ske på vissa servicekontor som inte utfärdar id-kort.[93] Enligt uppgift från Skatteverket utfärdade myndigheten 196 711 id-kort 2022.[94]

Pass och nationellt identitetskort utfärdas av Polismyndigheten på omkring 110 platser och därutöver finns det ytterligare utlämningsställen. Enligt uppgift från Polismyndigheten gjordes 3 667 960 ansökningar om pass och nationella id kort 2022.[95] Företrädare för Polismyndigheten har till utredningen uppgett att nivån fortsatt är hög och att omkring två miljoner pass utfärdats under första halvåret 2023.

Utifrån angiven statistik kan vi alltså konstatera att beträffande verksamhet med rese- och identitetshandlingar har Polismyndigheten fortfarande en påtagligt större närvaro i samhället än Skatteverket. Vidare har Polismyndighetens överlägset större rutin vad gäller att genomföra identitetskontroller, vilket är av avgörande betydelse även om myndigheten för närvarande inte deltar i någon verksamhet med att utfärda e-legitimationer.

Sedan 2017 års ID-kortsutredning lämnade sina förslag har en ny lag om samordningsnummer trätt i kraft (se avsnitten 3.3 och 7.4.2). De nya bestämmelserna medför bl.a. att Skatteverket ska genomföra grundligare identitetskontroller efter personlig inställelse. Som en följd

[93] www.skatteverket.se/omoss/kontaktaoss/besokservicekontor.4.515a6be615c637b9aa4acd5.html?filter=idcards, (hämtad 2023-09-20).
[94] Skatteverket, *Årsredovisning 2022*, (dnr 8-2211089), s. 85.
[95] Polismyndigheten, *Årsredovisning 2022*, (dnr A084.384/2022) s. 94.

därav kommer Skatteverket enligt vad som framgår av förarbetena till den nya lagen att behöva inrätta vissa nya rutiner och anpassa it-system, men såvitt framgår kommer inga ytterligare platser för ansökningar inrättas.[96] Således kommer de nya reglerna om samordningsnummer att innebära en delvis ny it-infrastruktur för Skatteverkets hantering men inte öka tillgängligheten för befolkningen i stort. Tillgängligheten för allmänheten kommer alltså fortfarande att vara väsentligt bättre hos Polismyndigheten än hos Skatteverket.

Polismyndighetens inställning till uppgiften att ansvara för grundidentifieringen tycks alltjämt vara densamma som vid tiden för 2017 års ID-kortsutredning. I en promemoria som upprättades i december 2022 med anledning av Diggs rapport anförde Polismyndigheten bl.a. följande[97]:

> Inom Polismyndigheten pågår ett arbete med att renodla polisens uppdrag. Syftet med att renodla myndighetens arbete är att ge polisen möjlighet att fokusera på sin kärnverksamhet. Detta för att polisen i ökad utsträckning ska kunna koncentrera sig på sin centrala funktion, dvs. att minska brottsligheten och öka tryggheten. Med anledning av det pågående arbetet är rådande uppfattning därför inledningsvis att nya uppgifter inom detta område inte bör påföras myndigheten. Detta eftersom uppgifterna inte har polisiär relevans eller direkt kräver polisiär befogenhet, utan kan påföras annan huvudman.

Vi anser emellertid – av samma skäl som anfördes av 2017 års ID-kortsutredning – att det inte nödvändigtvis finns ett motsatsförhållande mellan Polismyndighetens arbete med att renodla sin verksamhet och att myndigheten utför grundidentifieringen för den statliga e-legitimationen, inte minst när det gäller det brottsförebyggande arbetet. Vi har i avsnitt 6.7 redovisat den identitetsrelaterade brottslighetens utbredning i samhället och kopplingarna som finns till grov organiserad brottslighet. Självklart kommer denna inte stävjas endast genom att Polismyndigheten sköter grundidentifieringen inför utlämnande av e-legitimationer, men vi ser att det är ett led i att motverka den. Precis som 2017 års ID-kortsutredning anser också vi att uppgiften att utfärda pass och id-kort fortsatt motiveras av Polismyndighetens kärnuppgift att upprätthålla allmän ordning och säkerhet. Därmed motiveras även utförande av grundidentifiering vid utfärdande av statliga e-legitimationer av Polismyndighetens kärnuppgift.

[96] Prop. 2021/22:276 s. 131 ff.
[97] Polismyndigheten, Regeringsuppdraget om en statlig e-legitimation (dnr A356.966/2022), december 2022, s. 1.

7.6.3 Myndigheten för digital förvaltning ska ansvara för att utfärda den statliga e-legitimationen

Utredningens förslag: Den myndighet regeringen bestämmer ska tillhandahålla den statliga e-legitimationen.

Utredningens bedömning: Den statliga e-legitimationen ska tillhandahållas av Myndigheten för digital förvaltning.

Skälen för utredningens förslag och bedömning

I våra direktiv utpekas Digg som ansvarig myndighet för att utforma och tillhandahålla den statliga e-legitimationen. En omständighet som enligt direktiven talar för den ordningen är att myndigheten ansvarar för den offentliga förvaltningens tillgång till infrastruktur och tjänster för elektronisk identifiering och underskrift (3 § förordningen [2018:1486] med instruktion för Myndigheten för digital förvaltning). I den svenska infrastrukturen ingår bl.a. Diggs tillitsramverk, teknisk arkitektur och samordnad försörjning av tjänster för elektronisk identifiering. Andra myndigheter kan med hjälp av Digg som ombud ingå kontrakt med de leverantörer som omfattas av infrastrukturen, vilket regleras i lagen om valfrihetssystem i fråga om tjänster för elektronisk identifiering (eLOV).[98]

Vidare anges i våra direktiv att system för e-legitimationer och digital identifiering kräver särskild kompetens, vilket utgör ett ytterligare skäl till att Digg bör vara den myndighet som får ett uppdrag att ta fram en statlig e-legitimation.

Den särskilda kompetens som åsyftas inom Digg är både en förutsättning och en följd av de uppgifter och det ansvar som myndigheten redan har. Enligt eLOV fattar Digg bl.a. beslut om vilka villkor, inte minst säkerhetskrav, som ska uppfyllas för att en e-legitimations-

[98] Regeringen har föreslagit att valfrihetssystemen ska ersättas av ett auktorisationssystem (prop. 2023/24:6 se även avsnitten 4.6, 7.4.3 och 7.13.). Ombudsmodellen ska ersättas med en modell där Digg i eget namn ingår avtal om valfrihetssystem med leverantörerna. I likhet med nuvarande ordning kommer Digg att bestämma villkoren för auktorisationssystemen, bl.a. vilka säkerhetskrav som ska gälla. I tillägg till det som gäller i dag kommer Digg att ansvara för att bestämmelserna i den nya lagen följs och att de ställda säkerhetskraven upprätthålls (jfr prop. 2012/13:123 s. 51 f.). I övrigt ska ansvarsförhållandena framgå av de avtal som Digg ingår med de offentliga aktörerna och leverantörerna. Enligt förslaget ska den nya lagen träda i kraft den 1 januari 2024.

utfärdare ska få ingå i valfrihetssystemet, och om godkännande av e-legitimationsutfärdare enligt dessa krav.

Inom ramen för sitt ansvar att främja användningen av elektronisk identifiering förvaltar och utvecklar Digg även tillitsramverket för kvalitetsmärket Svensk e-legitimation (se mer om detta i avsnitt 4.3). En e-legitimation för vilken utfärdaren har ansökt om kvalitetsmärket granskas av Digg enligt kraven i tillitsramverket.[99] Digg har dock inte något tillsynsansvar över utfärdare i förhållande till eIDAS-förordningen.

Post- och telestyrelsen är tillsynsmyndighet enligt lagen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering, men ansvaret är begränsat till betrodda tjänster (se 4 § förordningen [2016:576] med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering). Utfärdare av e-legitimationer kan även ha viss rapporteringsskyldighet enligt lagen (2022:1568) om Sveriges riksbank.[100] Delar av sådana utfärdares verksamhet omfattas vidare av säkerhetsskyddslagen.[101]

Att utfärdare av e-legitimationer står under enbart begränsad tillsyn, vilken är uppdelad på flera statliga myndigheter utifrån deras uppgifter och befogenheter, har identifierats som en inte tillfredsställande ordning av bl.a. Finansinspektionen.[102] Betalningsutredningen har, i likhet med inspektionen, gjort bedömningen att det bör göras en översyn av tillsynsansvaret för e-legitimationer och betrodda tjänster.[103] I vårt andra deluppdrag ingår att bl.a. ta ställning till vilken myndighet som bör utses till tillsynsorgan med ansvar för ett register över förlitande parter enligt förslagen i den reviderade eIDAS-förordningen. Vi får därmed anledning att återkomma till tillsynsfrågan, men det handlar alltså om nödvändiga förändringar beroende på nya krav. Det faller

[99] Tillitsramverket utgör inte bindande rättsregler. Digg har inte några sanktionsmöjligheter kopplade till ramverket och utfärdares efterlevande av detsamma, *Staten och betalningarna* (SOU 2023:16) s. 350.

[100] Riksbanken har genom lagen, som trädde i kraft i januari 2023, fått ett utökat beredskapsansvar för betalningar i samhället. Företag som bedriver verksamhet som är av särskild betydelse för genomförandet av betalningar är bl.a. skyldiga att på begäran av Riksbanken lämna de uppgifter som är nödvändiga för Riksbankens beredskapsverksamhet. Utfärdare av e-legitimation har angetts som exempel på sådana företag, se *En ny riksbankslag* (SOU 2019:46), s. 1805.

[101] För sådan verksamhet är Länsstyrelsen i Stockholm säkerhetsskyddsstödjande myndighet och rapporterar säkerhetsskyddsincidenter till Säkerhetspolisen, *Staten och betalningarna* (SOU 2023:16) s. 351.

[102] Finansinspektionen, *Förstärkt digital motståndskraft hos företag i den finansiella sektorn, maj 2022, s.* 28. Vid sidan av ökad tillsyn som inte endast är händelsestyrd, framhöll Finansinspektionen behovet av reglering med tydliga krav på bl.a. säkerhetsnivå, redundans, samt lednings- och ägarprövning.

[103] *Staten och betalningarna* (SOU 2023:16) s. 380 ff.

emellertid, även för vårt kommande deluppdrag, utanför uppdragets ramar att göra en fullständig översyn av hela tillsynsstrukturen.

Både Betalningsutredningen och Finansinspektionen har i anslutning till tillsynsfrågan påtalat behovet av att fortsätta arbetet med att ta fram en statlig e-legitimation. Inspektionen har framhållit att en statlig e-legitimation, med hänsyn till den befintliga tillsynsstrukturen, är särskilt viktig om en ökad och samlad tillsyn över de privata aktörerna inte är möjlig att åstadkomma. Enligt Finansinspektionens egen bedömning är myndigheten inte ett lämpligt alternativ för ett sådant ansvar, eftersom det saknas ett naturligt samband mellan tillsyn av finansiella företag och e-legitimationer.[104]

Det finns, enligt vår bedömning, fog för Finansinspektionens och Betalningsutredningens uppfattning beträffande den bristande tillsynen på e-legitimationsområdet. Vårt förslag om införandet av en statlig e-legitimation kommer emellertid inte i sig att lösa problemet med att få till stånd en erforderlig tillsyn över utfärdare av e-legitimationer, eftersom den statliga utfärdaren också bör bli föremål för tillsyn. En myndighet som enligt vår bedömning i framtiden skulle kunna vara en kandidat att utöva sådan tillsyn är Digg.

Även med en i övrigt oförändrad ordning kommer Digg till följd av sitt nya uppdrag som utfärdare att behöva genomföra granskningar av sin egen verksamhet med den avsedda e-legitimationen. Granskningen kommer att ske mot de krav som myndigheten delvis själv uppställer. Således uppstår – redan genom att myndigheten utses till utfärdare av den statliga e-legitimationen – oundvikligen risk för rollkonflikter inom myndigheten. Ett eventuellt uppdrag om att utöva tillsyn skulle ytterligare förstärka rollkonflikten och vi ser det därmed som uteslutet att Digg både skulle kunna tillhandahålla den statliga e-legitimationen och ges ett framtida tillsynsansvar över e-legitimationsområdet.

Digg har i sin rapport uppmärksammat att rollkonflikter inom myndigheten riskerar att uppstå till följd av det tillkommande uppdraget med att utfärda och tillhandahålla en statlig e-legitimation. För att undvika dessa rollkonflikter har Digg bedömt att det i vart fall bör krävas att myndigheten organisatoriskt skiljer på rollen som utfärdare av e-legitimationen från övriga uppgifter inom e-legitimationsområdet i syfte att säkerställa att myndigheten lever upp till de krav som ställs

[104] Finansinspektionen, *Förstärkt digital motståndskraft hos företag i den finansiella sektorn, maj 2022*, s. 28.

på myndighetens verksamhet, framför allt vad gäller objektivitet, likabehandling och för att undvika en jävsproblematik. Vidare har Digg bedömt att myndigheten ska tydliggöra hur beslutsförfarandet ska se ut när myndigheten agerar i olika roller. Enligt Digg kan en förebild vara hur Försvarets materielverk har organiserats för att upprätthålla det krav på oberoende som följer av EU:s cybersäkerhetsakt.[105]

Vi bedömer att de rollkonflikter som kan uppstå inte enbart kan hanteras genom organisatoriska åtgärder och att det, som Digg i sin bedömning öppnat för, krävs ytterligare åtgärder.

Som också Digg påtalar är en ytterligare omständighet kopplad till rollkonflikter att myndigheten i sin granskning och revision av andras e-legitimationer, dvs. även kommersiella aktörers, kan ta del av affärshemligheter eller information som är skyddad av immaterialrätten. Detta kan vara förtroendeskadande.

7.6.4 Effekter av ett uppdelat myndighetsansvar för grundidentifiering respektive utfärdande

Utredningens bedömning: Ett uppdelat myndighetsansvar för grundidentifiering respektive utfärdande av den statliga e-legitimationen medför vissa effekter som behöver hanteras av de berörda myndigheterna.

Skälen för utredningens bedömning

Det finns skäl att problematisera effekterna av ett uppdelat ansvar

Våra direktiv ger inte utrymme för att lämna förslag om att någon annan myndighet än Digg ska ges i uppdrag att utfärda den statliga e-legitimationen, vilket får till följd att ansvaret för grundidentifiering och utfärdande behöver delas upp på två olika myndigheter.

Under vårt arbete med utredningen har vi likväl identifierat vissa effekter som ett uppdelat ansvar kan medföra. Redogörelsen gör inte anspråk på att vara uttömmande och innebär inte att vi har gjort bedömningen att ett bättre alternativ hade varit om en myndighet ansvarade för hela verksamheten. Som framgår av kapitel 5 förekom-

[105] Myndigheten för digital förvaltning, *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, s. 61 ff.

mer ett uppdelat ansvar vad gäller utfärdande av statliga e-legitimationer i andra länder och det finns givetvis även fördelar med att en expertmyndighet inom digitaliseringsområdet är den utfärdande myndigheten.

Eftersom det är fråga om effekter som dels kan vara beroende av vilken myndighet som slutligen ges i uppdrag att genomföra grundidentifieringen, dels kräver samråd mellan de berörda myndigheterna kan utredningen inte lämna några närmare förslag på hur effekterna ska lösas. De redovisade effekterna kan i stället hanteras av de berörda myndigheterna i samband med införandet av den statliga e-legitimationen.

Tillgänglighetsargumentet

Som framgått är en del av vårt uppdrag att lämna förslag som innebär att den statliga e-legitimationen görs tillgänglig för så många som möjligt, särskilt grupper som för närvarande saknar tillgång till digitala tjänster. Som tidigare beskrivits är utanförskapet på gruppnivå störst hos äldre och personer med funktionsnedsättning samt boende i utanförskapsområden (se avsnitt 6.6). Detta är grupper som kan förväntas vara hjälpta av tydlighet och förutsebarhet, särskilt i frågor som har med digitalisering eller myndighetskontakter att göra. Tillgänglighet bör i detta sammanhang ses i en vidare bemärkelse än att det rent faktiskt ska vara möjligt att skaffa en e-legitimation. Vi menar att en väsentlig del i att tillgängliggöra den statliga e-legitimationen också består i att det tydligt framgår vem som ansvarar för utfärdandet och vart en enskild ska vända sig vid eventuella problem eller vid behov av support.

Enligt vår bedömning kan en uppdelning av ansvaret med att genomföra grundidentifieringen respektive att utfärda och i övrigt tillhandahålla den statliga e-legitimationen leda till otydlighet. Detta gäller särskilt vid föreslagen ordning där ansökan i sin helhet görs hos den identitetskontrollerande myndigheten, trots att den myndigheten i själva verket endast ansvarar för en – låt vara mycket viktig, men – begränsad del av uppdraget. Den myndighet som efter ansökningstillfället ska ha det långsiktiga ansvaret för administration och support i användningsskedet är i stället den utfärdande myndigheten, alltså Digg. För den enskilde, som inte kommer i kontakt med Digg under ansökningsförfarandet, kommer det sannolikt inte att vara särskilt tydligt att det

är den myndigheten som ansvarar för utfärdandet. Vidare kan ovana användare tänkas ställa frågor kopplade till användningen redan vid utfärdandet, något som en enskild handläggare vid den identitetskontrollerande myndigheten behöver ha beredskap för.

Förvaltningsrättsliga frågeställningar

En uppdelning av ansvaret aktualiserar förvaltningsrättsliga frågeställningar, exempelvis med avseende på vilken myndighet som ska ansvara för ett visst beslut och i vilken ordning olika beslut ska överklagas.

Beslut som en myndighet fattar och åtgärder som vidtas gentemot en enskild utgör myndighetsutövning. Den identitetskontrollerande myndigheten kommer i samband med grundidentifieringen att kontrollera och bedöma om den information en sökande åberopar är sådan att identiteten ska anses styrkt. Detta får i sig anses utgöra myndighetsutövning och resultatet av bedömningen är i praktiken av avgörande betydelse för om Digg ska bifalla ansökan om en statlig e-legitimation eller inte. De överväganden som Digg gör och beslutet som övervägandena leder fram till utgör i sin tur myndighetsutövning som utövas av Digg. Vi har inte kunnat identifiera någon annan verksamhet i vilken skilda myndigheter, inom ramen för ett och samma ansökningsförfarande, utövar myndighet på ett motsvarande sätt.

Vi menar att uppdelningen, beroende på hur myndigheterna organiserar sitt samarbete, kan leda till gränsdragningsproblem som behöver hanteras. Således finns det skäl att beakta om såväl den identitetskontrollerande myndighetens som Diggs beslut är sådana att de måste kunna överklagas var för sig och i sådant fall vilka konsekvenser det får för enskilda som, vid avslag på ansökan, kan komma att behöva överklaga två skilda beslut i stället för ett. Om myndigheterna kan organisera sig på ett sätt där dubbla överklaganden undviks, finns det skäl att överväga hur ett nödvändigt informationsutbyte mellan myndigheterna ska ske vid en eventuell överprövning.

Uppdelat personuppgiftsansvar

Ett uppdelat ansvar för grundidentifieringen och utfärdandet leder som beskrivs i avsnitt 7.11 till ett uppdelat personuppgiftsansvar och att en myndighet får en biträdesroll till en annan. En stor mängd personuppgif-

ter behöver hanteras inom ramen för verksamheten med att tillhandahålla en statlig e-legitimation, vissa med betydande integritetsrisker. När uppgifterna ska delas mellan olika myndigheter ökar integritetsriskerna och det ställs särskilt höga krav på hanteringen. Såväl Skatteverket som Polismyndigheten hanterar dessutom i stor utsträckning motsvarande personuppgifter i sin egen verksamhet som de ska föra in i Diggs register. Detta medför att Diggs ansvar som personuppgiftsansvarig riskerar att bli svåröverskådligt exempelvis när tillsyn ska utföras.

Genomförandeaspekter

Med hänsyn till att utvecklingen på e-legitimationsområdet sker snabbt kommer det finnas behov av att smidigt kunna implementera nya rutiner eller bestämmelser för verksamheten med en statlig e-legitimation. Ett uppdelat ansvar förutsätter en god samverkan mellan de inblandade myndigheterna för att inte riskera att leda till ökad administration, som i sin tur kan orsaka längre införandetider och högre kostnader.

7.7 Giltighetstid och återkallelse

7.7.1 Den statliga e-legitimationens giltighetstid

Utredningens förslag: Den statliga e-legitimationen ska ha en giltighetstid om högst fem år.

Begränsning av giltighetstiden får föreskrivas bara i särskilt angivna fall.

Utredningens bedömning: Om den statliga e-legitimationen tillhandahålls på en fysisk id-handling ska giltighetstiden motsvara den som gäller för den fysiska id-handlingen.

Skälen för utredningens förslag och bedömning

Vid bedömningen av vad som utgör en lämplig giltighetstid för den statliga e-legitimationen finns det framför allt skäl att beakta säkerhetsriskerna med en alltför lång giltighetstid, men också användarperspektivet och administrationsbördan vid en för kort giltighetstid.

2017 års ID-kortsutredning föreslog att giltighetstiden för ett statligt id-kort skulle vara fem år och att e-legitimationen på kortet skulle ha motsvarande giltighetstid. Utredningen hänvisade till att giltighetstiden för det nationella identitetskortet, liksom för identitetskortet för folkbokförda är högst fem år. En sådan begränsning av giltighetstiden angavs vara av stor betydelse ur ett säkerhetsperspektiv eftersom innehavarens utseende inte hinner förändras i så stor utsträckning under giltighetstiden. Vidare framhöll utredningen att en begränsad giltighetstid minskar risken för att det samtidigt finns flera olika versioner av id-kortet tillgängliga på marknaden och gör att det finns goda förutsättningar för att handlingarna ska kunna innehålla de senaste säkerhetsdetaljerna, vilket motverkar förfalskningar.[106]

För BankID på kort och Svenska Pass e-legitimation gäller en giltighetstid om fem år. Även pass och nationella id-kort är giltiga i fem år, men för sökande under tolv år är giltighetstiden begränsad till tre år.[107] Enligt vår uppfattning saknas det skäl för att göra en annan bedömning vad avser giltighetstiden för den statliga e-legitimationen än vad som gäller för andra identitetshandlingar eller e-legitimationer på fysiska bärare. Giltighetstiden för den statliga e-legitimationen bör därför högst vara fem år.

Vi har mottagit synpunkten att kostnaden för att förnya sin e-legitimation vart femte år skulle bli oskäligt betungande för många människor. Den statliga e-legitimationen ska emellertid, precis som ett pass och det nationella id-kortet, betraktas som en värdehandling. Vi anser därför att det finns goda skäl för att den statliga e-legitimationen ska vara avgiftsbelagd på samma sätt. Vidare är säkerhetsaspekterna som motiverar en begränsad giltighetstid sådana att de överväger nackdelen med ifrågavarande kostnad. För det fall e-legitimationen utfärdas på en annan identitetshandling kan det emellertid finnas skäl att överväga en samordnad kostnad (se mer om avgifter i avsnitt 7.9).

Till skillnad från 2017 års ID-kortsutredning och Digg gör vi bedömningen att den statliga e-legitimationen ska kunna utfärdas till personer som innevarande kalenderår är eller ska fylla nio år (se avsnitt 7.4.2). Giltighetstiden för pass och nationella id-kort som utfärdas till barn under tolv år sänktes till tre år 2016. Som skäl för förändringen angav regeringen bl.a. att ett barns utseende genomgår väsent-

[106] *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14) s. 227.
[107] Se 3 § andra stycket passlagen (1978:302) och 5 § andra stycket förordning (2005:661) om nationellt identitetskort.

liga förändringar under uppväxtåren, vilket kunde leda till missbruk i form av s.k. ”lookalike-användning”.[108]

Enligt vår bedömning gör förväxlingsriskerna vid användning av en e-legitimation sig inte gällande i samma utsträckning som för en fysisk id-handling. Att begränsa giltighetstiden av det skälet är därför inte nödvändigt. Vi kan dock konstatera att en ordning där giltighetstiden för bäraren och e-legitimationen blir överlappande inte framstår som önskvärd. Av det skälet anser vi att giltighetstiden för e-legitimationer som utfärdats till personer under 12 år bör begränsas till tre år om de utfärdas på ett fysiskt id-kort. När så inte är fallet bör giltighetstiden i stället vara högst fem år.

2017 års ID-kortsutredning föreslog, med hänvisning till dess stora betydelse ur ett säkerhetsperspektiv, att giltighetstiden skulle regleras i lag.[109] Vi instämmer visserligen i att giltighetstiden är av stor betydelse ur ett säkerhetsperspektiv, men menar att det för den statliga e-legitimationen framstår som mer ändamålsenligt att giltighetstiden framgår av förordning. Skälet till den bedömningen är att det inte kan uteslutas att den snabba utvecklingen på e-legitimationsområdet medför att förändringar kan behöva genomföras med skyndsamhet.

Normgivningsnivån följer därmed också den som gäller för befintliga fysiska id-handlingar.

Undantag som innebär begränsningar av giltighetstiden får föreskrivas bara i särskilt angivna fall, exempelvis på grund av tillfälligt hinder mot att ta fingeravtryck. En begränsad giltighetstid i sådant fall bör lämpligen motsvara vad som gäller i fråga om provisoriska pass, dvs. högst sju månader (se 13 § passförordningen).[110]

För det fall den statliga e-legitimationen utfärdas på ett fysiskt id-kort bör begränsningar av giltigheten för det fysiska id-kortet gälla även för den statliga e-legitimationen.

7.7.2 Återkallelse och spärr av e-legitimationen

Utredningens förslag: Den statliga e-legitimationen ska återkallas och spärras om det är nödvändigt av säkerhetsskäl eller om förutsättningarna för utfärdande inte längre är uppfyllda eller har ändrats

[108] Prop. 2015/16 :81 s. 20 f.
[109] *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14), s. 227.
[110] Se även förslaget från 2017 års ID-kortsutredning, a.a. s. 290 ff.

väsentligt. E-legitimationen ska också kunna återkallas och spärras på begäran av innehavaren.

E-legitimationen ska också återkallas och spärras om den inte har aktiverats inom sex månader efter att ansökan och grundidentifieringen genomfördes eller om innehavaren är avliden.

Om den statliga e-legitimationen har återkallats eller spärrats måste ett nytt ansökningsförfarande initieras innan en ny statlig e-legitimation kan utfärdas.

En statlig e-legitimation ska spärras senast i samband med att en ny statlig e-legitimation utfärdas eller, om förnyelse inte har skett, automatiskt när giltighetstiden har gått ut.

Utredningens bedömning: Om den statliga e-legitimationen finns på en fysisk id-handling ska e-legitimationen återkallas om den fysiska id-handlingen återkallas.

Det bör av säkerhetsskäl inte vara möjligt att häva en spärr av e-legitimationen även om omständigheterna som föranledde spärren inte längre föreligger.

Skälen för utredningens förslag och bedömning

En statlig e-legitimation ska endast utfärdas under vissa angivna förutsättningar och kan i innehavarens hand ge åtkomst till betalmarknaden samt olika välfärdsförmåner. Om e-legitimationen missbrukas eller om förutsättningarna för utfärdande inte längre är uppfyllda måste det vara möjligt att återkalla och skyndsamt spärra e-legitimationen.

Det kan också finnas skäl att återkalla en statlig e-legitimation om väsentliga uppgifter om innehavaren förändras. Förändrade uppgifter kan i sin tur medföra att nya säkerhetsöverväganden måste göras eller att förutsättningarna för utfärdande inte längre kan anses vara uppfyllda, även om de var det när e-legitimationen utfärdades. Så kan exempelvis vara fallet om ett samordningsnummer får ändrad identitetsnivå eller förklaras vilande samt vid namnbyte eller byte av personnummer. Enligt vår bedömning är de uppgifter som en statlig e-legitimation innehåller till övervägande del av sådan betydelse att de ska anses rymmas inom begreppet väsentlig. Mindre betydande förändringar som inte inverkar på de höga säkerhetskrav som gäller bör dock inte medföra att e-legitimationen återkallas.

2017 års ID-kortsutredning föreslog att den statliga e-legitimationen skulle upphöra att gälla om det statliga identitetskort som den fanns på återkallades eller om det var nödvändigt av säkerhetsskäl. Vidare bedömde utredningen att återkallelsen skulle begränsas till viss bestämd tid, dock högst sex månader, om det var lämpligt med hänsyn till omständigheterna.[111]

Vår bedömning är att den statliga e-legitimationen så snart som möjligt ska tillhandahållas på en fysisk identitetshandling utfärdad av staten (se avsnitt 7.2.2). Vid en sådan ordning bör den statliga e-legitimationen upphöra att gälla om den fysiska bäraren återkallas.

Oavsett om e-legitimationen utfärdas på ett statligt id-kort eller inte finns det emellertid, som också 2017-års ID-kortsutredning konstaterade, situationer då det finns skäl att återkalla endast e-legitimationen. Enligt den utredningen kunde det till exempel gälla situationer med bedräglig användning av e-legitimationen som rör ett stort antal användare eller att en enskild e-legitimation används på ett sätt som gör att misstanke om bedräglig användning uppstår.[112] Vi ansluter oss till den bedömningen.

En statlig e-legitimation som har återkallats eller upphört att gälla bör göras obrukbar genom att den spärras elektroniskt. Om e-legitimationen tillhandahålls ensamt på en fysisk bärare bör det inte införas något krav på att e-legitimationen ska återlämnas efter återkallelsen. Skälet till det är att kortet kommer att vara obrukbart när e-legitimationen återkallats, varför någon risk för missbruk inte föreligger. Mot den bakgrunden framstår den administration som skulle krävas för att hantera och registrera återlämnade e-legitimationer som omotiverad. Inte heller om den statliga e-legitimationen placeras på en annan fysisk id-handling bör återlämnande krävas eftersom det fysiska id-kortet i ett sådant fall bör kunna användas trots att e-legitimationen är återkallad och spärrad. 2017-års ID-kortsutredning gjorde i detta avseende motsvarande bedömning.[113]

Om säkerhetsbrister upptäcks eller om misstanke uppkommer om att en e-legitimation använts i brottslig verksamhet kan det uppstå behov av att spärra e-legitimationen skyndsamt och utan att fullständigt underlag finns. 2017 års ID-kortsutredning identifierade motsvarande behov och ansåg att det skulle vara möjligt att återkalla en e-legitima-

[111] *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14), s. 346.
[112] A.a. s. 347.
[113] Ibid.

tion tillfälligt. Av 25 § första stycket 3 förvaltningslagen (2017:900) framgår att en myndighets beslut får meddelas omedelbart utan föregående kommunikation med parten om ett väsentligt allmänt eller enskilt intresse kräver det. Ett beslut om att återkalla en e-legitimation bör därför, som också 2017 års ID-kortsutredning kom fram till, ofta kunna fattas utan att parten underrättas i förväg.[114] Det ska också vara möjligt att spärra den statliga e-legitimationen efter anmälan av innehavaren.[115]

Av säkerhetsskäl och eftersom det inte ska vara möjligt att inneha mer än en statlig e-legitimation samtidigt ska den statliga e-legitimationen spärras senast när en ny e-legitimation utfärdas. Av samma skäl måste en automatisk spärr av e-legitimationen ske om innehavaren inte har inlett ett nytt ansökningsförfarande innan giltighetstiden har passerat.

Tillämpningsbestämmelser om förfarandet vid spärr av den statliga e-legitimationen meddelas på förordningsnivå eller i myndighetsföreskrifter.

Vi har övervägt om det ska finnas en möjlighet att häva spärren exempelvis om det skulle visa sig att ifrågavarande säkerhetsbrist eller brottsmisstanke inte längre föreligger. Syftet med det skulle främst vara att undvika den administrativa börda det skulle innebära för den identitetskontrollerande och utfärdande myndigheten att utfärda nya e-legitimationer. Det skulle också vara en praktisk hantering exempelvis i de fall den statliga e-legitimationen spärrats på begäran av innehavaren vid misstanke om att den förkommit men senare återfinns. Vi har dock kommit fram till att det av säkerhetsskäl inte är lämpligt att införa en möjlighet att häva en spärr utan att ett nytt ansökningsförfarande genomförs. Följden av att en statlig e-legitimation återkallas eller spärras blir alltså att innehavaren måste ansöka på nytt och i samband med det uppfylla de krav som ställs.

Att utfärdaren ska tillhandahålla en spärrtjänst följer av eIDAS-förordningen. I den mån det finns behov av att ytterligare reglera förfarandet vid spärr på innehavarens begäran kan det ske genom myndighetsföreskrifter.

[114] Ibid.
[115] Jfr t.ex. 3 kap. 1 § Rikspolisstyrelsens föreskrifter och allmänna råd om polismyndigheternas hantering av pass och nationellt identitetskort (RPSFS 2009:14).

7.8 Användningen av den statliga e-legitimationen

Utredningens förslag: Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om villkor för när och hur den statliga e-legitimationen får användas.

Skälen för utredningens förslag

Viss civilrättslig och straffrättslig reglering är tillämplig vid användning av e-legitimationer

Som framgått i kapitel 4 kan en e-legitimation ha olika användningsområden men gemensamt för samtliga e-legitimationer är att de kan användas för identifiering. Därutöver kan e-legitimationer användas för att skapa en elektronisk underskrift. Vid sidan av dessa båda funktioner kan en e-legitimation användas som betalningsinstrument. Hur en e-legitimation används påverkar vilken reglering som är tillämplig, och därmed vilka krav som gäller för utfärdaren, användaren och i förekommande fall förlitande part.

En av förutsättningarna för att kunna skaffa någon av de e-legitimationer som för närvarande tillhandahålls av svenska aktörer är att sökanden godkänner de villkor som gäller för utställande och användning. Genom avtal regleras således bl.a. skyldigheter för innehavaren, såsom att skydda sin e-legitimation och inte överlåta den till någon annan. Såvitt gäller användning av e-legitimationer som betalningsinstrument avtalas sådana aktsamhetsregler numera även till förmån för tredje man via s.k. tredjemansavtal.

Även övriga uppkomna partsrelationer är huvudsakligen avtalsreglerade; mellan e-legitimationsutfärdare, identitetsintygsutfärdare, tillhandahållare av anvisningstjänst, legitimeringstjänst, och behörighetskontrolltjänst samt förlitande part (se avsnitt 4.1). Vid användning av en e-legitimation, även obehörig sådan, är det alltså i första hand utifrån avtalsrättsliga regler frågan om innehavarens bundenhet får avgöras.

Obehörig användning av e-legitimation kan delas in i olika kategorier, t.ex. obehörig identifiering med e-legitimation, obehörig underskrift med e-legitimation och obehörig transaktion med betalningsinstrument, varav främst de två sistnämnda används för otillbörlig

förmögenhetsöverföring och därmed resulterar i större massmedial uppmärksamhet och fler straff- och civilrättsliga processer.

Förutsättningen för att innehavaren inte ska bli bunden är att det verkligen handlar om obehörig användning av e-legitimationen, dvs. det får varken föreligga samtycke eller fullmakt som grund för den aktuella användningen. Möjligen kan passivitet inför förfalskningen – att personen trots kunskap om den obehöriga användningen underlåter att meddela motparten detta, tänkas leda till bundenhet.[116]

Som framgår nedan finns det särreglering beträffande användning av e-legitimation som betalningsinstrument, bl.a. regler om ansvarsfördelning vid uppkommen skada. I övrigt får skadeståndslagen (1972:207) och allmänna skadeståndsrättsliga principer tillämpas. Den skada som åsamkas utgörs normalt av ren förmögenhetsskada, dvs. ekonomisk skada som uppkommer utan samband med en person- eller sakskada (se 1 kap. 2 § skadeståndslagen). Skadeståndsrätten skiljer också mellan skador som uppkommer i avtalsförhållanden och skador som uppkommer utanför avtalsförhållanden, s.k. utomobligatoriska förhållanden. Skadeståndslagen innehåller en särskild bestämmelse om ersättning för ren förmögenhetsskada i utomobligatoriska förhållanden. Enligt 2 kap. 2 § i den lagen ska den som vållar ren förmögenhetsskada genom brott ersätta skadan.

Vad gäller strafflagstiftningen har den vid ett antal tillfällen uppdaterats för att anpassas för elektroniska underskrifter. Brotten mot urkunder inkluderar numera elektroniska urkunder (14 kap. 1 § brottsbalken). Reglerna om urkundsförfalskning och sanningsbrotten (t.ex. osann försäkran, osant intygande och missbruk av urkund i 15 kap. brottsbalken) gäller på samma sätt för en elektronisk urkund. Dessutom finns även bestämmelser om olovlig identitetsanvändning (4 kap. 6 b § brottsbalken) samt olovlig befattning med betalningsverktyg (9 kap. 3 c §) som också kan tillämpas. Det är alltså kriminaliserat att exempelvis använda någon annans e-legitimation som gällande för sig eller att överlämna e-legitimationen och säkerhetskod till någon annan för att missbrukas på det sättet (missbruk av urkund, 15 kap. 12 § brottsbalken). Det utgör samtidigt ett avtalsbrott mot utställaren av e-legitimationen.

[116] Aagaard, M., *Obehörig användning av e-legitimation och läran om misstagsbetalning*, JT nr 4 2021–22, s. 866 ff., och den däri gjorda hänvisningen till Hessler, H. *Obehöriga förfaranden med värdepapper – en studie över de civilrättsliga verkningarna av förfalskning och annan oegentlighet beträffande löpande skuldebrev, växlar, checkar och bankböcker*, 1981.

Skadeståndsansvar vid gränsöverskridande användning enligt eIDAS-förordningen

I eIDAS-förordningen finns bestämmelser om skadeståndsansvar i artikel 11 såvitt gäller e-legitimationer. Skadeståndsansvar gäller för den som utfärdar en e-legitimation och för den som handhar autentiseringsförfarandet[117], vid underlåtelse att uppfylla sina respektive skyldigheter enligt förordningen (artikel 11.2 och 11.3). Som tidigare redovisats gäller förordningens bestämmelser om elektronisk identifiering, såväl som bestämmelserna om betrodda tjänster, enbart vid användning över landsgränserna inom EU. För sådan gränsöverskridande användning av en svensk e-legitimation krävs att Sverige som medlemsstat anmäler e-legitimationssystemet enligt ett särskilt förfarande (se beskrivning i avsnitt 4.2.3). Medlemsstaten utgör en garant för att anmälda system uppfyller förordningens krav och omfattas därför också av skadeståndsansvar vid underlåtelse att uppfylla ålagda skyldigheter (artikel 11.1 och artikel 7).

Även för tillhandahållare av betrodda tjänster föreskrivs skadeståndsansvar för skada som åsamkats en fysisk eller juridisk person avsiktligt eller på grund av oaktsamhet genom underlåtenhet att uppfylla kraven i förordningen (artikel 13). Med betrodda tjänster avses enkelt uttryckt elektroniska tjänster som erbjuder vissa utpekade funktioner kopplade till elektroniska underskrifter, elektroniska stämplar, elektroniska tidsstämplingar eller certifikat för autentisering av webbplatser. Dessutom utgör elektroniska tjänster för rekommenderade leveranser, i sig, betrodda tjänster (se legaldefinitionen i artikel 3.16 i eIDAS-förordningen). När en e-legitimation, som erbjuds tillsammans med möjligheten att skapa elektroniska underskrifter (såsom BankID och Freja+), används för att skapa sådana elektroniska underskrifter, utgör tjänsten en betrodd tjänst.

Givet att den föreslagna statliga e-legitimationen anmäls för gränsöverskridande användning, och kan användas för att framställa kvalificerade elektroniska underskrifter (se förslag i avsnitt 7.3), kan skadeståndsskyldighet enligt bestämmelserna i eIDAS-förordningen uppkomma för svenska staten i samtliga redovisade roller. I såväl artikel 11 som artikel 13 anges att förordningsreglerna vad gäller skadestånd ska tillämpas i enlighet med nationella bestämmelser om

[117] Härmed avses både nodmyndigheten och utfärdaren av e-legitimationen i sina respektive delar av autentiseringen, se *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 359.

skadeståndsansvar (se även skäl 18 och skäl 37 i förordningens ingress). Förordningen påverkar därmed inte tillämpningen av nationella bestämmelser om t.ex. definition av skada, oaktsamhet eller relevanta tillämpliga förfaranderegler, inbegripet regler om bevis. Som konstaterades av Utredningen om effektiv styrning av nationella digitala tjänster går det inte att med säkerhet säga vilken medlemsstats nationella regler som kan bli tillämpliga. I frågor om gränsöverskridande identifiering kan den skadelidande befinna sig i en medlemsstat och den skadeståndsansvarige i en annan. Dessa respektive medlemsstater kan ha nationell rätt som ger motstående lösningar på lagvalsproblemen. I dessa fall får ledning sökas i Europaparlamentet och Rådets förordning (EG) nr 864/2007 av den 11 juli 2007 om tillämplig lag för utomobligatoriska förpliktelser (Rom II).[118]

Även vid gränsöverskridande användning av den föreslagna statliga e-legitimationen är det alltså mot skadeståndslagen och allmänna skadeståndsrättsliga principer som uppkomna frågor om ersättningsrätt prövas, givet att svensk lag ska tillämpas. Hur dessa principer ska tillämpas på skador i nu aktuella fall får, som på andra områden inom skadeståndsrätten, bli en uppgift för rättstillämpningen att avgöra.

För det fall privata underleverantörer anlitas av staten för att uppfylla sina åtaganden har det tidigare påtalats att det är av vikt att tydliga avtal upprättas som reglerar skadeståndsansvar mellan staten och de privata aktörerna. Detta för att begränsa risken för att staten tvingas ta ett skadeståndsansvar som inte var påtänkt eller att tvister uppstår mellan avtalsparterna.[119]

Särskild reglering och rättspraxis i fråga om användning av e-legitimationer för betalningstransaktioner och ingående av kreditavtal

När en e-legitimation, såsom BankID, Freja+, eller den föreslagna statliga e-legitimationen, används som elektronisk underskrift för att initiera en betalningsorder, anses själva e-legitimationen utgöra ett betalningsinstrument enligt en tolkning av bestämmelsen i 1 kap. 4 § första stycket lagen (2010:751) om betaltjänster (härefter betaltjänst-

[118] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 367 ff.
[119] A.a. s. 360.

lagen).[120] I sådana fall gäller också reglerna om obehöriga transaktioner i samma lag.

En betaltjänstleverantör, t.ex. en bank eller kreditinstitut, har av konsumentskyddsskäl vissa skyldigheter att återställa konton (5 a kap. 1 § nämnda lag), men bestämmelserna fastslår också betaltjänstanvändarens ansvar att skydda sina personliga behörighetsfunktioner.

Vid ett grovt oaktsamt åsidosättande av de skyldigheter att skydda sitt betalningsinstrument som åvilar innehavaren enligt 5 kap. 6 § betaltjänstlagen, blir denne ansvarig för maximalt 12 000 kronor. Det är först vid ett *särskilt klandervärt* agerande som konsumentens ansvar blir obegränsat (5 a kap. 3 § nämnda lag). Ett prejudikat från Högsta domstolen ger viss vägledning avseende konsumenters ansvar för obehöriga transaktioner, när transaktionen möjliggjorts av konsumenten själv i samband med att denna utsatts för ett bedrägeri.[121]

Betaltjänstlagens regler omfattar däremot inte en ansökan om kreditavtal, eftersom det då inte är fråga om att e-legitimationen används som ett betalningsinstrument.[122] Som tidigare nämnts är det därför mot allmänna avtalsrättsliga och skadeståndsrättsliga regler och principer som frågan om bundenhet respektive ersättningsrätt får prövas.

Kreditgivaren (förlitande part) har genom den obehöriga användningen drabbats av en ren förmögenhetsskada och har därmed möjlighet att rikta sitt anspråk gentemot bedragaren (2 kap. 2 § skadeståndslagen). Eftersom bedragaren ofta är okänd har kreditgivare gjort vissa försök med att åberopa andra rättsliga grunder än avtalsbundenhet för att rikta anspråk mot innehavaren av den obehörigen använda e-legitimationen, bl.a. återbetalning med stöd i läran om misstagsbetalningar

[120] Enligt legaldefinitionen är ett betalningsinstrument ”ett kontokort eller något annat personligt instrument eller rutin som enligt avtal används för att initiera en betalningsorder.” I förarbetena har ”ett s.k. bank-id som registreras i datorn” nämnts som exempel på sådana betalningsinstrument, prop. 2009/10:122 s. 24.

[121] NJA 2022 s. 522 (”BankID-bedrägeriet”), om gränsen mellan ageranden som sker av grov oaktsamhet och ageranden som är särskilt klandervärda. Bankkunden lurades via telefonsamtal att medverka till att en bedragare kunde upprätta ett nytt mobilt BankID i kundens namn, vilket bedragaren sedan, och utan kundens vetskap, använde för att överföra cirka 400 000 kronor från kundens konto. Det sätt på vilket kunden medverkade var, utöver att på annans begäran använda sitt BankID och sin bankdosa för att legitimera sig, att ge ut åtminstone en svarskod från bankdosan till bedragaren. Högsta domstolen bedömde att bankkundens agerande inte var att bedöma som särskild klandervärt, och ansvaret begränsades till 12 000 kronor i enlighet med bestämmelsen i 5 a kap. 3 § andra stycket betaltjänstlagen. Allmänna reklamationsnämnden (ARN) har därefter meddelat ett antal avgöranden, som kan ge viss ytterligare vägledning för bedömningen av ansvarsfördelningen enligt betaltjänstlagen, se t.ex. Aagaard, M., *ARN och obehöriga transaktioner*, SvJT 2023 s. 457.

[122] I Norge har man däremot valt att på samma sätt som ”kontotömning” behandla agerande som består i att använda någon annans e-legitimation för att upprätta kreditavtal i dennes namn, lov-2020-12-18-146 (finansavtaleloven) § 3–20.

(condictio indebiti). En anledning till detta har varit att det tidigare rått osäkerhet huruvida den omständigheten att innehavaren brustit i sin skyldighet att skydda e-legitimationen och dess tillhörande behörighetsfunktioner kan utgöra ett avtalsbrott som kan åberopas av andra än utställaren av den ifrågavarande e-legitimation. Kreditgivaren är i relation till avtalet för utställandet av e-legitimationen att anse som tredje man.

Det finns förhållandevis få överrättsavgöranden och praxis är inte helt entydig för de fall som har prövats rättsligt i detta avseende. Enligt vad som tidigare angetts gäller dock numera aktsamhetskraven även till förmån för tredje man. Detta torde innebära att den som överlämnar sin e-legitimation och säkerhetskod till en bedragare vilken, i innehavarens namn, ingår kreditavtal, kan bli ersättningsansvarig gentemot kreditgivaren på grund av avtalsbrott (bristande aktsamhet). I dessa fall finns i Sverige inte konsumentskyddande regler motsvarande betaltjänstlagens bestämmelser om betaltjänstleverantörens skyldighet att återställa kontot. Huruvida det finns anledning att överväga ett författningsreglerat konsumentskydd för dessa situationer ligger dock utanför ramen för vårt utredningsuppdrag.

Vissa åtgärder som kan minska risken för obehörig användning och missbruk av e-legitimationer

Lösenord eller aktiveringskod är, som framgått, nödvändiga för att använda en e-legitimation, exempelvis för inloggning för en digital tjänst eller betalningstransaktioner. I vissa fall ställs ytterligare krav.

Vid bl.a. inloggning online på betalkonto och vid betalningstransaktioner ska betaltjänstleverantören tillämpa stark kundautentisering (5 b kap. 4 § betaltjänstlagen).[123] I en av Kommissionen antagen förordning med tekniska standarder fastställs de krav som betaltjänstleverantörer ska efterleva i fråga om att genomföra säkerhetsåtgärder så att det blir möjligt för dem att bl.a. tillämpa förfarandet för en stark kundautentisering och skydda betaltjänstanvändarens personliga be-

[123] Enligt legaldefinitionen i 1 kap. 4 § betaltjänstlagen är det fråga om ”en autentisering som grundas på användning av två eller flera komponenter, kategoriserade som kunskap (något som bara användaren vet), innehav (något som bara användaren har) och unik egenskap (något som användaren är), som är fristående från varandra så att det förhållandet att någon har kommit över en av komponenterna inte äventyrar de andra komponenternas tillförlitlighet, och som är utformad för att skydda autentiseringsuppgifterna mot obehörig åtkomst”. Se mer om begreppet autentisering i avsnitt 3.4.

hörighetsuppgifter.[124] Förordningen innehåller regler om dynamiska kopplingar, dvs. vid den starka kundautentiseringen ska transaktionen kopplas till ett specifikt belopp och en specifik betalningsmottagare (artikel 5, se även 5 b kap. 4 § andra stycket betaltjänstlagen). Betalaren ska med andra ord informeras om belopp och mottagare när stark kundautentisering tillämpas för en betalning. Som tidigare nämnts anses e-legitimationen utgöra ett betalningsinstrument när det använts för att initiera en betalningstransaktion.

Vid autentisering i andra sammanhang, som t.ex. vid elektronisk underskrift i samband med avtalsingående, kan det däremot räcka med att genomföra autentiseringsprocessen en gång. I syfte att försvåra bedrägerier och identitetsrelaterad brottslighet lämnas information mot vilken tjänst som identifieringen sker eller för vad som skrivs under, och innehavare uppmanas att alltid kontrollera denna text så att den överensstämmer med innehavarens avsikt.

Parallellt med ändrade eller nya författningskrav pågår, enligt vad utredningen erfarit, ett kontinuerligt utvecklingsarbete med befintliga e-legitimationer för att höja säkerheten vid utgivning och användning, ofta i samverkan med rättsutredande myndigheter.

Ett exempel på en säkerhetshöjande åtgärd från senare tid är ”Säker start” för Mobilt BankID, som verifierar att det är samma person som använder e-tjänsten som identifierar sig med e-legitimationen. Säker start av BankID blir obligatorisk från och med maj 2024 för samtliga myndigheter, företag och organisationer som använder BankID i sina e-tjänster.[125] Motsvarande funktion (QR-kodsidentifiering) finns även för Freja+.[126]

Ett nyligen presenterat säkerhetskrav för att skaffa eller förnya ett Mobilt BankID på distans, liksom att genomföra betalningstransaktioner av stora belopp, är en digital kontroll av sökandens respektive innehavarens svenska pass eller nationella identitetskort.[127] Kravet ökar

[124] Kommissionens delegerade förordning (EU) 2018/389 av den 27 november 2017 om komplettering av Europaparlamentets och rådets direktiv (EU) 2015/2366 vad gäller tekniska tillsynsstandarder för sträng kundautentisering och gemensamma och säkra öppna kommunikationsstandarder. I förordningen finns även tekniska krav, vilka ska uppfyllas utöver dem i eIDAS-regelverket när en e-legitimation används som ett betalningsinstrument.
[125] Säker start innebär att användning av e-legitimationer för alla e-tjänster behöver startas med (i) autostart när e-tjänst och BankID används i samma enhet, eller (ii) rörlig QR-kod när e-tjänst och BankID används i olika enheter, se www.bankid.com/tekniska-uppdateringar/saker-start-blir-tvingande-fran-1-maj-2024 (hämtad 2023-07-15).
[126] frejaeid.com/qr-koder-och-freja-eid/ (hämtad 2023-08-18).
[127] www.bankid.com/privat/skaffa-bankid (hämtad 2023-09-20). Det är den bank som utfärdar den ifrågavarande e-legitimationen som självständigt avgör tillämpningen av säkerhetskravet.

säkerheten men förutsätter samtidigt att personen i fråga har erforderlig identitetshandling och en smarttelefon med NFC-funktion för att trådlöst kunna avläsa identitetshandlingen.[128] Den som saknar en eller båda förutsättningarna är hänvisad att uppsöka ett bankkontor. Även Freja+ kan tillhandahållas på distans genom det beskrivna förfarandet.[129]

Behov av författningsreglering vid användning av den statliga e-legitimationen

Även om utfärdande och användning av befintliga e-legitimationer är i huvudsak avtalsstyrt finns det, som framgått, rörelselagstiftning samt civil- och straffrättslig reglering som kan tillämpas vid användning och missbruk av e-legitimationer. Befintlig reglering gäller oberoende av om det är e-legitimationer som utställts av kommersiella aktörer eller en statlig e-legitimation. Likväl måste det, för att en statlig e-legitimation ska kunna användas nationellt, etableras en relation mellan utfärdaren och förlitande parter motsvarande vad som gäller för de befintliga, kommersiella e-legitimationerna (se avsnitt 7.4.3).

I likhet med vad som anfördes av 2017 års id-kortsutredning finns det – även om avsikten är att den statliga e-legitimationen ska kunna användas brett – behov av att kunna meddela föreskrifter om villkor avseende i vilka situationer eller hos vilka aktörer den statliga e-legitimationen ska kunna användas (se även avsnitt 7.13). Som exempel angavs krav för att en aktör ska få använda identifiering med den statliga e-legitimationen i sin digitala tjänst. Sådana villkor kan exempelvis behövas för att säkerställa att den statliga e-legitimationen inte används i oseriösa sammanhang.[130] Ett annat tänkbart villkor för ökad säkerhet kan vara kontroll av biometriska uppgifter i samband med id-växling eller vid betalningstransaktioner över visst belopp (se även avsnitt 7.2).[131]

[128] Akronymen står för Near Field Communication, som är en standard för överföring av data, kontaktlöst över korta sträckor, vilken standardiseras av NFC-forum.
[129] frejaeid.com/registrering/ (hämtad 2023-09-20).
[130] *Ett säkert statligt id-kort – med e-legitimation* (SOU 2019:14), s. 344.
[131] Även Utredningen om effektiv styrning av nationella digitala tjänster föreslog föreskriftsrätt för bl.a. villkor för id-växling. Samtidigt gjordes bedömningen att den utfärdande myndighetens ansvar omfattar att verifiera identiteten hos en användare som ansöker om id-växling, men inte för den andra utfärdarens fortsatta hantering av uppgifterna om personen i fråga, se *reboot – omstart för den digitala förvaltningen* (SOU 2017:114) s. 203.

Likaså kan det, enligt vår bedömning, finnas ett behov att uppställa aktsamhetskrav på innehavare av en statlig e-legitimation, motsvarande de som enligt avtal gäller för befintliga e-legitimationer. Regeringen eller den myndighet regeringen bestämmer bör därför få meddela föreskrifter om villkor för när och hur den statliga e-legitimationen får användas.

7.9 Finansiering av den statliga e-legitimationen

Utredningens förslag: Kostnaderna för utfärdandet av den statliga e-legitimationen och grundidentifieringen ska i huvudsak finansieras via anslag.

Den som ansöker om en statlig e-legitimation ska betala en avgift. För prövning av ansökan gäller i övrigt bestämmelserna gäller bestämmelserna i 11–14 §§ avgiftsförordningen (1992:191).

Användningen av statlig e-legitimation ska ske på samma kommersiella villkor inom offentlig förvaltning som kommersiella e-legitimationer enligt gällande valfrihetssystem eller kommande auktorisationssystem.

Utredningens bedömning: Avgiften för att få en statlig e-legitimation och avgifter för användning av e-legitimationen kommer att bidra med viss, men inte full, kostnadstäckning.

Om den statliga e-legitimationen utfärdas på en fysisk identitetshandling bör en samordnad kostnad övervägas.

Skälen för utredningens bedömning och förslag

Våra förslag om att staten ska tillhandahålla en statlig e-legitimation innebär att verksamheter bestående i att utfärda en statlig e-legitimation, liksom att genomföra grundidentifiering behöver etableras. Denna etablering kommer främst att medföra fasta kostnader, varför antalet utfärdade e-legitimationer inte kommer vara av avgörande betydelse i kostnadshänseende. En stor volym utfärdade statliga e-legitimationer kan leda till ökade kostnader, men då som en följd av hantering av ökande ansökningsvolymer, supportärenden, transaktionsvolymer för nätverk och system samt ökat redundansbehov.

Med hänsyn till att antalet e-legitimationer inte är kostnadsdrivande framstår en modell med avgiftsfinansiering därmed inte som lämplig. En sådan modell skulle förutsätta en hög ansökningsavgift, vilket i motsats till syftet med våra förslag, skulle minska intresset för – och användningen av – den statliga e-legitimationen. Vi ser emellertid ett värde i att innehavet av en statlig e-legitimation är förknippat med en kostnad eftersom e-legitimationen är och behöver betraktas som en värdehandling.

I likhet med vad som gäller för befintliga statliga identitetshandlingar bör det införas en bestämmelse om att en avgift ska betalas vid ansökning om den statliga e-legitimationen samt en hänvisning till bestämmelserna i 11–14 §§ avgiftsförordningen (1992:191). Avgiften bör som utgångspunkt motsvara den som erläggs vid ansökan om pass eller nationellt identitetskort. Om den statliga e-legitimationen, på det sätt som vi menar är lämpligt (se avsnitt 7.2.2), i ett senare skede kommer tillhandahållas på en statligt utfärdad fysisk id-handling bör en samordnad kostnad övervägas.

Vi bedömer att den statliga e-legitimationen av konkurrensskäl ska hanteras på samma sätt som de kommersiella e-legitimationerna i samband med användning (se mer om detta i avsnitt 7.13). Den statliga e-legitimationen kommer därmed att kunna användas för identifiering i den offentliga förvaltningens digitala tjänster på samma villkor som de kommersiella e-legitimationerna i valfrihetssystemen eller kommande auktorisationssystem. Även om den statliga e-legitimationen enligt vår bedömning initialt inte kommer att utfärdas i sådana volymer att den genererar några omfattande intäkter, kommer intäkter från förlitande parter att bidra till viss kostnadstäckning.

Vi bedömer i likhet med Digg att anslagsfinansiering är en förutsättning för att långsiktigt bygga upp verksamheten med att utfärda den statliga e-legitimationen.[132] Verksamheten med att utföra grundidentifiering kan enligt vår bedömning delvis finansieras via avgiften för den statliga e-legitimationen, men kommer därutöver att kräva kompletterande anslagsfinansiering.

[132] Myndigheten för digital förvaltning, *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, s. 90.

7.10 Konkurrensrättsliga frågor

7.10.1 Den statliga e-legitimationen ska vara ett komplement till privata alternativ

Utredningens bedömning: Syftet med den statliga e-legitimationen är inte att den ska vara en konkurrent till befintliga privata alternativ.

Införandet av en statlig e-legitimation kan bidra till bättre förutsättningar för en ökad konkurrens på e-legitimationsområdet.

Skälen för utredningens bedömning

Syftet med den statliga e-legitimationen är inte att ersätta befintliga aktörers lösningar utan att vara ett komplement till de kommersiella alternativ som finns på marknaden (se mer om de privata utfärdarna i avsnitt 4.4). Trots den avsikten kommer den statliga e-legitimationen oundvikligen att i viss omfattning konkurrera med privata aktörer.

Givet rätt förutsättningar kan en ökad konkurrens emellertid också bidra till utvecklingen på området. I kommittédirektiven till Utredningen om effektiv styrning av nationella digitala tjänster framhölls att privat sektors medverkan i utveckling och leverans av digitala tjänster är en nyckelfaktor för tillväxt och innovation samt för att tillvarata teknikens möjligheter. Vi ansluter oss till såväl den uppfattningen som till den att ett positivt samspel mellan offentlig och privat sektor kan bidra till förnyelse i offentlig verksamhet och samtidigt leda till innovation och internationell konkurrenskraft i näringslivet.[133] Vi ser nämligen att införandet av en statlig e-legitimation, särskilt genom att erbjuda nya valmöjligheter, kan bidra till att skapa bättre förutsättningar för en ökad konkurrens på e-legitimationsområdet. Detta kan bl.a. ske genom att den id-växling som den statliga e-legitimationen möjliggör kan minska tröskeln för nya aktörer att ta sig in på marknaden.

En förbättrad konkurrens kommer emellertid inte per automatik att uppstå till följd av att en statlig e-legitimation införs, men de förslag som lämnas i avsnitt 7.13 kommer enligt vår bedömning skapa bättre förutsättningar för konkurrens mellan olika e-legitimationer vid användning av den offentliga sektorns tjänster. Bristande konkurrens

[133] Dir. 2016:39.

finns även inom den privata sektorn men eventuella överväganden i det avseendet ligger utanför ramen för vårt uppdrag.[134]

För vår del är det i stället relevant att ur ett konkurrensrättsligt perspektiv överväga på vilka villkor och i vilka tjänster den statliga e-legitimationen ska erbjudas. Vid dessa överväganden är offentliga aktörers handlingsalternativ vid anskaffande av e-legitimationer, liksom hur de bör erbjudas inom privat sektor av betydelse.

7.10.2 Konkurrensrättsliga överväganden

Utredningens bedömning: Statens verksamhet att tillhandahålla en e-legitimation kommer att utgöra en ekonomisk verksamhet för vilken vissa förfaranden omfattas av förbudet mot konkurrensbegränsande offentlig verksamhet.

Skälen för utredningens bedömning

Konkurrensbegränsande offentlig säljverksamhet

I 3 kap. 27 § konkurrenslagen (2008:579) finns en konfliktslösningsregel som kan tillämpas vid konkurrensbegränsande offentlig säljverksamhet i kommunal eller statlig regi.[135] Regeln innebär, för statlig verksamhets del, att staten får förbjudas att i sådan säljverksamhet som omfattas av konkurrenslagen tillämpa ett visst förfarande om förfarandet:

– snedvrider eller är ägnat att snedvrida förutsättningarna för en effektiv konkurrens på marknaden, eller
– hämmar eller är ägnat att hämma förekomsten eller utvecklingen av en sådan konkurrens.

[134] Se bl.a. avsnitt 7.13.4 samt ett vidare resonemang om konkurrensen på betalmarknaden och e-legitimationens roll i det sammanhanget se *Betalningsutredningen* (SOU 2023:16), avsnitt 8.8 och kapitel 9.

[135] I lagens förarbeten (prop. 2008/09:231 s. 35) angavs att konkurrenssnedvridningar som följd av offentlig säljverksamhet i allmänhet har sin grund i att staten, kommunen eller landstinget kan bedriva sådan verksamhet utan några påtagliga risker för verksamhetens existens, eftersom dessa aktörer inte kan försättas i konkurs. Därmed verkar offentliga aktörer på marknaden under andra förutsättningar än vad privata företag gör.

Med säljverksamhet avses en offentlig verksamhet av ekonomisk eller kommersiell natur. Verksamheten behöver inte vara inriktad på ekonomisk vinst för att omfattas av bestämmelserna. Tillämpning av konfliktlösningsregeln kräver inte heller att en offentlig aktör har en dominerande ställning eller har ingått något avtal. För den del av verksamheten som består i myndighetsutövning är bestämmelserna inte tillämpliga.[136]

En konkurrensbegränsning innebär att en offentlig aktör snedvrider eller hämmar en effektiv konkurrens. Begreppet snedvrida avser situationen att konkurrens inte råder på så lika villkor som möjligt, exempelvis eftersom den offentliga aktören behandlar företag olika utan saklig grund eller drar oberättigade fördelar av en myndighetsroll vid sidan av säljverksamheten. Begreppet hämma tar sikte på förfaranden som leder till att privata alternativ faller bort eller att privata aktörer över huvud taget inte träder in på marknaden. Det kan även vara så att de privata företagens tillväxt och utveckling i övrigt hejdas eller på annat sätt hålls tillbaka.[137]

Det är Konkurrensverket som utreder om ett agerande skadar drivkrafterna till konkurrens på en viss marknad. Utgångspunkten för bedömningen är om konkurrenstrycket på den relevanta marknaden ökar eller minskar till följd av en offentlig aktörs beteende. Det är de långsiktiga effekterna som ska beaktas och inte vad som sker eller kan ske på kort sikt. Neutrala beteenden påverkar inte konkurrensen och en offentlig aktör kan exempelvis ha rätt att upprätthålla service och annan infrastruktur på områden där det saknas ett kommersiellt utbud.[138]

Förbud får inte meddelas för förfaranden som är försvarbara från allmän synpunkt. I förarbetena till bestämmelsen angavs som en väsentlig utgångspunkt för regeringens förslag att det, vid tillämpning av konfliktlösningsregeln, måste vara möjligt att ta hänsyn till andra allmänna intressen än konkurrensintresset som kan uppväga den konkurrenssnedvridning som ett visst beteende kan ge upphov till. Beteenden som kunde försvaras från allmän synpunkt skulle enligt regeringen inte förbjudas med stöd av konfliktlösningsregeln. Huruvida försvarbarhet föreligger eller inte skulle enligt regeringen prövas i det särskilda fallet. En för bedömningen viktig faktor angavs dock vara om det konkurrensfientliga beteendet följer av lag, en annan författning eller något

[136] Prop. 2008/09:231 s. 56 f.
[137] Konkurrensverket, *Offentligt privat, Konkurrens i kristider, Analys i korthet* (Rapport 2023:5), s. 7.
[138] Konkurrensverket, *Tio år med bestämmelser om konkurrensbegränsande offentlig säljverksamhet – Kommuners säljverksamhet i fokus*, (Rapport 2020:2), s.21.

annat för den offentliga aktören bindande direktiv, t.ex. bolagsordning eller ägardirektiv. Vidare skulle motiven för det konkurrenssnedvridande beteendet vägas in i bedömningen. Externa motiv, dvs. det allmännas behov av att säljverksamheten bedrivs, skulle kunna göra ett beteende försvarbart. Slutligen angavs att det borde beaktas om det fanns någon annan väg att tillgodose det andra intresset än just det beteende som skadar konkurrensen när konkurrensintresset vägdes mot ett belagt annat allmänt intresse. För det fall andra möjligheter att tillgodose det allmänna intresset fanns skulle det aktuella beteendet inte anses försvarbart från allmän synpunkt.[139]

Patent- och marknadsdomstolen är behörig domstol och talan om förbud kan i första hand väckas av Konkurrensverket. Om Konkurrensverket för ett visst fall beslutar att inte väcka talan om förbud kan talan väckas av de företag som själva berörs av förfarandet eller verksamheten.[140]

Vår bedömning är att utfärdande av en statlig e-legitimation kommer att utgöra ekonomisk verksamhet i konkurrenslagens mening eftersom den kommer att verka på samma konkurrensutsatta marknad som de privata alternativen. Förfaranden som snedvrider eller hämmar konkurrensen och inte är försvarbara från allmän synpunkt kan alltså riskera att förbjudas. Det är därför relevant att överväga vilka åtgärder som kan vidtas för att åstadkomma ett så konkurrensneutralt agerande som möjligt. Vidare finns det – i de fall en viss konkurrenssnedvridning framstår som oundviklig – skäl att överväga om några åtgärder kan och bör vidtas för att säkerställa och tydliggöra att en statlig e-legitimation tillgodoser samhälleliga intressen som överväger intresset av att säkerställa konkurrens på lika villkor.

7.10.3 Den statliga e-legitimationen ska verka på lika villkor som de privata alternativ som finns på marknaden

Utredningens bedömning: Genom att den statliga e-legitimationen anmäls till valfrihetssystemen eller auktorisationssystemen dit även privata aktörer kan ansluta sig undviks konkurrensbegränsningar till följd av:

[139] Prop. 2008/09:231 s. 37f.
[140] 3 kap 27 och 32 §§ konkurrenslagen.

– underprissättning,
– att företag behandlas på olika sätt utan godtagbara skäl eller
– att företag nekas tillträde till strategiska nyttigheter.

Skälen för utredningens bedömning

Den statliga e-legitimation vi föreslår är, liksom den som Digg, 2017 års ID-kortsutredning och Utredningen om effektiv styrning av nationella digitala tjänster föreslagit, avsedd att vara ett komplement till de e-legitimationer som utfärdas av privata aktörer. För att uppnå ett så stort mått av konkurrensneutralitet som möjligt bör den statliga e-legitimationen, undantaget anslagsfinansieringen, som utgångspunkt verka under liknande villkor som gäller för de privata aktörerna på marknaden.

Ett ökat konkurrenstryck leder till att samhällets resurser används mer effektivt. Generellt sett ökar risken för skada på konkurrensen, som följd av en viss verksamhet eller förfarande, ju högre marknadsandel den offentliga aktören har. Det bör dock påpekas att reglerna om konkurrensbegränsande offentlig säljverksamhet är dynamiska – det som begränsar konkurrensen i ett fall behöver inte göra det i ett annat och kan förändras över tid.[141]

Förfaranden som kan snedvrida eller hämma en effektiv konkurrens är exempelvis underprissättning, att behandla företag på olika sätt utan godtagbara skäl, att neka tillträde till strategiska nyttigheter eller att blanda myndighetsutövning med affärsverksamhet.[142] Låga priser är som utgångspunkt bra för konsumenterna, men kan också hämma eller snedvrida konkurrensen om effektiva företag, till följd av den offentliga aktörens prissättning, slås ut eller inte vill träda in på marknaden.

Vårt förslag är att den statliga e-legitimationen ska anmälas till valfrihetssystemet eller eventuellt kommande auktorisationssystem och att det ska vara obligatoriskt för alla offentliga aktörer och vissa privata utförare av offentligfinansierad verksamhet att godta de e-legitimationer som ingår i auktorisationssystemen (se avsnitt 7.13). Till dessa system ska det även, enligt den nyligen lämnade propositionen om auk-

[141] Konkurrensverket, *Konkurrensbegränsande offentlig säljverksamhet. Så fungerar reglerna i konkurrenslagen*, juli 2019.
[142] Konkurrensverkets rapport, *Offentligt privat, Konkurrens i kristider, Analys i korthet,* (Rapport 2023:5), s. 8.

torisationssystem, vara möjligt för privata utförare av offentligfinansierad verksamhet att ansluta sig.[143]

I systemen erbjuds alla anslutna e-legitimationer på samma villkor, varför underprissättning, diskriminering eller uteslutning från strategiska nyttigheter i stor utsträckning undviks. Någon risk för att den statliga e-legitimationen kommer att få en så dominerande ställning på marknaden att det blir fråga om en situation med otillbörlig konkurrens framstår därmed inte som överhängande. Genom möjligheten att använda den statliga e-legitimationen för id-växling kan potentiellt kostnaderna för privata aktörer, och därmed även barriärerna för inträde på marknaden, sänkas. Något som kan leda till ökad konkurrens mellan privata utfärdare. Det kan dock finnas anledning för den utfärdande myndigheten att skapa rutiner för att följa upp utvecklingen i takt med att den statliga e-legitimationer blir mer etablerad.

7.10.4 Åtgärder för att säkerställa konkurrensneutralitet

Utredningens bedömning: För att säkerställa konkurrens på lika villkor bör den utfärdande myndigheten vidta åtgärder för att separera verksamheten med att tillhandahålla en statlig e-legitimation från annan verksamhet.

Skälen för utredningens bedömning

Enligt Konkurrensverket är det vanligt förekommande att privata aktörer upplever att statliga myndigheter agerar utanför sitt uppdrag. För att skapa så lika förutsättningar som möjligt bör därför som redan framgått konkurrensneutralitet eftersträvas. Åtgärder som kan vidtas för att åstadkomma konkurrensneutralitet är enligt Konkurrensverket att den offentliga säljverksamheten separeras organisatoriskt från annan verksamhet, att särredovisning sker och att verksamheten bedrivs på affärsmässig grund. Genom sådana åtgärder minskar risken för korssubventionering och otillbörligt gynnande av den egna affärsverksamheten.[144]

[143] Prop. 2023/24:6 s. 31 ff.
[144] Konkurrensverket, *Offentligt privat, Konkurrens i kristider, Analys i korthet* (Rapport 2023:5), s. 13. (I rapporten anges att Konkurrensverket uppmanar offentliga aktörer att anta en policy som föreskriver att deras säljverksamheter ska agera så konkurrensneutralt som möjligt).

Av våra direktiv framgår att Digg ska utfärda och tillhandahålla den statliga e-legitimationen. Det är också Digg som för närvarande beslutar vilka krav som ska uppfyllas för att en e-legitimationsutfärdare ska få ingå i valfrihetssystemen.[145] Vidare är det Digg som fattar beslut om e-legitimationsutfärdare uppfyller kraven för kvalitetsmärket Svensk e-legitimation. Digg kommer således i båda dessa avseenden att pröva sin egen verksamhet mot krav som myndigheten själv satt upp.

Digg uppmärksammar ifrågavarande rollkonflikter i sin rapport och redovisar där att myndigheten bl.a. avser att motverka dem genom organisatoriska åtgärder. [146] Enligt vår bedömning krävs det emellertid mer än organisatoriska åtgärder för att säkerställa långsiktig konkurrensneutralitet när riskerna för sammanblandning är så betydande. Se mer om problematiken kring Diggs dubbla roller i avsnitt 7.6.3 och 7.6.4.

7.10.5 Regler om statsstöd

Utredningens bedömning: Verksamheten med att tillhandahålla en statlig e-legitimation aktualiserar inte reglerna om statsstöd.

Skälen för utredningens bedömning

I sin rapport angav Digg att stadsstödsfrågor kopplade till den statliga e-legitimationen borde utredas vidare i ett nästa steg.[147]

Med statsstöd avses att det offentliga stödjer en ekonomisk verksamhet med offentliga medel och det resulterar i att mottagaren får en fördel, som påverkar konkurrensen och handeln mellan EU:s medlemsstater, gentemot andra aktörer på marknaden. Med det offentliga avses staten, kommuner eller regioner.

EU:s statsstödsregler finns i artiklarna 107–109 i fördraget om Europeiska unionens funktionssätt. Vidare finns bestämmelser om tillämpningen av statsstödsreglerna i lagen (2013:388) om tillämpning av Europeiska unionens statsstödsregler samt i de lagar och förordningar

[145] Digg föreslås också utses som tillhandahållande myndighet för ett kommande auktorisationssystem, se prop. 2023/24:6 s. 23.
[146] Myndigheten för digital förvaltning, *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, s. 61 ff.
[147] A.a. s. 96.

som svenska myndigheter tillämpar vid sin stödgivning (s.k. stödordningar).

Statsstödsreglerna finns för att skydda konkurrensen på EU:s inre marknad. Statsstöd kan, rätt utformat, ge företag inom EU förutsättningar att konkurrera på lika villkor och bidra till en hållbar utveckling, säkerställa infrastruktur, välfärd och konkurrenskraftiga företag.[148]

Den statsstödsrättsliga definitionen av ett företag motsvarar i stort den som gäller enligt konkurrenslagen. All verksamhet, oavsett om den är vinstdrivande eller inte, som går ut på att erbjuda varor och tjänster på en marknad utgör en ekonomisk verksamhet och är således att betrakta som ett företag. Det innebär att en verksamhet som bedrivs av en myndighet i egen regi kan betraktas som ett företag enligt statsstödsreglerna.[149]

Verksamheten med att tillhandahålla en statlig e-legitimation skulle i och för sig kunna omfattas av företagsbegreppet. Det är emellertid inte fråga om en verksamhet som kan påverka konkurrensen och handeln mellan EU:s medlemsstater. Vår bedömning är därför att reglerna om statsstöd inte blir tillämpliga till följd av våra förslag.

7.11 Behandling av personuppgifter

7.11.1 Dataskyddsförordningen är tillämplig

Utredningens bedömning: Dataskyddsförordningen är tillämplig vid den personuppgiftsbehandling som sker vid tillhandahållande av en statlig e-legitimation. Även dataskyddslagen och förordningen med kompletterande bestämmelser till EU:s dataskyddsförordning gäller vid personuppgiftsbehandlingen.

[148] www.upphandlingsmyndigheten.se/statsstod/statsstod-oversikt/ (hämtad 2023-10-02).
[149] www.upphandlingsmyndigheten.se/statsstod/vad-ar-statsstod/kriterier/foretagskriteriet/ (hämtad 2023-10-02).

Skälen för utredningens bedömning

Inledning och kort om gällande bestämmelser för personuppgiftsbehandling

Bestämmelser som reglerar personuppgiftsbehandling finns i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), här benämnd dataskyddsförordningen. Förordningen är direkt tillämplig i varje medlemsstat, men både förutsätter och tillåter att det i vissa fall finns nationella bestämmelser som kompletterar eller utgör undantag från förordningens regler. I Sverige finns sådana bestämmelser i lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) och förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning (kompletteringsförordningen).

Ett av dataskyddsförordningens syften är att skydda enskildas grundläggande rättigheter och friheter, särskilt rätten till skydd för personuppgifter. Rätten till skydd för privatlivet framgår också av artikel 8 i den Europeiska konventionen om skydd för de mänskliga rättigheterna och grundläggande friheterna samt av artikel 7 i EU:s stadga om de grundläggande rättigheterna. I artikel 8 i stadgan anges även att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Vidare framgår av 2 kap. 6 § andra stycket regeringsformen att var och en gentemot det allmänna skyddas mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.

Personuppgifter kommer att behandlas hos den identitetskontrollerande och den utfärdande myndigheten

En förutsättning för att dataskyddsförordningen ska vara tillämplig är att personuppgifter behandlas. Med *personuppgifter* avses varje upplysning som avser en identifierad eller identifierbar fysisk person som är i livet. Avgörande är om den personuppgiftsansvarige eller någon annan kan knyta den aktuella uppgiften, ensamt eller i kombination

med andra uppgifter, till en individ. Vidare krävs att personuppgifterna *behandlas* och med det avses exempelvis insamling, registrering, lagring, bearbetning, utlämnande genom överföring, spridning eller radering.[150]

Vid grundidentifieringen och ansökan kommer den identitetskontrollerande myndigheten att på ett automatiserat sätt behandla personuppgifter som finns i de handlingar som sökanden presenterar. Handlingarna innehåller regelmässigt namn, personnummer eller annan unik identifierare och kan också innehålla biometriska uppgifter som ansiktsbilder och i vissa fall fingeravtryck. Utöver jämförelser med dessa handlingar kommer kontroller mot folkbokföringsdatabasen att behöva genomföras. Vidare kommer den identitetskontrollerade myndigheten att ta en ansiktsbild av sökanden och dennes fingeravtryck samt föra in ansiktsbilden i den utfärdande myndighetens register. Den identitetskontrollerande myndigheten kommer även att dela uppgifter med den utfärdande myndigheten.

Den utfärdande myndigheten kommer att ta emot personuppgifter från den identitetskontrollerande myndigheten. Därutöver kommer den utfärdande myndigheten inom ramen för ansökningsförfarandet att på ett automatiserat sätt behandla personuppgifter såsom personnummer, samordningsnummer, namn och adressuppgifter samt föra en databas över innehavare av den statliga e-legitimationen. Vidare kan det uppstå behov av att inhämta uppgifter från Skatteverkets system för distribution av folkbokföringsuppgifter (Navet).

Vid användningen av den statliga e-legitimationen kommer den utfärdande myndigheten också att lämna ut personuppgifter till förlitande parter i syfte att intyga att en viss identitet är kopplad till e-legitimationen samt att e-legitimationen är giltig och i bruk. Det är vid den behandlingen fråga om uppgifter som finns lagrade i bäraren av den statliga e-legitimationen. Om fråga uppkommer om felaktig användning kan kontroller i dessa avseenden liksom sådana med kopplingar till utfärdandeprocessen behöva utföras i efterhand.

[150] Se artikel 4.1 och 4.2 i dataskyddsförordningen samt skäl 26 och 27 till dataskyddsförordningen.

7.11.2 Personuppgiftsansvariga myndigheter

Utredningens bedömning: Den identitetskontrollerande myndigheten är personuppgiftsansvarig för den personuppgiftsbehandling som sker i samband med grundidentifieringen. För den behandling som sker vid ansökan är den identitetskontrollerande myndigheten personuppgiftsbiträde åt den utfärdande myndigheten.

Den utfärdande myndigheten är personuppgiftsansvarig för den personuppgiftsbehandling som sker i samband med utfärdandet och tillhandahållandet av den statliga e-legitimationen.

Utredningens förslag: Personuppgiftsansvaret för respektive myndighet ska framgå av bestämmelser i den föreslagna lagen om elektronisk identifiering.

Skälen för utredningens bedömningar och förslag

För bedömningen av integritetsriskerna kan rollfördelningen mellan de aktörer som kan komma att hantera personuppgifter kopplade till den statliga e-legitimationen vara relevant. I det sammanhanget har det betydelse vem som är personuppgiftsansvarig, om det föreligger gemensamt personuppgiftsansvar eller om behandling av personuppgifter sker genom ett personuppgiftsbiträde.

En personuppgiftsansvarig är enligt artikel 4.7 i dataskyddsförordningen en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. En personuppgiftsansvarig fastställer behandlingsändamålet och behandlingssättet, dvs. varför och hur en behandling ska utföras. Den personuppgiftsansvarige måste besluta angående både ändamål och behandlingssätt. Det är den personuppgiftsansvarige som har ansvaret för att behandlingen av personuppgifter följer dataskyddsförordningen. Vidare ska denne lämna information till de registrerade, föra ett register över behandlingar, vidta lämpliga säkerhetsåtgärder, anmäla personuppgiftsincidenter till tillsynsmyndigheten och utse dataskyddsombud. Det är till den personuppgiftsansvarige som de registrerade ska vända sig om de exempelvis vill begära rättelse eller radering av personuppgifter.

Av artikel 26 framgår att om två eller fler personuppgiftsansvariga gemensamt fastställer ändamålen med och medlen för behandlingen ska de vara gemensamt personuppgiftsansvariga. Gemensamt personuppgiftsansvar föreligger inte om de personuppgiftsansvariga har olika ändamål för behandlingen även om de gemensamt bestämt vilka ändamål var och en har.

Ett personuppgiftsbiträde är enligt artikel 4.8 i dataskyddsförordningen en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning. Personuppgiftsbiträdet får bara behandla personuppgifter enligt instruktioner från den personuppgiftsansvarige. Den personuppgiftsansvarige och personuppgiftsbiträdet ska reglera hanteringen dem emellan genom ett avtal.

Digg gjorde i sin rapport bedömningen att Digg, i egenskap av utfärdande myndighet, är personuppgiftsansvarig för den behandling som sker vid utfärdandet och tillhandahållandet av den statliga e-legitimationen. Vidare att den identitetskontrollerande myndigheten dels är personuppgiftsansvarig för den personuppgiftsbehandling som sker i samband med grundidentifieringen, dels personuppgiftsbiträde åt Digg för den personuppgiftsbehandling som i övrigt sker för Diggs räkning vid ansökan och utlämnande av e-legitimationen.[151]

Vi ansluter oss till Diggs bedömning och konstaterar att en uppdelning av ansvaret för personuppgiftsbehandlingen blir nödvändig vid en ordning där grundidentifieringen respektive utfärdandet hanteras av olika myndigheter.

Myndigheterna kommer att ha olika ändamål för sin behandling och precis som Digg anförde i sin rapport kommer den identitetskontrollerande myndigheten inte ha något eget inflytande över de personuppgifter som lämnas av sökanden i ansökningshandlingarna. På samma sätt ska inte heller Digg ha något eget inflytande över hur den identitetskontrollerande myndigheten utför själva grundidentifieringen. Den identitetskontrollerande myndigheten ska inte heller använda de uppgifter som samlas in vid grundidentifieringen för att registrera vem som innehar en statlig e-legitimation, utan endast meddela den utfärdande myndigheten om identiteten är styrkt eller inte. Det blir därför inte fråga om något gemensamt personuppgiftsansvar för de båda myndigheterna.

[151] Myndigheten för digital förvaltning, *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, s. 66 ff.

7.11.3 Centrala bestämmelser om personuppgiftsbehandling ska införas i lagen om elektronisk identifiering

Utredningens förslag: Centrala bestämmelser om personuppgiftsbehandling för att tillhandahålla en statlig e-legitimation ska finnas i den nya lagen om elektronisk identifiering.

Bestämmelserna om personuppgiftsbehandling i den nya lagen ska komplettera dataskyddsförordningen och dataskyddslagen.

Skälen för utredningens förslag

Vi har i avsnitt 7.1 redovisat våra överväganden avseende att centrala bestämmelser om personuppgiftsansvar och behandling av personuppgifter i verksamheten med att tillhandahålla en statlig e-legitimation bör regleras i lag.

Dataskyddsförordningen är direkt tillämplig vid den personuppgiftsbehandling som sker vid tillhandahållande av en statlig e-legitimation. Bestämmelserna i förordningen utgör en del av den svenska rättsordningen och kompletteras av dataskyddslagen som är subsidiär till andra lagar och förordningar. Genom de bestämmelser vi föreslår införs kompletterande bestämmelser till förordningen och dataskyddslagen vilket ska tydliggöras genom att en särskild bestämmelse med sådan innebörd införs i den nya lagen om elektronisk identifiering.

7.11.4 Ändamålen med personuppgiftsbehandlingen ska framgå av lagen

Utredningens förslag: Personuppgifter ska få behandlas av den identitetskontrollerande myndigheten om

- det är nödvändigt för att kunna styrka en sökandes identitet vid ansökan om statlig e-legitimation och
- säkerställa att en viss fysisk person kan kopplas till en viss statlig e-legitimation.

Personuppgifter ska få behandlas av den utfärdande myndigheten om

– det är nödvändigt för att handlägga och administrera ärenden om statlig e-legitimation, inklusive att föra en databas över statliga e-legitimationer,
– det är nödvändigt för att möjliggöra en säker användning.

Personuppgifter som har samlats in för ovan angivna ändamål ska även få behandlas

– om det är nödvändigt för att tillhandahålla information som behövs i Polismyndighetens verksamhet för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa uppbörd eller upprätthålla allmän ordning och säkerhet,
– om det är nödvändigt för att fullgöra uppgiftsutlämnande som sker i överensstämmelse med lag eller förordning, och
– för andra ändamål, under förutsättning att uppgifterna inte behandlas på ett sätt som är oförenligt med det ändamål för vilket uppgifterna samlades in.

Ändamålsbestämmelserna ska även omfatta sådan behandling av personuppgifter i verksamheten med att tillhandahålla en statlig e-legitimation som sker utanför databasen över statliga e-legitimationer.

Skälen för utredningens förslag

De övergripande ändamålen med personuppgiftsbehandlingen

En grundläggande princip är att personuppgifter endast får samlas in för särskilda uttryckligt angivna ändamål som också ska vara berättigade ur ett integritetsskyddsperspektiv.

Det övergripande ändamålet med den identitetskontrollerande myndighetens personuppgiftsbehandling i samband med grundidentifieringen är främst att på ett rättssäkert sätt identifiera den som ansöker om en statlig e-legitimation och säkerställa att en viss fysisk person kan kopplas till en viss statlig e-legitimation. Den behandling som sker för den utfärdande myndighetens räkning vid ansökan och utlämnande

av e-legitimationen sker för att myndigheten ska kunna behandla sökandens ansökan och sedan lämna ut e-legitimationen.

Det övergripande ändamålet med den utfärdande myndighetens personuppgiftsbehandling är att kunna handlägga och administrera ärenden om statlig e-legitimation samt att verksamheten med att utfärda den statliga e-legitimationen ska fungera på ett säkert och effektivt sätt.

Enligt vår bedömning är risken för att de insamlade uppgifterna kommer att behandlas för andra ändamål än de tillåtna, eller sådana sekundära ändamål som vi anser befogade, begränsad. Syftet med behandlingen är inte heller att kartlägga eller övervaka den enskilde.

Särskilda ändamål ska författningsregleras

Såväl den identitetskontrollerande som den utfärdande myndigheten måste behandla personuppgifter inom ramen för verksamheten med att tillhandahålla en statlig e-legitimation. Som redovisats ovan får insamling av personuppgifter ske för särskilda, uttryckligen angivna samt berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Denna princip om ändamålsbegränsning i dataskyddsförordningen är central i regelverket om dataskydd.

Bestämmelserna i dataskyddsförordningen medger att särskilda ändamålsbestämmelser införs i nationell rätt (artikel 6.4 och 23.2 a). Med hänsyn till den stora mängd personuppgifter som en databas över statliga e-legitimationer kan förväntas innehålla anser vi att det finns skäl att författningsreglera särskilda ändamålsbestämmelser. Vilka specifika uppgifter som samlas in och hur de hanteras bör dock framgå av de materiella författningsbestämmelserna. Det är därför inte nödvändigt att i en ändamålsbestämmelse räkna upp samtliga de åtgärder som medför personuppgiftsbehandling. Bestämmelserna måste dock uppnå ett visst mått av konkretion för att fylla en funktion.

Enligt vår bedömning ska den bestämmelse som reglerar den identitetskontrollerande myndighetens primära ändamål utformas utifrån att ändamålet med personuppgiftsbehandlingen är att styrka en sökandes identitet vid en ansökan om statlig e-legitimation och säkerställa att en viss fysisk person kan kopplas till en viss statlig e-legitimation. Med en sådan formulering ryms enligt vår uppfattning samtliga de åtgärder som behöver genomföras vid grundidentifieringen, men ges också en yttre ram för behandlingen.

För den utfärdande myndigheten bör bestämmelsen utformas på så sätt att personuppgifter får behandlas om det är nödvändigt för att handlägga och administrera ärenden om statlig e-legitimation, inklusive att föra en databas över statliga e-legitimationer och för att möjliggöra en säker användning. Det senare innefattar exempelvis att säkerställa att inte flera statliga e-legitimationer utfärdas till samma person, att e-legitimationen ska kunna användas i förlitande tjänster för elektronisk identifiering och elektroniskt undertecknande samt att motverka att den statliga e-legitimationen används vid identitetsrelaterad brottslighet. Formuleringen innehåller en sådan generell skrivning som har ansetts tillräcklig exempelvis i lagen om identitetskort för folkbokförda (se 12 §), men tydliggör också att behandlingen även avser den fortsatta användningen av e-legitimationen.

Enligt vår bedömning finns det inte skäl att tillåta *insamling* av personuppgifter för några andra ändamål än dessa. Bestämmelsen kommer därmed innehålla en uttömmande reglering av de ändamål som den identitetskontrollerande respektive den utfärdande myndigheten får samla in personuppgifter för med stöd av lagen.

Det finns skäl att reglera personuppgiftsbehandling för vissa sekundära ändamål

Inom ramen för Polismyndighetens huvuduppgift att förebygga, förhindra och upptäcka brottslig verksamhet, utreda och lagföra brott samt upprätthålla allmän ordning och säkerhet kan det finnas behov av att få tillgång till personuppgifter som har samlats in i verksamheten med att tillhandahålla en statlig e-legitimation.

I departementspromemorian *Passdatalag – en ny lag som kompletterar EU:s dataskyddsförordning* redovisades att Polismyndigheten i sin brottsbekämpande verksamhet inte sällan använder personuppgifter som samlats in i passverksamheten. Som exempel angavs att fotografier i passregistret används vid fotokonfrontationer och spaningsarbete. Enligt promemorian fanns det goda skäl för att Polismyndigheten ska få använda sig av personuppgifter från passverksamheten för att bekämpa och lagföra brott samt upprätthålla allmän ordning och säkerhet. Utan en specifik ändamålsbestämmelse skulle det enligt promemorian kunna uppfattas som oklart om behandling för sådana ändamål är förenlig med det ändamål som personuppgifterna har samlats in för, dvs. handläggning av passärenden. Vid bedömningen av

integritetsriskerna med en sådan behandling anfördes bl.a. att brottsbekämpning, lagföring och upprätthållande av allmän ordning och säkerhet är viktiga samhällsintressen som erkänns även i dataskyddsförordningen. Vidare angavs att brottsdatalagen (2018:1177) och lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område, vars uttryckliga syften är att skydda fysiska personers grundläggande rättigheter och friheter, kommer att gälla om personuppgifter från passverksamheten behandlas för de angivna ändamålen. Behandlingen skulle alltså omfattas av lagarnas bestämmelser om bl.a. rättslig grund, ändamål, lagringstider och överföring till tredjeland och stå under tillsyn av dåvarande Datainspektionen samt Säkerhets- och integritetsskyddsnämnden. Enligt promemorian skulle en behandling för brottsbekämpande ändamål därmed omfattas av ett väl utvecklat regelverk till skydd för den enskildes personliga integritet. Slutligen anfördes att personuppgifterna i passverksamheten ofta är av mindre integritetskänsligt slag och att flertalet personuppgifter samlats in direkt från den enskilde. Motsvarande bedömningar gjordes även av 2017-års ID-kortsutredning.[152]

Vi anser att det – på samma sätt som inom passverksamheten – finns goda skäl för att Polismyndigheten för vissa ändamål ska få använda sig av personuppgifter från verksamheten med en statlig e-legitimation. De skäl som promemorian angav för att behovet överväger integritetsriskerna gäller enligt vår bedömning även för uppgifter som inhämtas i verksamheten med att tillhandahålla en statlig e-legitimation. En bestämmelse om rätt till personuppgiftsbehandling för angivet ändamål bör således föras in i lagen.

Personuppgifter som har samlats in i verksamheten med att tillhandahålla en statlig e-legitimation kan vidare behöva behandlas för att vara möjliga att lämna ut till andra myndigheter eller till enskilda. I ovan angiven promemoria konstaterades att en allmän förutsättning för utlämnande av uppgifter till andra får antas vara att uppgiftslämnandet sker i överensstämmelse med lag eller förordning, dvs. med stöd av bestämmelser som påbjuder eller tillåter utlämnande. Vidare framhölls att det vid införande av sådana bestämmelser får förutsättas att en avvägning mellan intresset av utlämnande och intresset av att skydda enskilda personers integritet har genomförts, samt att man vid den avvägningen har funnit att uppgiften ska eller får lämnas ut. Vi ansluter

[152] Se *Passdatalag – en ny lag som kompletterar EU:s dataskyddsförordning* (Ds 2019:5), s. 113 ff. och jfr *Ett säkert statligt ID-kort-med e-legitimation,* (SOU 2019:14), s. 265 f.

oss till den bedömningen och anser att det finns skäl att införa en bestämmelse som tillåter att personuppgifter behandlas för sådana ändamål. En sådan bestämmelse föreslogs också för passverksamhetens del i nämnd promemoria och av 2017-års ID-kortsutredning.[153]

Slutligen bör uppgifter kunna behandlas för andra sekundära ändamål under förutsättning att behandlingen inte är oförenlig med de ursprungliga ändamålen. Även om en sådan bestämmelse medför att det inte på förhand går att avgöra exakt vilka uppgifter som kan komma i fråga gör vi bedömningen att den föreslagna bestämmelsen är motiverad ur integritetssynpunkt. Vi bedömer, vilket också anfördes i promemorian om en ny passdatalag, att finalitetsprincipen i sig utgör en garant för att behandlingen inte får vara oförenlig med ursprungsändamålet. De personuppgifter som kommer att behandlas är inte heller av sådan integritetskänslig karaktär att föreslagen behandling framstår som utesluten. Motsvarande bestämmelse finns dessutom i lagen om identitetskort för folkbokförda och i flertalet registerförfattningar (exempelvis 7 § domstolsdatalagen [2015:728] och 4 § kriminalvårdsdatalagen [2018:1235]) samt föreslogs införas i en ny passdatalag och av 2017 års ID-kortsutredning.[154]

7.11.5 Lagen ska innehålla bestämmelser om databasen över statliga e-legitimationer

Utredningens förslag: Den utfärdande myndighetens rätt att föra en databas över statliga e-legitimationer ska framgå av lagen.

Databasen över statliga e-legitimationer ska få innehålla uppgifter om personer som är eller har varit parter i ett ärende om utfärdande av en statlig e-legitimation.

Nödvändiga preciseringar om exempelvis innehållet i databasen ska lämpligen framgå av den förordning som kompletterar den nya lagen om elektronisk identifiering.

[153] Se *Passdatalag – en ny lag som kompletterar EU:s dataskyddsförordning* (Ds 2019:5), s. 116 samt där gjorda hänvisningar och *Ett säkert statligt ID-kort-med e-legitimation* (SOU 2019:14), s. 262 f.
[154] *Ett säkert statligt ID-kort-med e-legitimation* (SOU 2019:14) , s. 263 och *Passdatalag – en ny lag som kompletterar EU:s dataskyddsförordning* (Ds 2019:5), s. 118 f.

Skälen för utredningens förslag

Tidigare författningsförslag har varit olika omfattande

För att det ska vara möjligt att på ett ändamålsenligt sätt tillhandahålla en statlig e-legitimation krävs att den utfärdande myndigheten ges rätt att föra en databas över statliga e-legitimationer. Tidigare författningsförslag har i fråga om vilka uppgifter registret ska få innehålla varit olika omfattande, sannolikt delvis eftersom de avsett olika identitetshandlingar.

Digg föreslog i sin rapport att det av en ny förordning skulle framgå att myndigheten ges rätt att föra ett register över innehavare av e-legitimationer. I registret skulle enligt Digg åtminstone följande uppgifter behandlas:

- uppgifter om sökandens namn, personnummer, dag för utfärdande och giltighetstid,
- uppgift om e-legitimationens unika identifierare (en hash[155] av den unika kryptografiska nyckeln) och serienummer, status för e-legitimationen såsom om den inte är aktiverad, om den är spärrad eller utgången,
- aktiveringskod (endast tillfällig uppgift[156]) och hash av innehavarens personliga kod,[157]
- kontaktuppgifter till innehavaren av e-legitimationen i form av e-post, bostadsadress och telefonnummer.[158]

2017 års ID-kortsutredning föreslog ett nytt id-kortsregister som skulle innehålla uppgifter om sökanden, utfärdade identitetskort och uppgifter från handläggningen av ärenden om identitetskort. Registret skulle enligt utredningen innehålla uppgift om den information som finns i den statliga e-legitimationen samt om att e-legitimationen har förlustanmälts eller återkallats och vad som har utgjort skälet därtill.

---

[155] Benämningen på svenska är *kondensat*.
[156] Koden skapas 24 timmar efter att kortet överlämnas till innehavaren, om aktivering sker enligt alternativ 3 i den process som redovisas i avsnitt 7.4.2. Aktiveringskoden är således i praktiken användarens första personliga kod fram tills dess att kortet aktiverats. Se vidare Myndigheten för digital förvaltning, *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, bilaga 1 s. 4 f.
[157] Ibid. Endast det underlag för nollkunskapsbevis som behövs för att verifiera den personliga koden ska lagas.
[158] A.a. s. 74.

De närmare bestämmelserna om innehållet i registret skulle enligt utredningen framgå av förordning. Enligt förordningen skulle, utöver kopia av ansiktsbild och biometriska uppgifter därur som angavs i lagen, följande uppgifter registreras:

– sökandens fullständiga namn, personnummer eller, i förekommande fall, samordningsnummer, födelsetid, svenskt medborgarskap, behövliga kontaktuppgifter, längd och kön,
– dag för utfärdande av identitetskortet, kortnummer och giltighetstid,
– sökandens namnteckning eller, i förekommande fall, anteckning om anledningen till att namnteckning saknas,
– hur sökanden har styrkt sin identitet,
– intygsgivare, bud, vittne och företrädare för inrättning för vård eller omsorg i förekommande fall,
– den information som finns i den e-legitimation som finns i lagringsmediet på identitetskortet,
– beslut om att ansökan har avslagits, skälen för detta beslut och uppgift om att ansökan har återkallats, och
– att identitetskortet eller e-legitimationen har förlustanmälts eller återkallats och vad som har utgjort skäl för beslutet om återkallelse.[159]

I promemorian om en ny passdatalag föreslogs att passregistret, för att kunna fylla sitt ändamål, skulle få innehålla uppgifter om personer som har eller har haft pass. De uppgifter som skulle få behandlas var följande:

– namn,
– person- eller samordningsnummer,
– medborgarskap,
– födelseort,
– kön,
– längd,

[159] *Ett säkert statligt ID-kort-med e-legitimation*, (SOU 2019:14), s. 55, 271 f. och 348 f.

– ansiktsbilder som tagits vid ansökan och biometriska uppgifter som tagits fram ur ansiktsbilderna,
– namnteckning som har lämnats vid passansökningar,
– uppgifter i handlingar som har kommit in eller upprättats,
– uppgifter om pass och handläggningen av ärenden om pass.[160]

Integritetsriskerna motiverar lagreglering

En databas över statliga e-legitimationer kommer, i vart fall på sikt, sannolikt att omfatta en stor del av befolkningen. Databasen ska enligt våra förslag, till skillnad från Diggs, även innehålla ansiktsbilder och biometriska uppgifter som tillsammans med andra personuppgifter kan medföra integritetsrisker. Detta är omständigheter som motiverar att bestämmelser om att en databas ska föras och hur känsliga personuppgifter får behandlas ska regleras i lag och inte förordning. Reglering om databasens innehåll i övrigt bör dock lämpligen framgå av förordning (se även avsnitt 7.1).

Databasen ska få innehålla uppgifter om personer som har eller har haft en statlig e-legitimation

En databas över statliga e-legitimationer behöver – även utan koppling till en annan fysisk id-handling på det sätt som utgjorde en förutsättning för 2017 års ID-kortsutredning – innehålla i stort sett samma uppgifter som då föreslogs. Vi anser därför att ytterligare uppgifter, utöver de som Digg föreslagit, behöver kunna tillföras databasen över statliga e-legitimationer.

Databasen bör få innehålla uppgifter om personer som har eller har haft en statlig e-legitimation, liksom uppgifter om personer som har ansökt men nekats, för att kunna fylla sitt ändamål.[161] En sådan möjlighet får anses utgöra en viktig säkerhetsfunktion för att kunna säkerställa att inga oriktigt utfärdade e-legitimationer förekommer. Som en integritetshöjande och lagringsminimerande åtgärd ska regler om gallringsfrister gälla (se avsnitt 7.11.8).

[160] *Passdatalag – en ny lag som kompletterar EU:s dataskyddsförordning* (Ds 2019:5), s. 130 f.
[161] Jfr *Passdatalag – en ny lag som kompletterar EU:s dataskyddsförordning* (Ds 2019:5), s. 130 för motsvarande uppfattning såvitt avser registerföring i förslag till ny passdatalag.

Enligt vår bedömning ska följande uppgifter få behandlas i en databas över statliga e-legitimationer:

- uppgifter om sökandens namn, person- eller samordningsnummer för personer med styrkt identitet, dag för utfärdande och giltighetstid,
- uppgift om e-legitimationens unika identifierare (ett kondensat av den unika kryptografiska nyckeln) och serienummer,
- aktiveringskod (tillfällig uppgift) och kondensat av innehavarens personliga kod
- kontaktuppgifter till innehavaren av e-legitimationen i form av e-post, bostadsadress och telefonnummer,
- uppgift om hur sökanden styrkt sin identitet,
- ansiktsbilder som tagits vid ansökan och de biometriska uppgifter som tagits fram ur dessa,
- status för e-legitimationen såsom om den inte är aktiverad, om den är spärrad, återkallad eller utgången,
- beslut om att en ansökan har avslagits och skälen för beslutet,
- beslut om att e-legitimationen återkallats och skälen för beslutet,
- uppgifter i handlingar som kommit in eller upprättats.

Enligt vår bedömning finns det inte skäl att registrera medborgarskap eller längd och kön på sökanden eftersom dessa uppgifter inte är direkt relevanta vid utfärdande av en statlig e-legitimation. Inte heller behövs uppgift om kortnummer eller namnteckningar eftersom kortnumret ersätts av serienummer och namnteckningen inte ska framgå av bäraren. Vi ser inte heller att uppgifterna är nödvändiga för att kunna säkerställa identiteten vid utfärdande av e-legitimationen. Vidare kommer det enligt våra förslag inte vara möjligt att ansöka om en statlig e-legitimation utan personlig inställelse, varför något behov av att registrera intygsgivare, bud, vittne eller företrädare för inrättning för vård eller omsorg inte föreligger.

Vid ansökan om en statlig e-legitimation får uppgifter om bl.a. namn och personnummer hämtas ur Skatteverkets folkbokföringsdatabas (se avsnitt 7.4.2). För att tydliggöra att databasen över den statliga e-legitimationen får tillföras sådana uppgifter bör en bestäm-

melse om detta föras in i den nya förordningen om elektronisk identifiering (jfr 12 § förordningen [2015:904] om identitetskort för folkbokförda i Sverige).

7.11.6 Förslagen är förenliga med de regelverk som styr behandlingen av personuppgifter

Utredningens bedömning: Den behandling av personuppgifter som förslagen ger upphov till är förenlig med EU:s dataskyddsförordning, dataskyddslagen och de föreskrifter som har meddelas med stöd av den lagen.

Skälen för utredningens bedömning

Utgångspunkter för behandlingen av personuppgifter

I artikel 5.1 dataskyddsförordningen stadgas vissa principer som måste uppfyllas vid varje behandling av personuppgifter. Enligt artikeln ska personuppgifter behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. Vidare anges att personuppgifterna ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål samt att de inte senare får behandlas på ett sätt som är oförenligt med dessa ändamål. Uppgifterna ska vara adekvata och korrekta och får inte förvaras under en längre tid än vad som är nödvändigt samt måste behandlas på ett sätt som säkerställer lämplig säkerhet.

Principerna i artikel 5.1 är – precis som de i artikel 6.1 som beskrivs nedan – grundläggande och kumulativa. Enligt artikel 5.2 är det den personuppgiftsansvariga som ansvarar för att principerna för personuppgiftsbehandlingen följs.

Om känsliga personuppgifter behandlas gäller att behandlingen ska kunna hänföras till något av undantagen i artikel 9.2 från det förbud som gäller enligt artikel 9.1. Behandling av person- eller samordningsnummer utan samtycke får endast ske när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl (artikel 87 och 3 kap. 10 § dataskyddslagen).

Dataskyddsförordningens krav på laglighet och rättslig grund för behandling av personuppgifter

För att personuppgiftsbehandling ska få ske i verksamheten med att tillhandahålla en statlig e-legitimation krävs som utgångspunkt att behandlingen har stöd i ett eller flera av de villkor som framgår av artikel 6.1 dataskyddsförordningen. Uppräkningen i artikel 6.1 är uttömmande. Om inget av de villkor som anges där är tillämpligt är behandlingen inte laglig och får inte utföras eftersom det då saknas rättslig grund för hanteringen.

Den rättsliga grunden för personuppgiftsbehandlingen vid tillhandahållandet av den statliga e-legitimationen finns i första hand i artikel 6.1 e, dvs. behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. När det gäller behandling som sker med stöd av artikel 6.1 e måste grunden för behandlingen enligt artikel 6.3 i dataskyddsförordningen fastställas i nationell rätt eller EU-rätt. I svensk rätt kan den rättsliga grunden för behandlingen fastställas i lag eller annan författning. Det är den rättsliga förpliktelsen, uppgiften av allmänt intresse eller rätten att utöva myndighet som ska fastställas i den rättsliga grunden, och inte själva personuppgiftsbehandlingen. [162]

Enligt artikel 6.3 andra stycket första meningen i dataskyddsförordningen ska syftet med behandlingen, i fråga om behandling enligt punkt 1 e, vara nödvändigt för att utföra en uppgift av allmänt intresse. Ändamålet med varje enskild behandling måste vara nödvändigt för att utföra den fastställda uppgiften. Bestämmelsen uttrycker det samband som måste finnas mellan behandlingen och den fastställda uppgiften och riktar sig till den som bestämmer de särskilda ändamålen för behandlingen, vilket i normalfallet är den personuppgiftsansvarige men i vissa fall även kan vara lagstiftaren. Detta krav på samband framgår även av artikel 5.1 b, där det anges att de särskilda ändamålen ska vara berättigade.[163]

En uppgift av allmänt intresse kan enligt 2 kap. 2 § dataskyddslagen följa av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. För myndighetsutövning gäller att denna ska ha stöd i lag eller annan författning.

[162] Prop. 2017/18:105 s. 46 ff.
[163] A.a. s. 56.

Att myndigheter kan sköta sina uppdrag på ett korrekt, rättssäkert och effektivt sätt är av allmänt intresse.[164] Myndigheters uppdrag och åligganden framgår av författningar och regeringsbeslut, antagna i enlighet med regeringsformens bestämmelser om normgivningskompetens. De åtgärder som en myndighet vidtar i syfte att utföra dessa uppdrag eller uppfylla dessa åligganden har därmed i sig en legal grund.

Uppgiften att tillhandahålla en statlig e-legitimation är alltså av allmänt intresse. Det är nödvändigt för såväl den identitetskontrollerande som den utfärdande myndigheten att behandla personuppgifter eftersom det är av avgörande betydelse att det går att säkerställa att en viss fysisk person kan kopplas till en viss e-legitimation innan en e-legitimation utfärdas. Vidare är det nödvändigt att den utfärdande myndigheten för en databas dels för att kunna säkerställa att inte flera statliga e-legitimationer utfärdas till en och samma person, dels för att administrera en återkallelse- och spärrfunktion. Eftersom vårt förslag innebär att verksamheten med att tillhandahålla en statlig e-legitimation regleras i lag kommer den rättsliga grunden framgå av nationell rätt.

7.11.7 Behandling av integritetskänsliga personuppgifter

Utredningens förslag: Känsliga personuppgifter ska få behandlas i verksamheten med att tillhandahålla en statlig e-legitimation om det är absolut nödvändigt för ändamålet med behandlingen.

Ansiktsbilden och de biometriska uppgifter som kan tas fram ur denna får lagras i databasen över statliga e-legitimationer. Dessa uppgifter ska som utgångspunkt inte vara tillåtna att använda som sökbegrepp utom vid ansökan om en statlig e-legitimation och då endast för att kontrollera om sökandens ansiktsbild finns i databasen.

Fingeravtrycken och de biometriska uppgifter som tas fram ur dessa får inte behandlas i databasen över statliga e-legitimationer och kan därmed inte användas som sökbegrepp. De får, liksom ansiktsbilden, behandlas i samband med grundidentifieringen och då lagras tillfälligt i ärendehanteringssystemet. När e-legitimationen lämnas ut eller då ansökan återkallas eller avslås ska fingeravtrycken och de biometriska uppgifterna som tagits fram ur dessa omedelbart förstöras.

[164] Prop. 2017/18:105 s. 85.

Utredningens bedömning: Den behandling av känsliga personuppgifter som föreslås vid grundidentifieringen, utfärdandet, tillhandahållandet och användningen i såväl den identitetskontrollerandes som den utfärdande myndighetens verksamhet är tillåten enligt artikel 9.2 g i dataskyddsförordningen.

Skälen för utredningens förslag och bedömning

Känsliga personuppgifter kommer att behandlas

I verksamheten med att tillhandahålla en statlig e-legitimation kommer vissa känsliga personuppgifter att behandlas. Med känsliga personuppgifter avses bl.a. personuppgifter som avslöjar ras eller etniskt ursprung och biometriska uppgifter för att entydigt identifiera en fysisk person. Biometriska uppgifter är enligt definitionen i artikel 4.14 i dataskyddsförordningen personuppgifter som erhållits genom en särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar identifieringen av denna person.

Vid grundidentifieringen kommer den identitetskontrollerande myndigheten behandla uppgifter om namn tillsammans med ansiktsbilder och fingeravtryck som – även om uppgifterna sedda för sig inte omfattas av dataskyddsförordningens definition – utgör känsliga personuppgifter. Vidare kommer biometriska uppgifter ur ansiktsbilderna och fingeravtrycken att samlas in och analyseras i syfte att identifiera sökanden och säkerställa att den identitetshandling som presenteras är äkta. Den identitetskontrollerande myndigheten behöver därtill behandla andra integritetskänsliga uppgifter såsom person- och samordningsnummer vid grundidentifieringen och – när uppgifterna förs in i den utfärdande myndighetens system – vid ansökan och utlämnande av den statliga e-legitimationen.

Den utfärdande myndigheten kommer att behandla person- och samordningsnummer, uppgifter om lagöverträdelser samt föra en databas över innehavare av statlig e-legitimation. Vi anser dessutom, till skillnad från Digg, att vid grundidentifieringen inhämtade ansiktsbilder och fingeravtryck samt dess biometriska uppgifter ska lagras i bäraren av e-legitimationen och att en kopia av ansiktsbilden och dess biometriska uppgifter ska sparas i databasen över statliga e-legitimationer.

Uppgifterna i bäraren och databasen ska kunna användas i jämförande syfte vid en ny ansökan om statlig e-legitimation.

Vid användningen av den statliga e-legitimationen ska ansiktsbilden och fingeravtrycken som finns lagrade i bäraren också kunna användas av förlitande parter för biometrisk autentisering i syfte att säkerställa att det är personen som den statliga e-legitimationen utfärdades till som också använder den. Det är i sådant fall fråga om personuppgiftsbehandling som sker i de förlitande parternas verksamhet och inte i verksamheten med att tillhandahålla en statlig e-legitimation.

Behandlingen av känsliga personuppgifter är tillåten

Behandling av känsliga personuppgifter är enligt huvudregeln i artikel 9.1 i dataskyddsförordningen förbjuden om inte något av undantagen i artikel 9.2 a–j är tillämpligt. Uppräkningen i artikel 9.2 är uttömmande men det är möjligt att införa mer specifika bestämmelser i fråga om behandling av känsliga personuppgifter som sker med stöd av artikel 6.1 c och e. Frågan är därmed om något av de undantag som räknas upp i artikel 9.2 är tillämpligt för den behandling som vi föreslår.

Enligt artikel 9.2 g får känsliga uppgifter behandlas om en behandling är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

Artikel 9.2 g kompletteras av bestämmelsen i 3 kap. 3 § dataskyddslagen. Av den bestämmelsen framgår att känsliga personuppgifter får behandlas av en myndighet med stöd av artikel 9.2 g i EU:s dataskyddsförordning om (1) uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag, (2) om behandlingen är nödvändig för handläggningen av ett ärende eller (3) i annat fall, om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse och inte innebär ett otillbörligt intrång i den registrerades personliga integritet.

Som tidigare konstaterats är verksamheten med att tillhandahålla en statlig e-legitimation ett viktigt allmänt intresse. När personuppgifter behandlas inom verksamheten är följaktligen behandlingen nöd-

vändig med hänsyn till ett viktigt allmänt intresse och behandling av känsliga personuppgifter är därmed också tillåten. En förutsättning är dock att det finns bestämmelser som medför ett skydd för den registrerades grundläggande intressen och rättigheter. Utöver behandlingen som sker för de primära ändamålen får den utfärdande myndighetens möjlighet att, i enlighet med föreslagna sekundära ändamål, lämna ut uppgifter när det följer av lag eller förordning anses ske för ett viktigt allmänt intresse. Detsamma gäller möjligheten att behandla personuppgifter för andra ändamål än det för vilket de samlades in eftersom behandlingen inte får vara oförenlig med de primära ändamålen.

Enligt vår bedömning får all personuppgiftsbehandling som är tillåten med stöd av de primära och sekundära ändamålen anses ske för ett viktigt allmänt intresse i enlighet med artikel 9.2 g i dataskyddsförordningen. De bestämmelser vi föreslår om reglering av personuppgiftsansvar, bestämda ändamål, sökbegränsningar, gallringsfrister, sekretess och rätt att överklaga tillgodoser kraven på skydd för den registrerades grundläggande intressen och rättigheter.

Sammanfattningsvis är den behandling av känsliga personuppgifter som kommer att ske tillåten enligt artikel 9.2 g i dataskyddsförordningen.

Behandlingen av känsliga personuppgifter ska vara absolut nödvändig

Att behandlingen av personuppgifter ska vara nödvändig enligt unionsrätten innebär inte ett krav på att den ska vara helt oundgänglig. Behandlingen kan exempelvis anses nödvändig om den leder till effektivitetsvinster.[165] Vi anser därför, i likhet med vad som föreslogs i promemorian med förslag till ny passdatalag, att det finns skäl att föreskriva att behandling av känsliga personuppgifter ska vara absolut nödvändig för ändamålet. Som anges i promemorian finns motsvande bestämmelser i flertalet registerförfattningar.[166]

[165] Prop. 2017/18:105 s. 46f och 189.
[166] *Passdatalag – en ny lag som kompletterar EU:s dataskyddsförordning* (Ds 2019:5), s. 140.

Ansiktsbilder och fingeravtryck i bäraren är nödvändiga av säkerhetsskäl

Våra förslag innebär som framgått en skyldighet för sökanden att låta den identitetskontrollerande myndigheten ta sökandens fingeravtryck och en digital ansiktsbild vid ansökan. Ansiktsbilden och fingeravtrycken ska sedan jämföras med sökandens befintliga identitetshandlingar och sparas i bäraren vilket innebär en integritetsrisk (se om grundidentifiering i avsnitt 7.5, utformningen i avsnitt 7.2.6 och om utgivningsprocessen i avsnitt 7.4.2). Förslagen innebär dock inte att det ska vara obligatoriskt att ansöka om en statlig e-legitimation, varför skyldigheten att lämna ifrån sig integritetskänsliga uppgifter såsom ansiktsbilder eller fingeravtryck inte kan sägas stå i strid med den enskildes grundläggande fri- och rättigheter. Motsvarande ordning gäller dessutom redan och har bedömts proportionerlig för pass och nationella id-kort. Enligt vår bedömning finns det inga skäl som motiverar en sämre möjlighet att koppla den statliga e-legitimationen till en fysisk person än vad som gäller för pass och nationella id-kort. Som 2017 års ID-kortsutredning konstaterade är användningen väl beprövad och det finns inga indikationer på något annat än att kontroll av sådana uppgifter är ett säkert sätt att fastställa kopplingen mellan en handling och en viss individ.[167]

Syftet med den behandling av känsliga personuppgifter som vi i detta avseende föreslår är att den statliga e-legitimationen ska vara tillräckligt säker. Den identitetsrelaterade brottsligheten ökar och har, som vi beskriver i avsnitt 6.7, ett nära samband med den organiserade brottsligheten. Det är mot den bakgrunden av avgörande betydelse att den statliga e-legitimationen tillhandahålls på ett sätt som försvårar en bedräglig användning så långt det är möjligt.

Införandet av ytterligare en bärare med integritetskänsliga uppgifter, om den statliga e-legitimationen inte utfärdas på ett statligt ID-kort som 2017 års ID-kortsutredning föreslog, kan visserligen tänkas både öka och minska riskerna ur ett integritetsskyddsperspektiv. Riskerna ökar eftersom fler handlingar innehåller integritetskänsliga uppgifter som riskerar att spridas, men minskar eftersom de olika identitetshandlingarna ofrånkomligt kan komma att användas vid utfärdande av vartannat och då behöver ha enhetliga säkerhetskrav.

[167] *Ett säkert statligt ID-kort – med e-legitimation (*SOU 2019:14), s. 291.

Enligt vår uppfattning framstår det – oavsett slutlig bärare av den statliga e-legitimationen – inte ändamålsenligt att ställa andra krav på en statlig e-legitimation än på andra identitetshandlingar. Vikten av att de identitetshandlingar som staten utfärdar uppnår en erforderlig säkerhetsnivå är avgörande. De risker som kan tänkas finnas för individen ur ett integritetsperspektiv övervägs enligt vår bedömning inte bara av statens intresse av säkra identitetshandlingar, utan också av individens berättigade behov av att kunna skydda sin identitet.

Tidigare utredningar har föreslagit sökmöjlighet på biometriska uppgifter i register

Efter att grundidentifieringen genomförts och den statliga e-legitimationen lämnats ut måste insamlade ansiktsbilder och fingeravtryck hanteras. För pass och nationella id-kort gäller i dag att ansiktsbilder får sparas i passregistret respektive registret över nationella id-kort. Det är dock inte tillåtet att spara fingeravtryck, biometriska uppgifter från ansiktsbilder och fingeravtryck eller att söka automatiserat i registren.

2017 års ID-kortsutredning, vars förslag som framgått bereds i Regeringskansliet, ansåg att det fanns skäl att göra nya överväganden avseende möjligheten att göra automatiserade sökningar på samtliga ansiktsbilder i det av utredningen föreslagna registret. Enligt utredningen skulle det, genom en jämförelse av ansiktsbilderna i registret med sökandens, vara möjligt att upptäcka om en person ansökte om identitetshandlingar för flera identiteter. Som skäl för sin ståndpunkt anförde utredningen, efter en redovisning av förarbetsuttalanden i vilka man inte funnit skäl att införa ifrågavarande möjlighet, bl.a. följande[168]:

> Att spara fingeravtryck i id-kortsregistret och möjliggöra sökning på dessa eller att möjliggöra sökning på de ansiktsbilder som finns i registret skulle i princip omöjliggöra att samma person kan skaffa sig flera identitetshandlingar i olika identiteter. Ett register med möjlighet att söka bland ansiktsbilder och/eller fingeravtryck avseende en stor del av befolkningen i Sverige medför dock stora risker för den personliga integriteten. När det gäller ansiktsbilderna kan emellertid konstateras att de redan lagras i syfte att användas bl.a. i den identitetskontroll som görs vid ansökan. Att tillåta viss sökning på dessa medför inte att något ytterligare biometriskt underlag sparas utan enbart att ansiktsbilderna får behandlas på ett nytt sätt. För att en sådan sökning ska vara möjlig behöver även vissa biometriska uppgifter kopplade till ansiktsbilderna sparas i id-kortsregistret. Bedrägeri-

[168] A.a. s. 297.

> brottsligheten som begås med hjälp av falska och felaktiga identitetshandlingar får stora konsekvenser för både den enskilde, privata aktörer och samhället. Brottsligheten har som framgått ökat under de senaste åren. För att kunna stävja den brottslighet som beror på att identitetshandlingar utfärdas för en och samma person i flera identiteter finns ingen annan effektiv metod än sökning på ansiktsbilderna. Vi anser mot denna bakgrund att det finns tungt vägande skäl som talar för att möjliggöra sådana sökningar. För att uppnå syftet att inte samma person ansöker om identitetshandlingar i flera olika identiteter bör sökning på ansiktsbilder i id-kortsregistret även få göras vid en ansökan om pass. Sökmöjligheten måste dock förenas med effektiva säkerhetsåtgärder för att undvika att sökningar görs i andra syften än de avsedda. Det bör därför bara vara tillåtet att använda ansiktsbilden och de biometriska uppgifter som kan tas fram ur den för att göra en sökning vid ansökan i syfte att kontrollera om sökandens ansikte finns i registret, dvs. för att kontrollera om ansiktsbilden har förekommit i en annan ansökan. Sökning bör endast tillåtas om det är nödvändigt för detta syfte.

I promemorian om en ny passdatalag redovisades de problem som ett förbud mot att göra biometriska jämförelser leder till enligt följande:

> Svenska pass håller en hög säkerhetsnivå. De är svåra att förfalska. Det är också svårt att använda en annan persons pass, eftersom den ansiktsbild och de fingeravtryck som tas vid en passkontroll kan jämföras biometriskt med den ansiktsbild och de fingeravtryck som finns sparade i passet. Det går därigenom att upptäcka om en person försöker använda någon annans pass, även om personerna är lika. Ett problem som däremot är svårt att motverka effektivt med dagens regelverk är den typ av identitetsstöld som går ut på att en person utger sig för att vara någon annan redan när han eller hon ansöker om pass. Det händer således att en person lyckas få pass under felaktig identitet eller att en och samma person lyckas få flera pass under olika identiteter. Sådana pass kan användas för brottslig verksamhet. Identitetsstölden går inte heller att upptäcka vid en passkontroll, eftersom den ansiktsbild och de fingeravtryck som finnas sparade i passet faktiskt tillhör den som använder passet. Sökandens identitet ska naturligtvis kontrolleras när han eller hon ansöker om pass. Identiteten kan dock styrkas på olika sätt och ytterst kan det räcka att t.ex. en anhörig intygar att sökanden är den som han eller hon utger sig för att vara. Det finns alltid en risk för att sökanden identifierar sig med en förfalskad identitetshandling eller ett felaktigt intyg. I dessa fall hjälper det inte att passet i sig håller en hög säkerhetsnivå, eftersom det kommer att utfärdas för en person som inte är den som han eller hon utger sig för att vara.

I promemorian redogjordes också för att Polismyndigheten och dåvarande Rikspolisstyrelsen, Statens kriminaltekniska laboratorium (numera Nationellt forensiskt centrum) och Migrationsverket framfört behov av att kunna göra biometriska jämförelser. Vidare framfördes

att felaktigt utfärdade identitetshandlingar har stor betydelse vid bedrägeribrottslighet samt att felaktigt utfärdade pass också kan användas vid allvarligare brottslighet som exempelvis människosmuggling, människohandel och terroristbrott. Slutligen gjordes bedömningen att biometriska jämförelser av ansiktsbilder, i syfte att kontrollera sökandens identitet och innehav av pass vid en ansökan om pass, är tillåtna enligt dataskyddsförordningen. Ett förslag om att biometriska jämförelser av ansiktsbilder skulle tillåtas lämnades således.[169] Förslaget bereds för närvarande i Regeringskansliet.

I förarbetena till lagen om samordningsnummer konstaterade regeringen att en möjlighet att spara biometriska uppgifter, som vissa remissinstanser påpekat, skulle kunna bidra till att motverka att en person får en identitetsbeteckning under flera eller falska identiteter. Regeringen menade att det är angeläget att förhindra förekomsten av multipla identiteter, men ansåg att det saknades underlag för att i det lagstiftningsärendet överväga en ordning där uppgifterna sparas för framtida jämförelser. Även om det angavs att det kan finnas skäl att återkomma till frågan föreslogs därmed inte några sådana bestämmelser.[170]

Biometriutredningen föreslog i sitt betänkande att det – vid viss allvarlig brottslighet – skulle vara tillåtet att genomföra biometriska jämförelser mot ansiktsbilder i passregistret samt mot fingeravtryck och ansiktsbilder i Migrationsverkets register över fingeravtryck och fotografier. Följande överväganden gjordes i fråga om behovet i förhållande till det integritetsintrång som behandlingen skulle innebära:

> Brottsutvecklingen är sådan att polisen med nödvändighet behöver fler verktyg för att klara upp allvarliga brott och för att stoppa den våldsspiral som finns i samhället. Det är vår uppfattning att effektiva verktyg som bidrar till att polisen i högre utsträckning kan säkra bevis och att gärningsmän lagförs typiskt sett har betydligt större påverkan på brottsutvecklingen än t.ex. strängare straffskalor. Det ligger då närmast i sakens natur att biometriska jämförelser med ansiktsbilder och fingeravtryck i andra myndighetsregister kan utgöra sådana verktyg. Det gäller t.ex. passregistret, som innehåller så många ansiktsbilder att det är svårt att dra någon annan slutsats än att biometriska jämförelser i det registret skulle öka polisens och andra brottsbekämpande myndigheters förutsättningar att hitta den som har begått ett brott och på så sätt möjliggöra att fler brott kan klaras upp […]. Vi delar därför den uppfattning som kommer till uttryck i våra direktiv om att det skulle vara mycket värdefullt för polisen att ha

[169] *Passdatalag – en ny lag som kompletterar EU:s dataskyddsförordning* (Ds 2019:5) s. 145 ff. och där gjorda hänvisningar.
[170] Prop. 2021/22:276 s. 72.

> tillgång till fler register. Samtidigt är det av fundamental betydelse i en rättsstat att ett myndighetsregister som innehåller ansiktsbilder eller fingeravtryck och som förs för andra än brottsbekämpande ändamål inte utan vidare kan användas för att genom biometriska jämförelser klara upp brott. Detta eftersom en sådan behandling innebär en stark integritetskränkning genom att ansiktsbilder eller fingeravtryck av personer som inte är misstänkta eller dömda för brott genom automatiserad teknik jämförs med ansiktsbilder eller fingeravtryck av oidentifierade misstänkta gärningsmän.
>
> Mot denna bakgrund anser vi att det endast är vid allvarlig brottslighet som det kan vara motiverat att ge polisen rätt att göra biometriska jämförelser med uppgifter som finns i myndighetsregister som samlar personuppgifter i helt andra syften. En annan ordning skulle enligt vår bedömning resultera i en oproportionerlig behandling av känsliga personuppgifter som till merparten är hänförlig till personer som varken är misstänkta eller lagförda för brott.

Utredningen föreslog vidare, som en konsekvens av förslaget om att tillåta jämförelser mot Passregistret, att passlagens nuvarande krav på att förstöra biometriska uppgifter som tagits fram ur en ansiktsbild efter det att passet har lämnats ut eller passansökan har återkallats eller avslagits, skulle tas bort. Några bestämmelser som skulle möjliggöra biometriska jämförelser i registret över nationella identitetskort föreslogs inte.[171] Utredningens förslag bereds i Regeringskansliet.

Det ska vara möjligt med biometriska jämförelser av ansiktsbilder i databasen över statliga e-legitimationer

Vi kan konstatera att den identitetsrelaterade brottsligheten som ovan nämnda utredningar hänvisat till fortsatt är ett omfattande samhällsproblem med tydliga kopplingar till den organiserade brottsligheten (se mer om detta i avsnitt 6.7). Brottsligheten medför inte bara ekonomiska konsekvenser för enskilda personer och företag utan också omfattande sådana för de brottsbekämpande myndigheterna och därigenom staten.

Ekonomiska transaktioner och avtalsslut sker direkt i den digitala världen. Felaktigt utfärdade statliga e-legitimationer som kan användas för att id-växla till andra e-legitimationer kan därför snabbt få allvarliga konsekvenser för den identitetsrelaterade brottsligheten. Användningsområdena för elektroniska underskrifter kan dessutom förväntas öka i framtiden. Exempelvis har Utredningen om en ny förköpslag

[171] *Biometri – för en effektivare brottsbekämpning*, (SOU 2023:32) s. 423 ff.

fått i uppdrag att lämna förslag på de författningsändringar som krävs för att möjliggöra överlåtelser av fast egendom med användning av elektroniska överlåtelsehandlingar, och elektronisk ansökan i alla inskrivningsärenden. Uppdraget ska redovisas senast den 1 april 2024.[172] Med hänsyn till de betydande värden som kan komma i fråga vid fastighetsöverlåtelser torde en säker metod för att säkerställa de inblandades identiteter vara av vikt vid en sådan framtida möjlighet. Vi menar att en möjlighet att använda biometriska uppgifter således kan få betydelse i exempelvis ett sådant sammanhang.

Vidare innebär våra förslag att personer med styrkt samordningsnummer ska kunna få en statlig e-legitimation (se avsnitt 7.4.2). Samordningsnummer har historiskt sett använts vid välfärdsbrottslighet och för att skapa falska identiteter eller vid användning av s.k. fordonsmålvakter.[173] Även om bestämmelserna som trädde i kraft den 1 september 2023 är tänkta att stärka systemet med samordningsnummer kommer utfärdade samordningsnummer inte vara kopplade till någon identitetshandling. Således finns det fortsatt vissa risker förenade med möjligheten att medge ansökan om e-legitimation för en person med styrkt samordningsnummer. Jämförande sökningar på biometriska ansiktsbilder i en databas över statliga e-legitimationer skulle på ett väsentligt sätt bidra till att undanröja risken för att en och samma person får flera statliga e-legitimationer.

Vi menar sammanfattningsvis att en möjlighet att använda biometriska uppgifter ur ansiktsbilder, som får lagras i databasen, för jämförande sökningar i samband med ansökan om en statlig e-legitimation vore ett effektivt sätt att förhindra att flera e-legitimationer utfärdas till en och samma person. Att motverka missbruk av den statliga e-legitimationen utgör ett sådant viktigt allmänt intresse som avses i artikel 9.2 g. För att uppfylla det intresset är det enligt vår bedömning nödvändigt att kunna söka i databasen för att ta reda på om samma person redan har fått en e-legitimation utfärdad eller inte. Det finns inget mindre integritetskränkande sätt att uppnå det syftet. En sökmöjlighet som begränsar sig till ansökningstillfället framstår inte heller som särskilt integritetskränkande i förhållande till vikten av att säkerställa individens rätt till att dennes identitet inte missbrukas. Således framstår åtgärden proportionerlig.

[172] Tilläggsdirektiv till Utredningen om en ny förköpslag (Fi 2022:07).
[173] Se till exempel prop. 2021/22:276 s. 29 ff. och där gjorda hänvisningar.

Fingeravtrycken och dess biometriska uppgifter ska omedelbart förstöras

I 6 a § passlagen anges beträffande fingeravtryck att dessa och biometriska data som kan tas fram ur dessa omedelbart ska förstöras när passet har lämnats ut eller passansökan har återkallats eller avslagits. Enligt 4 § förordningen om nationellt identitetskort ska fingeravtryck som inte sparats i ett lagringsmedium i identitetskortet och de biometriska data som tas fram ur fingeravtrycken omedelbart förstöras när identitetskortet har lämnats ut eller, om kortet inte har lämnats ut, när det har gått 90 dagar från den dag då det utfärdades. Om ansökan har återkallats eller avslagits ska uppgifterna omedelbart förstöras.

Enligt vår bedömning framstår det, såvitt avser fingeravtryck och dess biometriska uppgifter, inte som motiverat med en annan ordning för den statliga e-legitimationen än vad som gäller för pass och nationella id-kort. Fingeravtrycken och dess biometriska uppgifter som inhämtas av den identitetskontrollerande myndigheten får alltså inte lagras eller sparas efter att grundidentifieringen har genomförts. Detta ska gälla för alla uppgifter som inhämtats oavsett om de lämnats av sökanden eller inhämtats via kontroll mot befintliga register. Inhämtade fingeravtryck samt de biometriska uppgifter som hämtas ur dessa ska således omedelbart förstöras efter att kontrollen är genomförd. Kravet bör, på samma sätt som gäller för pass, vara absolut. Det ska alltså inte vara möjligt att meddela föreskrifter om att uppgifterna får bevaras för några andra ändamål.

Den ansiktsbild som tas av den identitetskontrollerande myndigheten i samband med grundidentifieringen och utlämnandet av den statliga e-legitimationen ska föras in i den utfärdande myndighetens system för att, tillsammans med biometriska uppgifter som hämtats ur den, lagras i databasen över statliga e-legitimationer. Uppgifterna ska dock inte få lagras hos den identitetskontrollerande myndigheten.

7.11.8 Det finns behov av vissa ytterligare integritetshöjande åtgärder

Utredningens förslag: Uppgifter och handlingar i databasen över statliga e-legitimationer ska endast få behandlas under den tid som är nödvändig för ändamålet med behandlingen, dock längst tio år räknat från utgången av det år då den statliga e-legitimationen utfärdades, en ansökan avslogs eller återkallades eller ärendet avslutades på annat sätt.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om att uppgifter och handlingar i databasen får bevaras längre tid än tio år för arkivändamål av allmänt intresse eller vetenskapliga, statistiska eller historiska ändamål samt om att uppgifterna i sådant fall ska avskiljas från den löpande verksamheten.

Det ska inte vara tillåtet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter eller uppgifter om lagöverträdelser som avses i artikel 10 i dataskyddsförordningen.

Utredningens bedömning: Det finns inte behov av att införa bestämmelser om hur personuppgifter som rör lagöverträdelser får behandlas annat än såvitt avser sökbegränsningar.

Lagen behöver inte innehålla bestämmelser om personnummer eller samordningsnummer.

Skälen för utredningens förslag och bedömning

Bestämmelser om längsta tid för bevarande av personuppgifter

Vid lagring av personuppgifter som sker helt eller delvis automatiserat eller när personuppgifter ingår i eller kommer att ingå i en databas omfattas behandlingen av dataskyddsförordningens krav på lagringsminimering. Enligt artikel 5.1 e får personuppgifter inte lagras på ett sätt som möjliggör identifiering under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Behandling för arkivändamål av allmänt intresse är enligt artikel 5.1 b generellt sett laglig, eftersom behandlingen anses vara förenlig med det ändamål för vilket uppgifterna ursprungligen samlades in.

Enligt artikel 6.2 och 6.3 i dataskyddsförordningen får medlemsstaterna införa bestämmelser om lagringstider, när behandlingen grundar sig på artikel 6.1 e, vilket är fallet för den statliga e-legitimationen (jfr avsnitt 7.11.6)

Den svenska arkivlagstiftningens utgångspunkt är att allmänna handlingar ska bevaras oavsett om de innehåller personuppgifter eller inte. Bestämmelser om bevarande av allmänna handlingar genom arkivering finns i arkivlagen (1990:782), arkivförordningen (1991:446) och Riksarkivets föreskrifter (RA-FS och RA-MS).

Den personuppgiftsbehandling som en myndighet utför för att arkivera allmänna handlingar enligt arkivlagstiftningen ska enligt regeringen anses ske för arkivändamål av allmänt intresse i den mening som begreppet har i dataskyddsförordningen. Det skydd som enligt svensk rätt gäller för myndigheters arkiv uppfyller enligt regeringen dataskyddsförordningens krav på skyddsåtgärder och personuppgifter får därmed bevaras under en längre tid än vad som framgår av principen om lagringsminimering, om den svenska arkivlagstiftningen kräver att uppgifterna ska bevaras.[174]

2017-års ID-kortsutredning föreslog att bestämmelser om hur lång tid uppgifter skulle få bevaras skulle införas i lag. Enligt utredningens förslag skulle uppgifter och handlingar få bevaras i längst tio år efter utgången av det kalenderår då giltighetstiden för handlingen gått ut. Utöver att särskilda bestämmelser behövde införas om inte arkivlagens huvudregel om bevarande skulle gälla anförde utredningen bl.a. följande:[175]

> Förutom de behov som redovisats ovan är det av stor vikt för säkerheten i utfärdandeprocessen att den utfärdande myndigheten kan kontrollera uppgifter i registret i samband med att en person ansöker om ett nytt id-kort. Uppgifterna behövs således bl.a. för att kunna kontrollera att inte samma person innehar flera kort med olika identiteter och att den sökande inte ansöker om att få ett kort med en annan persons identitet. Detta gäller inte minst de ansiktsbilder och biometriska data som vi […] föreslår ska sparas i id-kortsregistret i syfte att möjliggöra sökning på dessa uppgifter. Många uppgifter kan av det skälet behöva sparas under lång tid. Vi menar att det är en lämpligare ordning att utforma lagregleringen så att den bättre återspeglar den behandling som faktiskt sker än att enbart låta detta framgå av myndighetsföreskrifter.

[174] Prop. 2017/18:105 s. 110 ff.
[175] *Ett säkert statligt ID-kort-med e-legitimation*, (SOU 2019:14), s. 273 ff.

I promemorian om en ny passdatalag föreslogs att en särskild gallringsfrist skulle införas för handlingar och uppgifter i passregistret i syfte att skydda den enskildes personliga integritet, underlätta de personuppgiftsansvarigas arbete och skapa goda förutsättningar för tillsyn. Fristen föreslogs vara tio år bl.a. mot bakgrund av att allmänna handlingar hos myndigheter inom utrikesrepresentationen får gallras efter tio år och att det är den tid som uppgifter i Migrationsverkets register över fingeravtryck och fotografier som längst får bevaras. Vidare anfördes att en tioårig frist för passregistrets del skulle innebära att registret kunde visa handlingar och uppgifter från de två senaste passärendena, förutsatt att passinnehavaren ansökte om nytt pass i anslutning till att det gamla löpte ut. I sådant fall skulle en jämförelse av ansiktsbilder från de senaste tio åren vara möjlig. Fristen skulle enligt promemorian lämpligen räknas från utgången av det år då ett pass utfärdades, en passansökan avslogs eller återkallades eller ärendet avslutades på annat sätt. Skälet till det angavs vara att passregistret enligt förslaget skulle få innehålla uppgifter både om personer som har beviljats pass och personer som har varit parter i passärenden utan att få pass samt att fristen därmed inte kunde knytas till utfärdandet av ett pass eller till passets giltighetstid.[176]

Vi anser att ovan redovisade skäl för att införa en lagringstid på tio år gör sig gällande även för databasen över statliga e-legitimationer. En bestämmelse om vilken tid uppgifter i databasen över statliga e-legitimationer som längst ska få bevaras bör därför införas i förordningen om elektronisk identifiering.

Våra förslag innebär, liksom promemorians om en ny passdatalag, att registret över statliga e-legitimationer ska få innehålla uppgifter om personer som är eller har varit parter i ärenden om ansökan om statlig e-legitimation. Bestämmelsen ska därmed lämpligen utformas på så sätt att uppgifter och handlingar ska gallras senast tio år efter utgången av det kalenderår då det ärende som uppgifterna eller handlingarna hänför sig till avslutades. Ett ärende kan avslutas i samband med att en statlig e-legitimation utfärdas, en ansökan avslås eller återkallas eller på annat sätt, exempelvis genom avvisning.

Det kan finnas skäl för att behandla vissa handlingar eller uppgifter i registret över statliga e-legitimationer längre än tio år om det sker för arkivändamål av allmänt intresse eller vetenskapliga, statistiska eller

[176] Se Passdatalag – en ny lag som kompletterar EU:s dataskyddsförordning (Ds 2019:5), s. 177 f. och där gjorda hänvisningar.

historiska ändamål. Om så sker bör emellertid uppgifterna, för att gallringsfristen ska få avsedd verkan, avskiljas från den löpande verksamheten. Riksarkivet bör, enligt en bestämmelse som tas in i förordningen om elektronisk identifiering, ges rätt att meddela föreskrifter i angivna avseenden.

Sökbegränsningar

Våra förslag innebär att fingeravtryck och ansiktsbild ska lagras i bäraren av den statliga e-legitimationen och att ansiktsbilden och dess biometriska uppgifter ska få lagras i databasen. Av integritetsskyddsskäl finns det, på samma sätt som för pass och nationella id-kort, skäl att införa sökbegränsningar för dessa uppgifter som ska gälla för all annan sökning än i samband med ansökan (se mer om detta i avsnitt 7.11.7).

Digg konstaterade i sin rapport att personuppgifter som rör lagöverträdelser sannolikt inte kommer att behandlas i någon särskilt stor omfattning i verksamheten med att tillhandahålla en statlig e-legitimation.[177] Vi ansluter oss till den bedömningen men anser liksom Digg att det, i syfte att undvika sådana integritetsrisker som behandlingen medför kan vara lämpligt att införa en sökbegränsning för uppgifter som rör lagöverträdelser.

Uppgifter om lagöverträdelser och person- eller samordningsnummer

Uppgifter om lagöverträdelser och person- eller samordningsnummer är inte känsliga personuppgifter men anses ändå vara en typ av uppgifter som förtjänar ett särskilt skydd.

Vid återkallelse eller spärr av den statliga e-legitimationen kan den tillhandahållande myndigheten komma att behandla personuppgifter som rör fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder. Stöd för sådan behandling inom ramen för en myndighets verksamhet finns i artikel 10 i dataskyddsförordningen och 3 kap. 8 § första stycket dataskyddslagen. Det finns därmed, utöver föreslagen sökbegränsning, inte skäl att införa särskilda bestämmelser om personuppgifter som rör lagöverträdelser.

[177] Myndigheten för digital förvaltning, *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, s. 76 f.

Av 3 kap. 10 § dataskyddslagen framgår att person- och samordningsnummer får behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. I verksamheten med att tillhandahålla en statlig e-legitimation är vikten av en säker identifiering uppenbar. Det finns således stöd för att behandla person- och samordningsnummer utan samtycke och någon särskild bestämmelse behöver inte införas.

7.11.9 Bestämmelser om direktåtkomst

Utredningens bedömning: Det finns för närvarande inte skäl att införa bestämmelser om att personuppgifter i databasen över statliga e-legitimationer ska få lämnas ut genom direktåtkomst.

Frågan om vilka brottsbekämpande myndigheter som bör ges direktåtkomst till databasen bör utredas vidare.

Skälen för utredningens bedömning

Med direktåtkomst avses vanligen att en myndighet har direkt tillgång till en annan myndighets register eller databas och på egen hand kan söka efter information, men inte påverka innehållet i registret eller databasen. Direktåtkomst har ansetts föreligga om en myndighet hos en annan har sådan teknisk tillgång till upptagningar som avses i nuvarande 2 kap. 6 § tryckfrihetsförordningen, dvs. om upptagningen är tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas eller avlyssnas eller uppfattas på annat sätt.[178]

En möjlighet till direktåtkomst myndigheter emellan kan, precis som konstaterades i promemorian till ny passdatalag, medföra effektivitetsvinster, dels för den myndighet som behöver uppgifter från en annan myndighet i sin verksamhet, dels för den utlämnande myndigheten.[179] Direktåtkomst kan emellertid också vara förknippat med risker för den personliga integriteten och bör således bara tillåtas om det finns ett faktiskt behov.

[178] *Myndighetsdatalag* (SOU 2015:39), s. 390 och HFD 2015 ref 61.
[179] *Passdatalag – en ny lag som kompletterar EU:s dataskyddsförordning* (Ds 2019:14), s. 162.

I såväl 2017 års ID-kortsutredning som promemorian om en ny passdatalag lämnades förslag om att en uppgift om ett id-korts respektive pass giltighet skulle få lämnas ut genom direktåtkomst.[180] En fråga om den statliga e-legitimationen är giltig eller inte kommer emellertid att besvaras automatiserat i och med att den används. Vi bedömer således att det saknas behov av en bestämmelse som ger direktåtkomst till uppgift om e-legitimationens giltighet.

Den statliga e-legitimationen kommer enligt våra förslag inte att utfärdas av någon annan myndighet än Digg. Som framgått begränsar sig den identitetskontrollerande myndighetens uppgift till att avgöra om identiteten är styrkt eller inte. Något behov för den senare myndigheten att kontrollera om den som ansöker redan har en giltig e-legitimation finns således inte. Det är i stället Digg, i egenskap av utfärdande myndighet, som genomför den kontrollen. Mot angiven bakgrund finns det inte skäl för att, på motsvarande sätt som för passverksamheten, införa bestämmelser om direktåtkomst mellan utfärdande myndigheter.

Enligt våra direktiv ska de förslag vi lämnar bl.a. syfta till att motverka bedrägerier som begås med hjälp av e-legitimationer. Som framgått menar vi att möjligheten att uppfylla detta syfte främst aktualiseras i samband med utfärdandet. Vi lämnar därför förslag som går ut på att det ska vara möjligt att säkerställa att en viss e-legitimation är kopplad till en viss fysisk person och att endast en statlig e-legitimation per individ utfärdas (se avsnitt 7.11.7). Vi bedömer inte att dessa förslag aktualiserar behov av bestämmelser om direktåtkomst. Vi ser dock att det finns ett behov för den utfärdande myndigheten att ges möjlighet att behandla uppgifter i databasen för statliga e-legitimationer, om det är nödvändigt för att tillhandahålla information som behövs i Polismyndighetens verksamhet med att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller upprätthålla allmän ordning och säkerhet. Av det skälet har vi föreslagit en bestämmelse med ett sekundärt ändamål med sådant innehåll (se avsnitt 7.11.4).

Vi ser att det kan finnas stora fördelar för såväl Polismyndigheten som andra brottsbekämpande och brottsutredande myndigheter med att få direktåtkomst till uppgifter i databasen över en statlig e-legitimation. Såväl i Promemorian med förslag till passdatalag som i Bio-

[180] *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14), s.251 och 258 samt *Passdatalag – en ny lag som kompletterar EU:s dataskyddsförordning* (Ds 2019:15), s. 163f.

metriutredningen lämnas också förslag om utökade möjligheter i angivet avseende. Ytterligare ställningstaganden kopplat till åtgärder som primärt rör rättsvårdande myndigheters möjligheter att – genom direktåtkomst till databasen över statliga e-legitimationer – bedriva sin verksamhet kan emellertid inte anses omfattas, eller tidsmässigt, rymmas i vårt uppdrag. Frågan bör dock utredas vidare.

7.11.10 Säkerhetshöjande åtgärder

Utredningens förslag: Endast den som behöver tillgång till personuppgifter för att kunna fullgöra sina arbetsuppgifter ska ha rätt att behandla personuppgifter inom ramen för verksamheten med en statlig e-legitimation. De personuppgiftsansvariga myndigheterna ska få meddela närmare föreskrifter om tillgången till personuppgifter.

Regeringen eller den myndighet som regeringen bestämmer ska kunna meddela ytterligare föreskrifter om säkerhetsåtgärder till skydd för personuppgifter.

Skälen för utredningens förslag

Våra förslag innebär att en stor mängd dels i rättslig mening känsliga, dels i övrigt integritetskänsliga uppgifter kommer att hanteras, inte minst eftersom biometriska uppgifter föreslås lagras i såväl bäraren som databasen över statliga e-legitimationer. Uppgifterna behöver skyddas mot obehörig eller otillåten åtkomst, kopiering och manipulering.

De krav som ställs på säkerheten när personuppgifter behandlas framgår av artikel 32 i dataskyddsförordningen. Enligt bestämmelsen ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå i förhållande till riskerna med behandlingen. Skyldigheten att vidta lämpliga tekniska och organisatoriska åtgärder genom att exempelvis begränsa tillgången till personuppgifter framgår även av artikel 24.1 och 25.2 samt av de allmänna principerna för personuppgiftsbehandling i artikel 5.1 f i dataskyddsförordningen. Att tillgången till personuppgifter ska begränsas på olika sätt följer således av dataskyddsförordningen. Det är emellertid möjligt att med stöd av

artikel 6.2 dataskyddsförordningen särskilt förordna om begränsningar i angivet avseende.[181]

Verksamheten med att tillhandahålla en statlig e-legitimation föreslås involvera två olika myndigheter. En sådan ordning kommer att ställa särskilt höga krav på de organisatoriska åtgärder som behöver vidtas, inte minst när det gäller åtkomsten till personuppgifter.[182] Enligt vår bedömning finns det mot den bakgrunden skäl att införa en bestämmelse som anger att tillgången till personuppgifter i verksamheten med en statlig e-legitimation ska begränsas till det som en viss medarbetare behöver för att fullgöra sina arbetsuppgifter.

Respektive myndighet får anses vara mest lämpad att ta ställning till på vilket sätt åtkomsten till personuppgifter ska begränsas och meddela nödvändiga föreskrifter. Ett bemyndigande bör därför tas in i föreslagen förordning om elektronisk identifiering.

Den tekniska och säkerhetsrelaterade utvecklingen sker i snabb takt och ytterligare krav på säkerhetsåtgärder kan komma att behövas. Det bör därför vara möjligt för regeringen eller den myndighet som regeringen bestämmer att meddela ytterligare säkerhetsföreskrifter till skydd för personuppgifter.

7.11.11 Behov av undantag enligt artikel 23 i dataskyddsförordningen

Utredningens förslag: Den rätt att invända mot personuppgiftsbehandling som framgår av artikel 21.1 i dataskyddsförordningen ska inte gälla vid behandling som är tillåten enligt den nya lagen om elektronisk identifiering eller föreskrifter som har meddelats i anslutning till lagen.

Skälen för utredningens förslag

Vid behandling av personuppgifter har den registrerade ett flertal rättigheter. Dessa regleras i kapitel III i dataskyddsförordningen. Bestämmelserna om den registrerades rättigheter, med motsvarande skyldighe-

[181] Prop. 2017/18:254 s. 36 och *Passdatalag – en ny lag som kompletterar EU:s dataskyddsförordning* (Ds 2019:5), s. 127.
[182] Se mer om utgivningsprocessen i avsnitt 7.4.2 och de problem vi identifierat med ett uppdelat ansvar i avsnitt 7.6.4.

ter för den personuppgiftsansvarige, är direkt tillämpliga. Rättigheterna är inte absoluta utan kan, enligt artikel 23 i dataskyddsförordningen, under vissa förutsättningar begränsas. Vissa generella begränsningar har införts genom dataskyddslagen och frågan är om det finns skäl till ytterligare begränsningar för verksamheten med att tillhandahålla en statlig e-legitimation.

Vid behandling av personuppgifter som sker för att utföra en uppgift av allmänt intresse, som ett led i myndighetsutövning eller efter en intresseavvägning (dvs. behandling enligt artikel 6.1 e eller f i dataskyddsförordningen) ska den registrerade enligt artikel 21.1 ha rätt att när som helst, av skäl som hänför sig till hans eller hennes specifika situation, göra invändningar mot behandlingen. Den personuppgiftsansvarige får då inte längre behandla personuppgifterna, såvida denne inte kan påvisa tvingande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter eller om det sker för fastställande, utövande eller försvar av rättsliga anspråk.

Personuppgifterna i det föreslagna registret över statliga e-legitimationer behandlas, som ovan redovisats, med stöd av artikel 6.1 e, varför rätten att göra invändningar gäller. Begränsningar av rätten att göra invändningar får enligt artikel 23.1 göras i syfte att säkerställa bl.a. ett viktigt mål av generellt allmänt intresse för medlemsstaten. Det krävs också att begränsningen uppfyller krav på nödvändighet och proportionalitet. Vidare måste lagstiftningen enligt artikel 23.2 innehålla specifika bestämmelser om bl.a. ändamål, kategorier av uppgifter, omfattningen av begränsningen, skyddsåtgärder, personuppgiftsansvar, lagringstid, riskerna för de registrerades rättigheter och friheter samt rätten att bli informerad om begränsningen, när så är relevant.

Såväl 2017 års ID-kortsutredning som Digg har, med hänvisning till det lagstiftningsärende[183] i vilket bl.a. lagstiftningen beträffande identitetskort för folkbokförda i Sverige sågs över med anledning av dataskyddsförordningen, ansett det befogat med en begränsning i rätten att göra invändningar.

I angivet lagstiftningsärende framhöll regeringen betydelsen av att personuppgifter får behandlas oberoende av den registrerades inställning i de aktuella verksamheterna och att behandlingen är en förutsättning för att myndigheterna ska kunna utföra sina uppgifter på ett korrekt, rättssäkert och effektivt sätt.[184] Den personuppgiftsansvariga

[183] Prop. 2017/18:95.
[184] A.a. s. 85 f.

myndigheten ansågs närmast undantagslöst kunna påvisa skäl för fortsatt behandling som väger tyngre än den registrerades intressen i det enskilda fallet. Regeringen menade att den registrerade inte borde ha rätt att motsätta sig sådan personuppgiftsbehandling som var tillåten enligt den lagen. Begränsningen ansågs utgöra en proportionerlig åtgärd i syfte att säkerställa ett viktigt mål av generellt allmänt intresse.

Det finns enligt vår uppfattning inte skäl att göra någon annan bedömning för den statliga e-legitimationen. Våra förslag uppfyller också de krav på skyddsåtgärder som uppställs i artikel 23.2. En bestämmelse om att rätten att göra invändningar inte gäller ska därför föras in i den nya lagen om elektronisk identifiering. Vi ser emellertid inte skäl att införa några ytterligare begränsningar av den registrerades rättigheter i den föreslagna lagen.

7.12 Sekretess

Utredningens förslag: I 6 § offentlighets- och sekretessförordningen (2009:641) ska, bland verksamheter som omfattas av sekretess, tilläggas den databas med uppgifter om statliga e-legitimationer som den utfärdande myndigheten ska föra.

Utredningens bedömning: Några sekretessbrytande bestämmelser behövs inte.

Skälen för utredningens bedömning och förslag

Vårt förslag om tillhandahållande av en statlig e-legitimation förutsätter personuppgiftsbehandling i flera avseenden och att en databas används i den utfärdande myndighetens verksamhet med e-legitimationer för bl.a. ärendehantering och kontroller.

Även den identitetskontrollerande myndigheten kommer att behandla personuppgifter vid upprättande av ansökan och registrering av uppgifter, samt för grundidentifieringen (se avsnitten 7.11.4 och 7.11.5).

Den registerföring och uppgiftskontroll som kommer att aktualiseras föranleder överväganden om behov av uppgiftssekretess och sekretessbrytande regler.

Databasen kommer innehålla uppgifter som inte är av känslig art, såsom namn, personnummer alternativt samordningsnummer, och giltighetstid.[185] Som framgår av avsnitten 7.11.7 och 7.11.8 kan dock även uppgifter om lagöverträdelser komma att behöva behandlas. Det kan exempelvis handla om misstankar om olovlig identitetsanvändning och olovlig befattning med betalningsverktyg. Dessutom kommer enligt vårt förslag ansiktsbilder och biometriska uppgifter som kan tas fram ur dessa att lagras i databasen. Det finns därmed behov av att kunna sekretesskydda sådana uppgifter.

De föreslagna ändamålsbestämmelserna för personuppgiftsbehandling omfattar både primära och sekundära ändamål. Bland de sistnämnda finns bl.a. ändamålet att fullgöra uppgiftsutlämnande som sker i överensstämmelse med lag eller förordning (se avsnitt 7.11.4). Att uppgiftslämnandet ska ske i överensstämmelse med lag eller förordning innebär att det ska ske med stöd av bestämmelser som antingen påbjuder eller tillåter utlämnande. Ett sådant exempel är 6 kap. 5 § offentlighets- och sekretesslagen (2009:400, OSL) som fastslår en allmän skyldighet för en myndighet att på begäran av en annan myndighet lämna ut uppgifter, om det inte skulle hindra arbetets behöriga gång.

Av 22 kap. 1 § första stycket OSL följer att sekretess gäller för uppgift i verksamhet som avser folkbokföringen eller annan liknande registrering av befolkningen. Sekretessen enligt denna bestämmelse gäller för enskilds personliga förhållanden, om det av särskild anledning kan antas att den enskilde eller någon närstående till denne lider men om uppgiften röjs. Huvudregeln i bestämmelsen är alltså att uppgifterna i de register som avses ska vara offentliga. Om det av särskild anledning kan antas att ett utlämnande skulle leda till skada eller men kan dock uppgifter hemlighållas. Det skulle kunna vara fallet i fråga om uppgifter om lagöverträdelser som kan förekomma i samband med att en e-legitimation har spärrats.

Sekretess gäller vidare enligt 22 kap. 1 § andra stycket OSL för uppgift i form av fotografisk bild av den enskilde, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men. Denna bestämmelse innehåller ett omvänt skaderekvisit, dvs. uppgiften omfattas av sekretess om det inte står klart att den kan röjas utan att den enskilde eller någon närstående till den enskilde lider men.

[185] Denna typ av uppgifter, som också finns i bl.a. passärenden, har regeringen ansett vara att betrakta som harmlösa i de flesta fall, prop. 2004/05:119 s. 44.

För sådan ”annan verksamhet som avser registrering av en betydande del av befolkningen” som avses i 22 kap. 1 § första stycket OSL får regeringen meddela föreskrifter om sekretess. Exempel på sådana verksamheter är Polismyndighetens passregister och register över nationella identitetskort samt Skatteverkets databas över identitetskort för folkbokförda i Sverige. Detta framgår av 6 § offentlighets- och sekretessförordningen (2009:641).

Den verksamhet med statliga e-legitimationer som nu föreslås är på motsvarande sätt skyddsvärd och bör omfattas av sekretess. Vi föreslår därför att 6 § offentlighets- och sekretessförordningen ändras med ett tillägg för den verksamhet som avser den utfärdande myndighetens databas för e-legitimationer.

Den identitetskontrollerande myndigheten kommer att granska såväl svenska som utländska identitetshandlingar. Såvitt gäller de svenska tillhandahåller både Skatteverket och Polismyndigheten tjänster för giltighetskontroll för de identitetshandlingar som myndigheterna tillhandahåller.[186]

Myndigheter har också enligt 2 kap. 8 § första stycket lagen om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet direktåtkomst till uppgift om bl.a. person- eller samordningsnummer, namn, adress, och avregistrering från folkbokföringen. Detta sker genom Navet, vilket är Skatteverkets tidigare nämnda system för distribution av folkbokföringsuppgifter. Det bedöms därmed inte finnas något sekretesshinder mot att utföra de nödvändiga identitetskontrollerna och, av den anledningen, saknas behov av att införa sekretessbrytande bestämmelser i detta avseende.

Enligt den föreslagna utgivningsprocessen för den statliga e-legitimationen ska ansökan upprättas och nödvändiga uppgifter från sökanden införas av den identitetskontrollerande myndigheten direkt i den utfärdande myndighetens system för e-legitimationer (se mer om utgivningsprocessen i avsnitt 7.4.2).

Denna gemensamma hantering av personuppgifter och myndigheternas respektive personuppgiftsansvar bör, i enlighet med förslagen i avsnitt 7.11.2, författningsregleras (se även avsnitt 7.11.5 om innehållet i den föreslagna databasen). Hur det elektroniska informations-

[186] polisen.se/tjanster-tillstand/pass-och-nationellt-id-kort/giltiga-svenska-resehandlingar/kontroll-av-passnationellt-id-kort/respektiveskatteverket.se/privat/folkbokforing/idkort/kontrolleranagon annansidkort.4.76a43be412206334b89800035809.html (hämtad 2023-06-01).

utbytet organiseras praktiskt mellan berörda myndigheter är en fråga för dessa att bestämma.

Den utfärdande myndigheten ska enligt förslaget om utgivningsprocess pröva ansökan i direkt anslutning till att grundidentifieringen har genomförts med ett positivt utfall och bekräftats i systemet av den identitetskontrollerande myndigheten (se avsnitt 7.4.2). Prövningen omfattar att kontrollera t.ex. att den åberopade identiteten finns registrerad i folkbokföringsdatabasen, och inte är markerad som avliden, försvunnen eller falsk. Som redan nämnts har myndigheter direktåtkomst till uppgifter i folkbokföringsdatabasen genom Navet. Det bedöms därmed inte heller för den utfärdande myndighetens vidkommande föreligga hinder i sekretesshänseende mot att utföra nödvändiga uppgifter för att utfärda en e-legitimation. Med beaktande härav finns inte heller i detta avseende något behov av sekretessbrytande bestämmelser.

Enligt vårt förslag om personuppgiftsbehandling ska det som ett sekundärt ändamål vara tillåtet att behandla uppgifter i databasen för statliga e-legitimationer, om det är nödvändigt för att tillhandahålla information som behövs i Polismyndighetens verksamhet för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller upprätthålla allmän ordning och säkerhet (se avsnitt 7.11.4).

Vi har som redovisas i avsnitt 7.11.9 inte bedömt att en allmän översyn kopplad till det brottsförebyggande eller brottsutredande arbetet omfattas av vårt uppdrag. Det kan dock uppmärksammas att personuppgifter som med stöd av den föreslagna ändamålsbestämmelsen tillhandahållits Polismyndigheten, under vissa förutsättningar, kan göras gemensamt tillgängliga för Ekobrottsmyndigheten och Säkerhetspolisen enligt 3 kap. 1 och 2 §§ lagen om polisens behandling av personuppgifter inom brottsdatalagens område. Genom bestämmelsen i 2 kap. 8 § samma lag får också bl.a. Åklagarmyndigheten och Skatteverket ta del av sådana personuppgifter som har gjorts gemensamt tillgängliga (med stöd av 3 kap. 2 §), om den mottagande myndigheten behöver uppgifterna i sin brottsbekämpande verksamhet. Mot denna bakgrund ser vi därför inte behov av att föreslå ytterligare sekretessbrytande regler i samband med dessa myndigheters brottsförebyggande och brottsutredande verksamheter.

7.13 Krav om att godta identifiering med vissa e-legitimationer

7.13.1 Inledning

Att e-legitimationsmarknaden domineras av en aktör och att det är mycket svårt för nya aktörer att etablera sig har länge lyfts fram som ett problem. I dagsläget finns inga krav om att förlitande parter i Sverige ska acceptera godkända svenska e-legitimationer. Det finns däremot krav om att erkänna utländska e-legitimationer i både eIDAS-förordningen och EU:s förordning om en gemensam digital ingång (se avsnitt 4.2.5). Det är således upp till de förlitande parterna att avgöra vilka svenska e-legitimationer de tillåter användare att identifiera sig med, och i många fall har förlitande parter inom både privat och offentlig sektor nöjt sig med att tillåta identifiering med endast BankID.

Enbart det faktum att en statlig e-legitimation i framtiden kommer att tillhandahållas innebär således inte nödvändigtvis att den kommer att gå att använda i olika e-tjänster då detta, om ingen reglering sker, är helt upp till de förlitande parterna.

Det är därmed av vikt att analysera om reglering om att godta den statliga e-legitimationen ska införas. Kopplat till denna fråga är även det uppdrag utredningen har om att analysera om det bör ställas krav på förlitande parter som tillhandahåller digitala tjänster inom offentlig sektor att acceptera alla e-legitimationsalternativ på marknaden förutsatt att de lever upp till den tillitsnivå som tjänsterna kräver.

7.13.2 Tidigare förslag och ställningstaganden

Inledning

Frågan om och hur det ska införas krav om att en statlig e-legitimation ska godtas samt krav som innebär att andra e-legitimationer måste godtas har utretts tidigare. I skrivande stund har emellertid inga av dessa förslag genomförts. Nedan redogörs för dessa förslag samt för remissinstansernas synpunkter.

Utredningen om effektiv styrning av nationella digitala tjänster

Förslaget om skyldighet att godta den statliga e-legitimationen

Utredningen om effektiv styrning av nationella digitala tjänster ansåg att den statliga e-legitimation de föreslog skulle fungera i alla e-tjänster där offentliga myndigheter kräver elektronisk identifiering. De uppgav att den statliga e-legitimationen ska vara en grundbult i den offentliga förvaltningen. Den ska också vara beständig över tid och inte beroende av om en offentlig myndighets upphandling omfattar den. Utredningen föreslog därför att det i deras föreslagna lag om statlig elektronisk identitetshandling skapas en skyldighet för alla offentliga myndigheter som kräver elektronisk identifiering i sina e-tjänster att godta den statliga e-legitimationen.[187]

Utredningen vidgick att det med en sådan bestämmelse kan hävdas att den statliga e-legitimationen kan vara konkurrenshämmande. De bedömde emellertid att syftet med den statliga e-legitimationen inte är att etablera en konkurrent till övriga e-legitimationer. Den statliga e-legitimationen skulle exempelvis inte uppfylla individers behov av mobila lösningar och utredningen fastslog vidare att individer därmed kommer att vilja använda den statliga e-legitimationen för att växla till sig en annan e-legitimation.[188]

Förslaget om obligatorisk anslutning till valfrihetssystemet

Utredningen föreslog även att alla statliga myndigheter, kommuner och regioner (då landsting, utr. anm.) med e-tjänster som kräver elektronisk identifiering ska ansluta sig till valfrihetssystemet. Utredningen bedömde att det ur ett förvaltningsövergripande perspektiv var mest effektivt om alla statliga myndigheter, kommuner och regioner anvisas ett sätt för anskaffning av funktion för elektronisk identitetskontroll. Genom ett anvisat och ensat sätt för alla offentliga myndigheter att anskaffa funktioner för elektronisk identitetskontroll skapas förutsättningar för att individer ges samma valmöjligheter när de ska identifiera sig elektroniskt vare sig detta görs hos en statlig myndighet, kommun eller region. Detta gjorde att utredningen bedömde att det var motiverat med ett förslag att statliga myndigheter, kommuner och regioner ska

[187] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 201.
[188] A.a. s. 202.

ansluta sig till valfrihetssystem. Utredningen bedömde vidare att en sådan skyldighet måste regleras i lag.[189]

Utredningen föreslog även att regeringen fick besluta om undantag från skyldigheten för statliga myndigheter, kommuner och regioner att ansluta sig till valfrihetssystem om det finns särskilda skäl. Utredningen bedömde att sådana särskilda skäl kan vara att den statliga myndigheten, kommunen eller regionen är bunden av befintliga avtalsvillkor som gör att den inte kan ansluta sig till valfrihetssystem eller att den måste genomföra omfattande tekniska anpassningar av sina egna system innan den kan följa de villkor som gäller inom valfrihetssystemet.[190]

Remissinstansernas synpunkter rörande förslaget om skyldighet att godta den statliga e-legitimationen[191]

E-hälsomyndigheten ansåg att det ur ett medborgarperspektiv var viktigt att inte endast statliga myndigheter, kommuner och regioner erkänner den statliga e-legitimationen utan att detta även omfattar vård-, omsorgsamt skolaktörer som drivs i privat regi.

Dåvarande *E-legitimationsnämnden* instämde i utredningens slutsats att alla offentliga myndigheter ska erkänna identifiering med den statliga e-legitimationen. Nämnden saknade dock att det i betänkandet inte förekom några överväganden om de upphandlingsrättsliga konsekvenserna av den reglering som utredningen föreslog. Funktion för identitetskontroll är en tjänst som offentliga myndigheter med dagens regelverk måste upphandla, oavsett om utfärdaren är en privat aktör eller en statlig myndighet.

Region Gotland framförde att behovet av elektronisk identifiering finns i hela samhället. Att då bara kravställa på den statliga e-legitimationen var enligt regionen inte rimligt. Regionen ansåg att kravet i stället borde vara att erkänna alla kvalitetsmärkta e-legitimationer.

Örebro kommun instämde i att den statliga e-legitimationen skulle fungera i alla e-tjänster där offentliga myndigheter kräver identifiering och att detta även ska gälla kommuner och landsting. Däremot ifrågasatte kommunen att såväl statliga myndigheter som kommuner och

[189] A.a. s. 230 f.
[190] A.a. s. 235.
[191] www.regeringen.se/remisser/2018/01/remiss-av-sou-2017114-reboot--omstart-for-den-digitala-forvaltningen/ (hämtad 2023-09-24).

regioner ska godta alla identitetshandlingar oavsett utfärdare. Detta då en bred flora av identifieringsmöjligheter via andra aktörers digitala identitetshandlingar riskerar att leda till ökade kostnader för de offentliga myndigheterna.

Skatteverket tillstyrkte förslaget men påtalade att det sannolikt skulle medföra omfattande kostnader för myndigheterna. Om det visade sig att problemen och kostnaderna var omfattande kunde det enligt Skatteverket vara lämpligt med en förlängd ikraftträdandebestämmelse, i varje fall för andra myndigheter än de statliga.

Sveriges Kommuner och Landsting (numera Sveriges Kommuner och Regioner) ansåg att kravet borde vara att erkänna alla kvalitetsmärkta elektroniska identitetshandlingar snarare än att specifikt peka ut den statliga elektroniska identitetshandlingen enskilt.

Skogsstyrelsen tillstyrkte att den elektroniska statliga identitetshandlingen ska erkännas hos alla statliga myndigheter, kommuner och regioner.

Stockholms läns landsting (numera Region Stockholm) bedömde att förslaget gick utöver den kommunala självstyrelsen och efterfrågade en kompletterande analys av påverkansgraden, särskilt inom hälso- och sjukvården.

Remissinstansernas synpunkter rörande förslaget om obligatorisk anslutning till valfrihetssystemet[192]

Tillväxtverket, *Konstnärsnämnden*, *Uppsala kommun*, *Örebro kommun*, *Skogsstyrelsen* och dåvarande *E-legitimationsnämnden* tillstyrkte utredningens förslag om ett krav på anslutning till valfrihetssystem.

Bolagsverket avstyrkte utredningens förslag och ansåg att behoven var olika för olika myndigheter och att det bör vara upp till respektive myndighet att besluta om en anslutning. Valfrihetssystemet hade dessutom enligt Bolagsverket hittills haft en mycket begränsad genomslagskraft.

E-hälsomyndigheten stödde i huvudsak utredningens förslag avseende valfrihetssystem. E-hälsomyndigheten saknade dock en analys av och jämförelse med eventuella andra möjliga modeller än valfrihetssystem. Förslaget att göra valfrihetssystemet obligatoriskt för alla myndigheter bygger på att valfrihetssystemet får en genomslagskraft

[192] www.regeringen.se/remisser/2018/01/remiss-av-sou-2017114-reboot--omstart-for-den-digitala-forvaltningen/ (hämtad 2023-09-24).

i praktiken, något som enligt myndigheten varit ett problem. E-hälsomyndigheten efterfrågade även en analys av vilka konsekvenser det kan få om myndigheter inte kan upphandla tjänster för elektronisk identifiering på annat sätt, t.ex. vid specifika behov, då behovet inte kan tillgodoses genom det inrättade valfrihetssystemet. E-hälsomyndigheten ansåg vidare att det ur ett medborgarperspektiv är viktigt att inte endast statliga myndigheter, kommuner och regioner ska ansluta sig, det är även viktigt att detta även omfattar privata aktörer inom vård och omsorg samt skola.

Länsstyrelsen i Västra Götalands län tillstyrkte förslaget men ansåg samtidigt att det var rimligt att det ska vara möjligt att få undantag när en offentlig myndighet har särskilda skäl för detta.

Skatteverket påtalade att myndigheten i grunden var positiv till valfrihetssystemet utifrån användarens och samhällets perspektiv men för att statliga myndigheter, kommuner och regioner ska ansluta sig till valfrihetssystemet måste några viktiga förutsättningar vara på plats. Obligatorisk anslutning till valfrihetssystemet kräver enligt Skatteverket att lösningen med en statlig grundidentifiering är genomförd och att BankID finns med i valfrihetssystemet då det är helt dominerande på marknaden. Förslaget innebar vidare enligt Skatteverket att det kommer bli ekonomiska konsekvenser som inte täcks av myndighetens anslag. Skatteverket har säkrat sin försörjning av e-legitimering via egen upphandling, detta genom att leverantör tillhandahåller de e-legitimationsutfärdare som Skatteverket kräver. För det fall det tillkommer nya utfärdare på marknaden är leverantören skyldig att ansluta även dessa om Skatteverket så vill. Den lösning som Skatteverket valt innebär att en myndighet kan upphandla tjänster som tillhandahåller flera olika e-legitimationer.

Valfrihetssystemet omhändertar enligt Skatteverket inte heller det operativa perspektivet för en myndighet. För att fungera praktiskt måste det skrivas ytterligare avtal vid sidan om valfrihetssystemet som reglerar säkerhetsaspekter, incidentproblem och förändringshantering, tillgänglighet, SIA, support och underhåll av miljöer, drift och förvaltning av tjänsten, dvs. all operativ samverkan som krävs för att myndighetens e-tjänst ska kunna nyttja e-legitimering och elektroniska underskrifter. Skälet till detta är enligt Skatteverket att olika myndigheter och kommuner har olika förutsättningar, såväl funktionella, tekniska, rättsliga och säkerhetsmässiga. Som exempel kan nämnas informationssäkerhetsområdet där den föreslagna lösningen kan leda till att

man håller hög säkerhet trots att tjänsterna som tillhandahålls av myndigheten inte har det kravet.

Statskontoret tillstyrkte förslaget och delade utredningens bedömning att individer ska ges samma identifieringsmöjligheter oavsett vilken statlig myndighet, kommun eller region som de ska identifiera sig elektroniskt mot. Myndigheten ansåg vidare att förslaget utgjorde ett exempel på en lämplig avvägning mellan effektiv styrning utifrån ett koncernperspektiv samtidigt som det medger en flexibilitet att undanta myndigheter vid behov.

Domstolsverket avstyrkte förslaget. Domstolsverket framförde att det i och för sig finns ett behov av styrning av statliga myndigheters, kommuners och regioners anskaffande av digitala tjänster och funktioner. Domstolsverket ansåg dock inte att användning av valfrihetssystem var ett ändamålsenligt sätt att ge denna styrning. Valfrihetssystem lämpar sig inte för digitala tjänster och funktioner eftersom denna typ av tjänster enligt myndigheten på grund av sin natur är och ska vara under konstant utveckling. En tydlig standardisering och certifiering av utfärdare var därför enligt Domstolsverket ett mer lämpligt sätt att uppnå sådan styrning.

Energimyndigheten framförde att det finns risker med att använda valfrihetssystem om systemet baseras på statsgemensamma priser till tekniskt gemensamma och styrande specifikationer för utfärdarna medför det en risk att leverantörer av kostnadsskäl eller tekniska skäl inte ansluter sig eller inte klarar att uppfylla kraven.

Finansiell ID-teknik BID AB uppgav att förutsatt vägvalet att använda valfrihetssystem för myndigheters försörjning av tjänster för elektronisk identifiering, så var de positiva till att via lag göra det tvingande för myndigheter, regioner och kommuner. Beräknat på nuvarande ersättningsnivåer som finns i Valfrihetssystem 2017 E-legitimering skulle mer än 50 procent av myndigheterna och kommunerna få en faktura på under 200 kronor varje månad, beräknat på faktiska BankID-volymer i november 2017. För nytillkomna utgivare med mindre volym än BankID, skulle detta förhållande vara ännu mer betungande. Bolaget önskade därmed att staten finner någon form av rimlig hantering för aktörer med låga volymer.

Försäkringskassan avstyrkte förslaget avseende valfrihetssystem och efterlyste att andra alternativ utreds vidare. Försäkringskassan anförde att de i likhet med flera andra myndigheter haft stora utmaningar med att säkra sin försörjning i och med att valfrihetssystemet haft

mycket begränsad genomslagskraft i praktiken och att myndigheterna med mycket kort varsel tvingats tillgå andra lösningar. Andra modeller än valfrihetssystem som på ett mer hållbart och långsiktigt sätt säkrar offentlig sektors och medborgarnas behov av e-legitimationer behöver därför utredas.

Försvarsmakten påtalade att utredningen i sitt förslag om undantaget på kravet om anslutning inte har beaktat den verksamhet som bedrivs inom försvarsområdet. Försvarsmakten ansåg att den egna myndigheten, tillsammans med övriga myndigheter inom försvarssektorn, ska undantas från förslaget. Detta med hänvisning till att försvarssektorns huvuduppgift är att försvara och upprätthålla rikets säkerhet. Ett lagkrav där försvarssektorn måste ansluta sig till valfrihetssystemet tar enligt Försvarsmakten till stor del bort möjligheten att påverka kravbilden gentemot leverantörerna vilket kan riskera men för rikets säkerhet.

Stockholms stad påtalade de problem som funnits med valfrihetssystemet och anförde också att det föreslagna valfrihetssystemet är begränsat eftersom det endast riktar sig till offentliga aktörer. Privata utförare omfattas inte av lösningen vilket innebär att invånarna kan behöva olika lösningar beroende på om utföraren är privat eller kommunal. Kommunen uppgav att det inte kan uteslutas att valfrihetssystem inom e-legitimationsområdet i sig är en funktionell lösning, men i dess hittillsvarande tillämpning finns inte mycket som tyder på det.

Stockholm läns landsting (numera Region Stockholm) anförde, i likhet med inställningen till förslaget om en skyldighet att godta den statliga e-legitimationen, att även detta förslag gick utöver den kommunala självstyrelsen och efterfrågade en kompletterande analys av påverkansgraden, särskilt inom hälso- och sjukvården.

Sveriges Kommuner och Landsting (numera Sveriges Kommuner och Regioner) underströk nödvändigheten av att föreslagna valfrihetssystem utformas så att privata utförare av offentlig service och näringslivet inte utestängs från att nyttja förvaltningsgemensamma digitala funktioner. Detta med anledning av att en invånare inte ser skillnad på skola och friskola, vårdcentral och privat vårdcentral osv.

Centrala studiestödsnämnden delade utredningens uppfattning att valfrihetssystemet i grund och botten är en bra lösning. Myndigheten påtalade emellertid att det är mycket viktigt att systemet blir attraktivt för leverantörer så att en mångfald skapas och att användare på så sätt kan välja vilken utfärdare som passar dem bäst. I annat fall blir valfri-

hetssystemet enligt CSN snarare en god tanke än en praktisk effektivisering.

2017 års ID-kortsutredning

Utredningens bedömning

Utredningen ansåg i likhet med Utredningen om effektiv styrning av nationella digitala tjänster att den statliga e-legitimationen ska kunna användas vid identifiering i e-tjänster i den offentliga sektorn. Utredningen utgick emellertid från att myndigheterna i samarbete med den utfärdande myndigheten ser till att möjliggöra en sådan identifiering. Någon lagreglerad skyldighet såg de dock inte behov av att införa. För det fall det framöver trots allt uppkommer ett behov av styrning i frågan bedömde de att det kan ske på annat sätt.[193]

Remissinstansernas synpunkter[194]

Försäkringskassan konstaterade att utredningen inte föreslog något obligatorium att acceptera den statliga e-legitimationen och att det inte heller utvecklades närmare i vilka situationer myndigheter bör använda den i stället för e-legitimationer på lägre tillitsnivåer. I den mån regeringen anser att alla myndigheter ska möjliggöra identifiering med den statliga e-legitimationen borde det enligt Försäkringskassan ske genom formell styrning i föreskrifter.

Digg underströk vikten av att den statliga e-legitimationen ska accepteras i offentliga e-tjänster oavsett hur regleringen sker.

Verisec AB framförde att utredningens ståndpunkt att förutsättningarna för att den statliga e-legitimationen skulle kunna ske genom samarbete i stället för att använda en lagreglerad skyldighet borde revideras om lagstiftaren önskade att bryta det monopol som finns. Utmaningen det offentliga Sverige har var enligt bolaget inte fler e-legitimationer utan att det offentliga inte erbjuder medborgarna att nyttja alla de alternativ som finns. Med mindre än att man från lagstiftarens håll kräver att offentliga e-tjänster kräver identifiering med e-legitimationer som har det statliga kvalitetsmärket Svensk e-legiti-

[193] *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14), s. 344 f.
[194] www.regeringen.se/remisser/2019/04/remiss-av-sou-201914-ett-sakert-statligt-id-kort--med-e-legitimation/ (hämtad 2023-09-24).

mation anförde bolaget att de praktiska problemen med en dominerande aktör kommer att kvarstå under överskådlig tid.

Promemoria om auktorisationssystem för elektronisk identifiering och för digital post

Förslaget om auktorisationssystem beskrivs närmare i avsnitt 4.7. I promemorian, som delvis ligger till grund för den nyligen lämnade propositionen om auktorisationssystem, föreslås att statliga myndigheter som har behov av tjänster för elektronisk identifiering ska använda de tjänster som tillhandahålls genom auktorisationssystem.[195] Eftersom förslaget i denna del endast var riktat mot statliga myndigheter gjordes bedömningen att regleringen lämpligen bör ske i förordning. Detta förslag behandlas därför inte i propositionen.[196]

Vad gäller frågan om vilken krets som ska omfattas av kravet på anslutning gjordes bedömningen att ett sådant krav för kommuner och regioner skulle inskränka det kommunala självstyret, då rätten att välja former för upphandling och avtalstecknande med leverantörer på e-legitimationsområdet skulle begränsas. I promemorian anfördes att införandet av ett sådant obligatorium sannolikt skulle ha marginella ekonomiska konsekvenser för kommuner och regioner. Det bedömdes emellertid att mindre långtgående alternativ till att uppställa krav som även omfattar kommuner och regioner bör övervägas. I promemorian framgick att de statliga myndigheterna står för cirka 70 procent av den offentliga förvaltningens samlade användning av tjänster för elektronisk identifiering. Ett krav på användning av tjänster för elektronisk identifiering för enbart statliga myndigheter skulle därmed ge i stort sett likvärdiga effekter som ett obligatorium för hela den offentliga förvaltningen. En hög anslutningsgrad kan alltså enligt promemorian uppnås samtidigt som kommuner kan erbjudas en större flexibilitet utifrån förutsättningarna i varje enskild kommun. I promemorian gjordes därmed bedömningen att övervägande skäl talar för att kravet på att använda tjänsterna inom auktorisationssystemen bör begränsas till statliga myndigheter med behov av tjänster för elektronisk identifiering.[197]

[195] *Auktorisationssystem för elektronisk identifiering och för digital post*, s. 41 ff.
[196] Prop. 2023/24:6.
[197] *Auktorisationssystem för elektronisk identifiering och för digital post*, s. 42 f.

Kravet borde enligt promemorian gälla oavsett vilken tillitsnivå för den elektroniska identifieringen som myndigheten tillämpar för åtkomst till de digitala tjänsterna, under förutsättning att det inom de inrättade auktorisationssystemen finns tjänster för den tillitsnivå som myndigheten tillämpar.[198]

Eftersom de statliga myndigheterna har anskaffat tjänster för elektronisk identifiering på olika sätt, fanns det enligt promemorian stora skillnader i löpande avtalstider. Flera statliga myndigheter kommer därmed att vara bundna av avtal som löper längre än det tilltänkta ikraftträdandedatumet för förordningen. Det gick inte heller enligt promemorian att utesluta att myndigheter kan komma att teckna avtal utanför existerande valfrihetssystem fram till dess. För att myndigheter inte ska hamna i en situation där tidigare ingångna avtal löper parallellt med kravet på användning av tjänster för elektronisk identifiering inom auktorisationssystemen bör det finnas en möjlighet att bevilja tidsbegränsade undantag från kravet. I promemorian föreslogs därför att Digg ska få besluta om sådana undantag. Undantag skulle dock beviljas med stor restriktivitet. Ett exempel på en situation där undantag kunde beviljas var när avtalsrättsliga förpliktelser gentemot tredje part förhindrar en övergång till auktorisationssystem och ett upphörande i förtid skulle leda till orimliga konsekvenser för myndigheten i fråga. Det faktum att en enskild myndighet inte är nöjd med de tjänster som erbjuds inom inrättade auktorisationssystem bör enligt promemorian inte vara grund för undantag.[199]

I promemorian bedömdes vidare att förutom i direkt anslutning till ikraftträdandet bör undantag inte förekomma annat än i undantagsfall. Det skulle kunna vara fallet om de godkända leverantörerna i auktorisationssystemet enbart representerar en begränsad krets av användare, t.ex. om de största leverantörerna inte ansluter sig. Digg kan då komma att behöva meddela ett generellt undantag som gäller för samtliga myndigheter. På så sätt kan det undvikas att det uppstår en situation där statliga myndigheter blir skyldiga att använda tjänster i auktorisationssystem som inte innefattar de största leverantörerna.[200]

I promemorian framfördes även att det kan uppstå behov av att inrätta parallella eller delvis överlappande auktorisationssystem. Exempelvis kan det inrättas auktorisationssystem som tar sikte på olika

[198] A.a. s. 43.
[199] A.a. s. 44.
[200] Ibid.

tillitsnivåer eller på olika tekniska lösningar som inte lämpar sig för att hanteras samlat inom ett och samma auktorisationssystem. Det bör därför enligt promemorian finnas en möjlighet för Digg att meddela föreskrifter om dels vilka tjänster för elektronisk identifiering inom auktorisationssystemen som kravet på användning avser, dels hur skyldigheten att använda tjänsterna ska fullgöras.[201]

Sammantaget gjordes i promemorian bedömningen att kostnaderna för teknisk anpassning blir marginella för de statliga myndigheterna, under förutsättning att den tekniska kravställningen för nya e-legitimationsutfärdare hålls snarlik den kravställning som görs för anslutning till förbindelsepunkterna för gränsöverskridande elektronisk identifiering.[202]

I promemorian noterades även att om 2017 års ID-kortsutrednings förslag om en statlig e-legitimation på högsta tillitsnivå genomförs får det övervägas i särskild ordning om det bör vara obligatoriskt för statliga myndigheter att använda även den tjänsten och hur detta i så fall bör regleras.[203]

Remissinstansernas synpunkter[204]

Centrala studiestödsnämnden uttalade att det både ur ett medborgar- och myndighetsperspektiv finns stor nytta i att en enskild kan använda samma e-legitimation hos samtliga statliga myndigheter. Denna nytta förutsätter att auktorisationssystemet är attraktivt för leverantörerna av tjänster för elektronisk identifiering att ansluta till. Det är olyckligt om leverantörer som representerar en majoritet av användarna inte ansluter sig och att myndigheternas möjlighet att använda tjänster tillhandahållna av en sådan leverantör annat än tillfälligt behöver bygga på undantag medgivna av Digg. Detta kan i så fall innebära både merkostnader och ökad administration för de statliga myndigheterna. För det fall en tjänst för elektronisk identifiering som är godkänd i auktorisationssystemet konstateras ha säkerhetsbrister kan Digg rimligen säga upp avtalet med leverantören eller medge undantag för de statliga myndigheterna att dessa inte behöver använda leverantörens tjänster.

[201] *A.a.* s. 44 f.
[202] A.a. s. 50.
[203] A.a. s. 43.
[204] www.regeringen.se/remisser/2020/12/remiss-av-promemoria-auktorisationssystem-for-elektronisk-identifiering-och-for-digital-post/ (hämtad 2023-09-24).

Dessa åtgärder kan dock i allmänhet inte ske omedelbart efter att en säkerhetsbrist har uppmärksammats. Det är viktigt att de statliga myndigheterna i en sådan situation har möjlighet att upphöra med användningen av tjänsten redan innan Digg har agerat enligt ovan.

Digg delade promemorians bedömning att möjlighet att meddela tidsbegränsade undantag från kravet på statliga myndigheters anslutning ska meddelas med stor restriktivitet. Digg kommer att ställa krav på att aktörer som ansluts till auktorisationssystemet ska ha förutsättningar att ansluta samtliga godkända leverantörer. Det är i enlighet med lagens syfte enligt Digg att enskilda ska ha rätt att välja den leverantör som ska utföra tjänsterna för deras räkning. Kraven att ansluta samtliga godkända leverantörer kan enligt Digg bli betungande i genomförande och kan få ekonomiska konsekvenser för anslutande offentliga aktörer.

Ekonomistyrningsverket tillstyrkte att det ska ställas krav på att statliga myndigheter som har behov av tjänster för elektronisk identifiering använder sig av de tjänster som erbjuds genom auktorisationssystemet.

Försvarsmakten anförde att de behöver full rådighet och handlingsfrihet att välja vilka tjänster som ska användas för respektive tillämpningsfall med hänsyn till myndighetens operativa uppgifter i hela konfliktskalan. Att tvingas nyttja vissa tjänster skulle innebära en begränsning i myndighetens hantering av uppgifter och information, särskilt de med höga krav på tillgänglighet och säkerhetsskydd. Försvarsmakten framförde att de borde ha en möjlighet att använda sig av tjänster för elektronisk identifiering som tillhandahålls genom det föreslagna auktorisationssystemet, men samtidigt kunna använda sig av andra tjänster för elektronisk identifiering om det är motiverat av säkerhetsskäl. De tyckte inte heller att det är lämpligt att behöva ansöka om undantag då detta kan riskera att menligt inverka på informationssäkerheten.

Försäkringskassan pekade på att förslaget innebar en risk för högre kostnader samt inlåsningseffekter. Försäkringskassan påtalade vidare att myndighetens verksamhet i dag i praktiken är helt beroende av att medborgarna kan identifiera sig elektroniskt. Försäkringskassans ansvar och möjligheter att säkra behoven, bl.a. givet aktuell hotbild, bör inte begränsas. En leverantör som medborgarna föredrar att använda kan välja att inte vara en del av ett auktorisationssystem och med ett obligatorium skulle det begränsa möjligheten att säkra försörjningen av nödvändiga leverantörer utanför auktorisationssystemet. Om För-

säkringskassan identifierar hot och risker hos en leverantör behöver myndigheten också ha möjligheten att stänga av leverantören för att skydda allmänheten och den egna verksamheten.

Kronofogdemyndigheten uttalade att myndigheten var tveksam till förslaget till följd av farhågor om att det kan bli kostnadsdrivande. Det var emellertid enligt myndigheten svårt att bedöma kostnader och andra konsekvenser av förslaget utifrån den information som fanns i promemorian.

Migrationsverket framförde att det inte framgick om verket kan fortsätta att använda identifieringslösningar som inte är del av auktorisationssystemet.[205] Migrationsverket ställer sig därför frågande till om de e-tjänster som myndigheten tillhandahåller sökande genom förslaget begränsas till att endast tillhandahålla identifiering via auktorisationssystemet eller om det fortsättningsvis blir tillåtet att exempelvis tillhandahålla en egen identifieringstjänst som komplement till auktorisationssystemets tjänster. Problematiken för Migrationsverket var att deras sökanden använder användarnamn och lösenord för att få tillgång till de e-tjänster myndigheten tillhandahåller då sökandena inte är svenska medborgare och inte har en e-legitimation. Migrationsverket önskade därför ett förtydligande i om verksamheten kan fortsätta tillhandahålla egna identifieringslösningar utanför auktorisationssystemet där det finns ett befogat behov att frångå valfrihetssystemet. Om det exempelvis krävs svensk folkbokföring så kommer Migrationsverket inte kunna använda auktorisationssystemet fullt ut.

Myndigheten för samhällsskydd och beredskap (MSB) yttrade att då det är tillhandahållande myndighet som ska vara ansvarig för kravställning mot leverantörerna i auktorisationssystemet är det av vikt att statliga myndigheter ges möjlighet att löpande föra dialog med tillhandahållande myndighet rörande både initiala säkerhetskrav och behov av förändringar i kravställning för auktorisationssystemet. Vidare bör enligt MSB statliga myndigheter ges möjlighet att avvakta med att ansluta sig tills dess att de – som informationsägare – har bedömt att tillräcklig säkerhet kan garanteras för auktorisationssystemet. Det är varje myndighets eget ansvar att genomföra riskanalyser i syfte att bedöma vilken information som myndigheten ska tillåta respektive inte tillåta vara åtkomlig genom auktorisationssystemet. MSB noterade att Digg ställer krav på utfärdare av e-legiti-

[205] Migrationsverket använder sig genomgående av begreppet valfrihetssystem i stället för auktorisationssystem i remissvaret. Här ändrat till auktorisationssystem för att underlätta förståelsen.

mationer genom avtal som refererar exempelvis till ”Tillitsramverk för kvalitetsmärket Svensk e-legitimation” där det exempelvis anges att ”efterlevnad av krav ska under en treårsperiod vara föremål för internrevision av oberoende intern eller extern kontrollfunktion”. Det bör enligt MSB fastställas att tillhandahållande myndighet ska samråda med MSB rörande den kravställning mot leverantörerna som berör informationssäkerhet. Det bör också klargöras om det finns begränsningar i hur statliga myndigheter får använda de system för elektronisk identifiering som inte är anslutna till auktorisationssystemet. Det bör vidare klargöras vilka ansvarsförhållanden som gäller för; leverantör, tillhandahållande myndighet, offentlig aktör och den enskilde då en elektronisk identifiering missbrukas, exempelvis då en e-legitimation utfärdats till bedragare och använts för åtkomst av information hos offentlig aktör. Det bör klargöras hur en leverantör kan sanktioneras och/eller helt stängas av från medverkan i auktorisationssystem, exempelvis då denna a) ej längre uppfyller säkerhetskraven i auktorisationssystemet eller b) denna utsatts för ett angrepp som omöjliggör tillit till utgivna e-legitimationer eller den tjänst som utger SAML-intyg. Det bör enligt MSB även klargöras – alternativt kravställas – hur och när uppföljning och tillsyn av leverantör ska ske, i syfte att identifiera informationssäkerhetsbrister och andra avvikelser från de krav som ställts för medverkan i auktorisationssystemet. Det bör därtill enligt MSB klargöras – alternativt kravställas – hur och när leverantör ska rapportera incidenter.

Nacka kommun påtalade vikten av att kommuner frivilligt får nyttja egna lösningar även framgent. Ett krav på att kommuner och regioner måste nyttja auktorisationssystem skulle enligt kommunen inskränka det kommunala självstyret, då rätten att välja former för upphandling och avtalstecknande med leverantörer på e-legitimationsområdet skulle begränsas.

Polismyndigheten avstyrkte förslaget. Om förslaget ändå genomförs ansåg Polismyndigheten att det bör införas en utökad möjlighet för statliga myndigheter att begära undantag från kravet. Polismyndigheten såg vissa svårigheter ur informationssäkerhetsperspektiv med ett krav på anslutning till auktorisationssystem. Myndigheterna har t.ex. inte någon kontroll över vilka nya leverantörer som får ansluta till systemet. Vid tillhandahållande av tjänster med högre skyddsvärden kan det därför vara olämpligt ur informationssäkerhetssynpunkt för myndigheter att ansluta till auktorisationssystem. Det bör även fort-

sättningsvis vara möjligt för statliga myndigheter att upphandla separata lösningar, t.ex. vid specifika behov av informationssäkerhet som inte kan tillgodoses inom ramen för auktorisationssystem. Ett krav på anslutning kan därmed innebära att myndigheten inte kan tillhandahålla digitala tjänster med elektronisk identifiering i lika stor utsträckning som annars.

Post- och telestyrelsen (PTS) tillstyrkte promemorians förslag med undantag av förslaget om att endast statliga myndigheter ska omfattas av kravet på användning av tjänster för elektronisk identifiering inom auktorisationssystem. För att kunna erbjuda likvärdig service av god kvalitet i hela landet och förenkla för enskilda att utöva sina rättigheter, fullgöra sina skyldigheter och ta del av den offentliga förvaltningens service, ansåg PTS att förslaget om krav på användning av tjänster för elektronisk identifiering inom auktorisationssystem, även ska inkludera kommuner. PTS ansåg vidare, mot bakgrund av att kunna erbjuda privatpersoner och företag likvärdig service av god kvalitet i hela landet och förenkla för enskilda att utöva sina rättigheter, fullgöra sina skyldigheter och ta del av den offentliga förvaltningens service, att systemet ska omfatta även kommuner. Kommuner tillhandahåller samhällsviktig service till medborgare genom digitala tjänster, såsom hemtjänster, olika former av social service och intyg, m.m. Det innebär att kommuner också behöver kommunicera alltmer digitalt. Att tillgängliggöra auktorisationssystemet för kommuner kan enligt PTS således underlätta för kommuner att sköta kommunikationen digitalt genom att bespara dem de resurser som kommunerna annars hade behövt lägga på att bl.a. själva ingå avtal med leverantörer.

Skatteverket ansåg att var svårt att överblicka de ekonomiska konsekvenserna av en obligatorisk anslutning till auktorisationssystem. Problematiken med auktorisationssystemet är att det inte omhändertar Skatteverkets behov av heltäckande lösningar. Vad som innefattas av auktorisationssystemet är endast en del av hela systemlösningen som är nödvändig för att säkerställa myndighetens behov av tillgängliga och stabila lösningar för e-legitimering och elektroniska underskrifter. För att Skatteverket ska kunna använda auktorisationssystemet i praktiken tillkommer sannolikt omförhandling av befintligt avtal alternativt ny upphandling. Som exempel har Skatteverket genom eget avtal omhändertagit behovet av skyndsam hantering och tillgängliggörande av e-legitimationer på marknaden som har fått, och kommer att få, kvalitetsmärket Svensk e-legitimation. Därigenom uppnås också

användarens möjlighet till valfrihet vid val av e-legitimation. Skatteverket anser att det är viktigt att utforma lösningen så att den inte blir sårbar ur ett samhällsperspektiv, bl.a. genom att säkerställa god tillgänglighet och hög prestanda. Enskilda myndigheter kan också behöva erbjudas möjlighet till direkt dialog med utfärdarna av e-legitimation i samband med incidenter eller verksamhetskritiska händelser såväl planerade som oförutsedda. Det är viktigt att deltagande aktörer i auktorisationssystemet har full insyn och har möjlighet att påverka utformning. Skatteverket anser vidare att det finns oklarheter i de fall en myndighet agerar värdmyndighet. Skatteverket är i dag värdmyndighet åt andra myndigheter och omhändertar i vissa fall åt dessa identifiering och underskrift med e-legitimation. Promemorian belyser inte hur dessa situationer ska hanteras när det kommer till obligatorisk anslutning till auktorisationssystem. Detsamma gäller även samverkanslösningar, t.ex. verksamt.se där Bolagsverket ombesörjer identifiering med e-legitimation på webbplatsen. Skatteverket anser att undantagsbestämmelserna beträffande obligatorisk anslutning till auktorisationssystem för e-identifiering behöver tillämpas generöst under en övergångsperiod.

I takt med att digitaliseringen ökar ställs allt högre krav på att Skatteverkets tjänster helt eller delvis ska vara nåbara även för målgrupper av användare som i dag inte har möjlighet att använda svenska e-legitimationer. Det är oklart om auktorisationssystemet kommer att hantera behovet av lägre tillitsnivåer än de som i dag omfattas av kvalitetsmärket Svensk e-legitimation. Skatteverkets tolkning är att auktorisationssystemet riskerar att endast uppfylla en delmängd av behoven vilket innebär att Skatteverket även framöver kommer att behöva upphandla ytterligare lösningar. Det kan inte uteslutas att det kan finnas lösningar som faller utanför det tillitsramverk som avses, eller som i vart fall kan vara svåra att avgöra till vilken tillitsnivå de hör. Det kan med andra ord uppstå en problematik kring gränsdragning för när tjänster inom auktorisationssystemen ska tillämpas.

Skatteverket hade svårt att uppskatta de merkostnader som förslaget innebär och exakt hur auktorisationssystemet för e-legitimering ekonomiskt kommer att påverka myndigheten. Under 2021 beräknas antalet slagningar landa på drygt 78 000 000 (avser Skatteverket, Kronofogdemyndigheten, Min Myndighetspost och Valmyndigheten).

Skolverket tillstyrkte att det blir obligatoriskt för statliga myndigheter att använda sig av tjänster inom auktorisationssystemet när det

gäller elektronisk identifiering. Skolverket förutsätter dock att detta inte innebär ett hinder mot att använda andra metoder för identifiering i digitala tjänster, än sådana som utgör tjänster för elektronisk identifiering i den föreslagna lagens mening. Specifikt utgår myndigheten från att kravet inte förhindrar användning av så kallad federerad inloggning, där identifiering i en digital tjänst hos Skolverket exempelvis kan ske via identitetsfederationer såsom Skolfederation och SWAMID.

Säkerhetspolisen anförde att det bör övervägas om statliga myndigheter som bedriver säkerhetskänslig verksamhet ska kunna besluta om undantag från kravet att använda tjänster för elektronisk identifiering inom auktorisationssystem.

Upphandlingsmyndigheten påtalade att för att bl.a. ta tillvara digitaliseringens möjligheter att effektivisera den offentliga sektorn samt för att förenkla för enskilda så bör kravet på att använda tjänsterna inom auktorisationssystem för elektronisk identifiering även gälla kommuner och regioner.

Örebro kommun anförde att kravet på obligatorisk anslutning även bör omfatta kommuner och regioner. Detta skulle öka förutsättningarna för att de gemensamma målen för den offentliga sektorn gällande digitalisering ska vara möjliga att realisera. Ett viktigt steg är att det ska vara möjligt för medborgare och företag att ha sina myndighetskontakter i digital form, även gentemot kommuner och regioner.

Myndigheten för digital förvaltning

I sin rapport om hur en statlig e-legitimation kan utformas konstaterar Digg att det inte bara räcker att den statliga e-legitimationen finns, utan att den även måste gå att använda.[206]

För att åstadkomma detta måste enligt Digg statliga myndigheter, kommuner och regioner acceptera alla e-legitimationer som Digg har granskat och godkänt. I dag får varje offentlig aktör själv bestämma vilka e-legitimationer som kan användas vid inloggning i de digitala tjänsterna. Digg har i en tidigare rapport till regeringen gjort bedömningen att en av de mest centrala åtgärderna på e-legitimationsområdet är att alla digitala tjänster ska acceptera alla e-legitimationer med tillräcklig tillitsnivå. Detta kräver lagstiftning.[207]

[206] Myndigheten för digital förvaltning, *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, s. 2.
[207] A.a. s. 13 f.

Digg hänvisade här till en tidigare rapport benämnd *Utveckling av det svenska e-legitimationssystemet* där myndigheten bedömt att man bör lagstifta om att alla offentliga myndigheter ska ansluta till auktorisationssystem för elektronisk identifiering och därmed godta alla av Digg godkända e-legitimationer som finns med under förutsättning att e-legitimationen i det aktuella fallet når erforderlig tillitsnivå. Att utöka kretsen som träffas av obligatoriet till även kommuner och regioner skulle öka efterfrågan på nya e-legitimationer. Den uppfattas i dag av e-legitimationsmarknaden som för liten då digitala tjänster bara godtar de etablerade e-legitimationerna som det stora flertalet använder. Detta gör det svårt för nya e-legitimationsutfärdare att få lönsamhet i att utveckla nya e-legitimationslösningar och få dem granskade och godkända av Digg. Här är auktorisationssystem med obligatorisk anslutning av statliga myndigheter som förlitande parter ett steg i rätt riktning, men ytterligare åtgärder krävs som ökar incitamenten för kommunala och regionala digitala tjänster att välkomna alla godkända e-legitimationer som Digg har avtal med. Digg anser att man bör lagstifta om att alla offentliga myndigheter ska ansluta till auktorisationssystem för elektronisk identifiering och därmed godta alla av Digg godkända e-legitimationer som finns med under förutsättning att e-legitimationen i det aktuella fallet når erforderlig tillitsnivå.[208]

Digg bedömer i rapporten om den statliga e-legitimationen att den tidigare föreslagna åtgärden att införa ett obligatorium i allra högsta grad är fortsatt angelägen och relevant. När en statlig e-legitimation införs krävs att den också kan användas för att uppfylla samhällets krav på säkerhet, tillgänglighet och robusthet i en säkerhetspolitiskt orolig tid. Digg anser att den statliga e-legitimationen ska finnas med som en del i det ekosystem som byggts upp under lång tid. Den statliga e-legitimationen ska utgöra ett komplement och en möjlighet att växla över till andras lösningar, inte en konkurrent eller ersättare. Vad som däremot är helt centralt är att den statliga e-legitimationen erbjuds tillsammans med samtliga godkända e-legitimationer i alla digitala tjänster i den offentliga förvaltningen. Det är alltså inte bara statliga myndigheter som bör omfattas av ett sådant obligatorium. För att så många som möjligt ska kunna identifiera sig digitalt måste

[208] Myndigheten för digital förvaltning, *Utveckling av det svenska e-legitimationssystemet (*dnr 2021–2493), s. 35.

även regioner och kommuner godta alla e-legitimationer som Digg har godkänt.[209]

7.13.3 Behövs det författningsreglerade krav?

Utredningens bedömning: Det behövs författningsreglering som uppställer krav om att den statliga e-legitimationen ska godtas för identifiering i digitala tjänster.

Skälen för utredningens bedömning

2017 års ID-kortsutredning är ensamma om att inte föreslå någon reglering som direkt eller indirekt leder till att en statlig e-legitimation skulle behöva godtas av offentliga aktörer. Utredningen utgick från att myndigheterna i samarbete med den utfärdande myndigheten skulle möjliggöra en sådan identifiering. Även om vi givetvis ser positivt på frivilligt samarbete inom offentlig sektor anser vi att både historiken och nuläget tydligt visar att det inom e-legitimationsområdet behövs styrning avseende möjliggörande av användning av den statliga e-legitimationen i digitala tjänster för att flera av de mål som uppställs i våra direktiv kan uppnås.

7.13.4 Vilka digitala tjänster, e-legitimationer och aktörer bör kravet omfatta?

Utredningens förslag: När en e-legitimation krävs för att få tillgång till en nättjänst som tillhandahålls av en offentlig aktör, och tjänsten helt eller delvis riktar sig till privatpersoner, ska medel som tillhandahålls av leverantör som är godkänd i enlighet med den föreslagna lagen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post erkännas för autentisering för tjänsten.

Kravet gäller endast om tillitsnivån för medlet för elektronisk identifiering motsvarar en tillitsnivå som är lika hög eller högre än

[209] Myndigheten för digital förvaltning, *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, s. 14.

den tillitsnivå som den offentliga aktören kräver för åtkomst till nättjänsten.

Kravet ska gälla för statliga myndigheter, kommuner, regioner och sammanslutningar av dessa aktörer samt aktörer som yrkesmässigt bedriver verksamhet som till någon del är offentligt finansierad och som

1. bedrivs av aktören i egenskap av enskild huvudman inom skolväsendet eller huvudman för en sådan internationell skola som avses i 24 kap. skollagen,
2. utgör hälso- och sjukvård enligt hälso- och sjukvårdslagen eller tandvård enligt tandvårdslagen, eller
3. bedrivs enligt socialtjänstlagen, lagen om vård av missbrukare i vissa fall, lagen med särskilda bestämmelser om vård av unga, lagen om stöd och service till vissa funktionshindrade eller utgör personlig assistans som utförs med assistansersättning enligt 51 kap. socialförsäkringsbalken.

Kravet ska även gälla enskilda utbildningsanordnare med tillstånd att utfärda examina enligt lagen om tillstånd att utfärda vissa examina, och som till största delen har statsbidrag som finansiering av högskoleutbildning på grundnivå eller avancerad nivå eller för utbildning på forskarnivå.

Utredningens bedömning: Frågan om det inom hela eller delar av den privata sektorn bör ställas krav på att acceptera vissa e-legitimationer bör utredas vidare.

Det bör även utredas huruvida utfärdare av e-legitimationer som godkänts enligt tillitsramverket för Svensk e-legitimation bör ges tillgång till för verksamheten relevanta uppgifter från vissa myndighetsregister.

Skälen för utredningens förslag och bedömning

Innan frågan om hur regleringen ska utformas hanteras behöver det först klargöras vad regleringen syftar till att uppnå och vilka eventuella problem med en regleringslösning som behöver beaktas.

Som framgår av avsnitt 7.13.3 ser vi att en reglering krävs för att uppnå flera i våra direktiv uppställda mål. Detta gäller framför allt målen om att uppnå en ökad tillgänglighet och en mer robust marknad för e-legitimationer. Således de behov som det redogörs för i avsnitt 6.5 och 6.6.

När det gäller effekter av en reglering som behöver beaktas är det naturligtvis så att införandet av krav medför kostnader för aktörer som inte i dagsläget uppfyller kravet. Dessa ekonomiska konsekvenser redogörs det för i avsnitt 9.7.1.

Regleringen får inte leda till osund konkurrens

En annan aspekt av en reglering som uppställer krav på användning är att den – om den endast omfattar den statliga e-legitimationen – kan skapa osund konkurrens. Utredningen om effektiv styrning av nationella digitala tjänster föreslog att det ska lagstiftas om en skyldighet för alla offentliga myndigheter som kräver elektronisk identifiering i sina digitala tjänster att godta den statliga e-legitimationen. Utredningen vidgick att detta innebar att det kunde hävdas att den statliga e-legitimationen kunde vara konkurrenshämmande. Slutsatsen var dock att syftet med den statliga e-legitimationen inte var att konkurrera med andra e-legitimationer.

Vi anser att det som skrivits om konkurrensfrågan i tidigare utredningar inte är alltigenom stringent. Även om syftet inte är att konkurrera med privata e-legitimationsutfärdare blir en statlig e-legitimation – som kan användas på samma sätt som andra e-legitimationer – de facto en konkurrerande lösning även om den till följd av exempelvis bärare kan antas vara ett mindre attraktivt alternativ för flertalet användare. Det finns även exempel på argument om att den statliga e-legitimationen av denna anledning inte är en konkurrent till andra e-legitimationer. Vi bedömer dock att det skapar en olycklig inlåsningseffekt om konkurrensanalysen låses fast vid en typ av bärare. Vi anser att ett förslag om införande av en statlig e-legitimation i möjligaste mån måste ta höjd för framtida teknisk utveckling och en analys som indirekt utgår från en viss teknisk lösning kan inte anses vare sig lämplig eller önskvärd. Konkurrensanalysen måste därmed utgå från att den statliga e-legitimationen i ett senare skede kan komma att erbjudas i form av en mobil lösning.

Även om syftet med en statlig e-legitimation inte är att konkurrera med privata alternativ, utan att i stället vara ett komplement, rör det sig om offentlig säljverksamhet som i detta avseende är en konkurrent till privata alternativ (se mer om konkurrensaspekterna i avsnitt 7.10). Vi anser således att en reglering som ger den statliga e-legitimationen fördelar i relation till privata alternativ är konkurrensbegränsande. Ett lagkrav om att en statlig e-legitimation ska godtas leder därmed till osund konkurrens från statens sida. Att utöka lagkravet till att även omfatta fler e-legitimationer skulle dock läka detta.

Som tidigare framgått har utredningen i uppdrag att analysera om det bör ställas krav på förlitande parter som tillhandahåller digitala tjänster inom offentlig sektor att acceptera alla e-legitimationsalternativ på marknaden förutsatt att de lever upp till den tillitsnivå som tjänsterna kräver.

Som framgår av avsnitten 6.5 och 6.6 är både ökad tillgänglighet och robusthet behov som delvis kan tillgodoses genom införandet av en statlig e-legitimation. Dessa behov kan dock även i stor utsträckning tillgodoses genom förbättrad konkurrens mellan privata utfärdare. Sådana aktörer kan även leverera mobila och innovativa lösningar som vi inte ser som den statliga e-legitimationens roll att uppfylla i dagsläget, även om en framtida utveckling av en mobil lösning kan vara möjlig. Att ha en välfungerande marknad för privata utfärdare är därmed något som är av stor betydelse för att uppnå ökad tillgänglighet och robusthet. Ett stort hinder för att uppnå en fungerande marknad för e-legitimationer är att det i dagsläget finns en dominerande aktör i form av BankID och att många förlitande parter endast godtar identifiering med denna e-legitimation. Detta påverkar givetvis hur användbara alternativa e-legitimationer upplevs vara och därigenom även hur attraktiva de är för användare att anskaffa. Det finns således med beaktande av både tillgänglighet och robusthet starka argument för att uppställa krav om att förlitande parter som tillhandahåller digitala tjänster inom offentlig sektor ska acceptera alla e-legitimationsalternativ på marknaden förutsatt att de lever upp till den tillitsnivå som tjänsterna kräver. Därtill kommer de ovan beskrivna konkurrensrättsliga aspekter som införandet av en statlig e-legitimation medför. Något som således också talar för att krav på att acceptera vissa e-legitimationer bör införas.

För vilka e-legitimationer ska kravet gälla?

Frågan är härnäst vilka e-legitimationer som ska omfattas. Om det uppställs krav på att vissa e-legitimationer ska gå att använda måste det säkerställas att dessa e-legitimationer lever upp till den tillitsnivå som tjänsterna kräver. Mot denna bakgrund är det naturligt att ha det svenska tillitsramverket som utgångspunkt (se mer om detta i avsnitt 4.3).

Utöver e-legitimationer som utfärdas till privatpersoner finns det även flera e-tjänstelegitimationer bland de e-legitimationer som har granskats och godkänts inom ramen för Diggs tillitsramverk. Det är således inte lämpligt att kravet omfattar alla dessa e-legitimationer. Därtill kompliceras kravställning med hänvisning till tillitsramverket genom att det inte är författningsreglerat.

Tillitsramverket utgör emellertid en central del i att bli godkänd i enlighet med valfrihetsystemen och föreslaget auktorisationssystem. Mot denna bakgrund anser vi att kravet bör omfatta de e-legitimationer som tillhandahålls av leverantör som är godkänd i enlighet med den föreslagna lagen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post. Att hänvisning görs till den föreslagna lagen och inte nuvarande valfrihetssystem grundar sig i att vi utgår från att förslagen i den nyligen lämnade propositionen kommer att genomföras.[210]

Vilka aktörer ska omfattas av kravet?

Utredningen om effektiv styrning av nationella digitala tjänster föreslog både att en statlig e-legitimation skulle fungera i alla digitala tjänster där offentliga myndigheter kräver elektronisk identifiering och att alla statliga myndigheter, kommuner och regioner med digitala tjänster som kräver elektronisk identifiering ska ansluta sig till valfrihetssystemet.[211]

I promemorian om auktorisationssystem för elektronisk identifiering och för digital post föreslås vidare att det ska ställas krav om att statliga myndigheter ska ansluta till auktorisationssystem. Denna avgränsning motiverades i huvudsak med att en hög anslutningsgrad kan uppnås enbart genom att ställa krav på att statliga myndigheter

[210] Se mer som förslagen i prop. 2023/24:6.
[211] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 201 f. och s. 230 ff.

ansluts samtidigt som kommuner kan erbjudas en större flexibilitet utifrån förutsättningarna i varje enskild kommun.[212]

Digg har å sin sida föreslagit att alla statliga myndigheter, kommuner och regioner med digitala tjänster som kräver elektronisk identifiering ska ansluta sig till valfrihetssystemen.[213]

Vi kan konstatera att det i närtid gjorts olika bedömningar rörande vilka aktörer som ska omfattas av obligatoriska krav som påverkar vilka e-legitimationer som måste godtas i aktörernas digitala tjänster. Bedömningarna har emellertid haft olika utgångspunkter utifrån de olika syften förslagen skulle tillgodose. I vårt fall ska våra förslag bl.a. stärka samhällets säkerhet och underlätta för så många som möjligt att kunna få tillgång till en e-legitimation. Som tidigare anförts ser vi att en viktig del i att uppnå detta syfte är att skapa förutsättningar för att det ska finnas fler e-legitimationer på marknaden som även kan användas i den offentliga sektorns digitala tjänster. Mot denna bakgrund ser vi det som en nödvändighet att krav på användning omfattar statliga myndigheter, kommuner och regioner samt sammanslutningar av dessa aktörer. Detta kommer att få konsekvenser för den kommunala självstyrelsen (se mer om detta i avsnitt 9.7.3).

En grupp som inte omfattats av tidigare förslag är privata utförare inom offentligfinansierad verksamhet. Detta är något som även kritiserats i vissa remissvar. Stora delar av den kommunala verksamheten utförs i privat regi. De aktörer som verkar inom skolområdet, hälso- och sjukvårdsområdet samt socialtjänstområdet är till stor del privata. Om dessa aktörer inte omfattas av kravet skulle således ett digitalt utanförskap kunna kvarstå i relation till central digital offentlig service för personer som i dag inte har en e-legitimation som kan användas för att identifiera sig i dessa utförares tjänster. Samma krav bör därför även ställas på dessa aktörer.

Vad avser frågan om vilka privata utförare som ska omfattas gör vi följande överväganden. Genom lagen (2018:1937) om tillgänglighet till digital offentlig service uppställs krav om tillgänglighetsanpassning av webbplatser och mobila applikationer (DOS-lagen). I lagens förarbeten bedömde regeringen att tillämpningsområdet, i relation till det EU-direktiv lagen genomför i svensk rätt, skulle utvidgas till att även omfatta privata aktörer som yrkesmässigt bedriver verksamhet inom

[212] *Auktorisationssystem för elektronisk identifiering och för digital post*, s. 42 f.
[213] Myndigheten för digital förvaltning, *Utveckling av det svenska e-legitimationssystemet (*dnr-2021–2493), s. 35.

särskilt utpekade områden och som till någon del är offentligt finansierad.[214] Med offentlig finansiering avses ett direkt stöd eller betalning från det allmänna för att driva verksamheten.[215] Ett utpekat område är verksamhet som bedrivs av en enskild huvudman inom skolväsendet eller en enskild huvudman för en sådan internationell skola som avses i 24 kap. skollagen (2010:800). Även verksamhet som utgör hälso- och sjukvård enligt hälso- och sjukvårdslagen (2017:30) eller tandvård enligt tandvårdslagen (1985:125) pekas ut. Detsamma gäller verksamhet som bedrivs enligt socialtjänstlagen (2001:453), lagen (1988:870) om vård av missbrukare i vissa fall, lagen (1990:52) med särskilda bestämmelser om vård av unga, lagen (1993:387) om stöd och service till vissa funktionshindrade samt personlig assistans som utförs med assistansersättning enligt 51 kap. socialförsäkringsbalken.

I propositionen om auktorisationssystem för elektronisk identifiering och för digital post föreslås att samma krets privata utförare, samt offentlig styrda organ, ska få använda de tjänster som tillhandahålls inom auktorisationssystemen.[216]

Vi anser att samma tydligt definierade krets ska omfattas av kravet på att tillåta identifiering med utpekade e-legitimationer. Kravet ska dock inte gälla för offentligt styrda organ.

I remissvaren som ligger till grund för propositionen om auktorisationssystem lyftes bl.a. fram att det skulle kunna vara fördelaktigt om en ännu större krets aktörer skulle omfattas. Regeringen bedömde dock att en sådan utökning, som inte framstår som helt godtycklig eller oklar, svårligen låter sig göras i det sammanhanget och skulle riskera att medföra svåröverblickbara konsekvenser för marknaden, på liknande sätt som vid en utvidgning till aktörer som utför en uppgift av allmänt intresse.[217]

Även om det finns aktörer med verksamhet som nära anknyter till den offentligfinansierade verksamhet som omfattas, exempelvis apoteksverksamhet, bedömer vi att eventuella krav på privata aktörer utan offentlig finansiering ligger utanför ramen för vårt uppdrag. Betalningsutredningen har även lyft frågan om ytterligare e-legitimationer bör kunna användas i finansiella tjänster och vi anser att frågan om det inom hela eller delar av den privata sektorn bör ställas krav på att accep-

[214] Prop. 2017/18:299 s. 33.
[215] Prop. 2016/17:31 s. 28.
[216] Prop 2023/24:6 s. 31 ff.
[217] A.a. s. 33.

tera vissa e-legitimationer bör utredas vidare.[218] I anslutning till detta bör det även utredas om utfärdare av e-legitimationer som godkänts enligt Diggs tillitsramverk ska ges åtkomst till vissa uppgifter från myndighetsregister på samma sätt som exempelvis myndigheter och banker i dagsläget har. Detta omfattar bl.a. validering av ett körkort genom körkortsregistret och uppgifter om vårdnadshavare i elektronisk form från det statliga personadressregistret.

Vilka digitala tjänster ska omfattas av kravet?

När det gäller vilka tjänster som ska omfattas av kravet är utgångspunkten att en statlig e-legitimation utfärdas till en person för att användas i privatlivet. Utöver att det givetvis kommer vara möjligt att id-växla till en e-tjänstelegitimation delar vi den bedömning som Utredningen om betrodda tjänster gjort om att privata e-legitimationer enbart i undantagsfall bör användas i tjänsten.[219] Kravet bör således endast omfatta de digitala tjänster som används inom ramen för privatlivet. Detta utesluter även de digitala tjänster inom utbildningsområdet där identifiering uteslutande sker med särskilda e-legitimationer som utfärdas till elever eller studenter.

Kravet på att godta vissa e-legitimationer gäller endast om den aktuella e-legitimationen har samma tillitsnivå eller högre än den nivå som krävs för tillgång till den aktuella digitala tjänsten. Vad gäller tjänster där identifiering sker med exempelvis sms-verifiering eller lösenord så innebär kravet inte att dessa tjänster måste anpassas för att även kunna godta identifiering med en e-legitimation. Kravet gäller endast sådana digitala tjänster där identifiering sker med e-legitimation.

Med hänsyn till att begreppet nättjänst används i eIDAS-förordningen ska detta begrepp även användas i författningsförslaget i stället för begreppet digital tjänst.

[218] *Staten och betalningarna* (SOU 2023:16), s. 371 ff.
[219] *Användning av e-legitimation i tjänsten i den offentliga förvaltningen* (SOU 2021:62), s. 128 ff.

7.13.5 Hur ska regleringen utformas och var ska den placeras?

Utredningens förslag: Krav om att statliga myndigheter, kommuner, regioner och sammanslutningar av dessa aktörer samt vissa privata utförare av offentlig service ska tillåta autentisering med e-legitimationer som tillhandahålls av leverantör som är godkänd i enlighet med den föreslagna lagen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post ska föras in i den föreslagna lagen om elektronisk identifiering.

Statliga myndigheter, kommuner och regioner samt sammanslutningar av dessa aktörer som har behov av tjänster för elektronisk identifiering ska använda de tjänster som tillhandahålls genom föreslaget auktorisationssystem.

Myndigheten för digital förvaltning ska få rätt att meddela föreskrifter om vilken typ av tjänster som kravet avser och om hur skyldigheten ska fullgöras.

Skälen för utredningens förslag

När det gäller frågan om hur regleringen ska utformas finns det, som framgår av de tidigare förslag som redovisas i avsnitt 7.13.2, två huvudalternativ. Ett alternativ är att lagstifta om att vissa e-legitimationer ska godtas och det andra att införa krav om obligatorisk anslutning av offentliga aktörer till valfrihetssystem eller föreslaget auktorisationssystem. Båda alternativ når samma resultat fast på olika sätt. Det går att uttrycka det i form av att det tidigare alternativet är en mer direkt lösning med ett riktat krav medan det senare är en indirekt lösning.

Med beaktande av de e-legitimationer och offentliga aktörer vi föreslår ska omfattas av kravet ser vi ett behov av att använda oss av båda lösningarna.

Till att börja med ser vi ett behov av att det i lag finns ett övergripande krav om att de aktörer som anges i avsnitt 7.13.4 ska godta identifiering med de e-legitimationer som kravet omfattar. Detta då privata utförare inte omfattas av det upphandlingsrättsliga regelverket och att det vare sig kan anses önskvärt eller lämpligt att tvångsansluta privata aktörer till ett auktorisationssystem.

Vi delar dock dåvarande E-legitimationsnämndens uppfattning om att det av upphandlingsrättsliga skäl finns andra problem med lagstift-

ningslösningen (se avsnitt 7.13.2). Därtill kräver den lösningen att det skapas en ny struktur för ersättning m.m. för offentliga aktörer. Att en sådan struktur existerar får anses vara en förutsättning för att kunna uppställa författningskrav om att godta identifiering med vissa e-legitimationer. Avsaknaden av en sådan struktur kan annars i teorin leda till att en offentlig aktör kan bli skyldig att godta identifiering med en viss e-legitimation utan hänsyn till den ersättning som utfärdaren begär.

Valfrihetssystem och auktorisationssystem innefattar redan en sådan struktur och därtill föreligger inga upphandlingsrättsliga problem med en sådan lösning. Från ett konkurrensrättsligt perspektiv är även denna lösning att föredra då alla e-legitimationsutfärdare som är en del av systemet får samma ersättning när e-legitimationen används i anslutna myndigheters digitala tjänster. Regeringen har även i propositionen om auktorisationssystem betonat vikten av förvaltningsgemensamma digitala lösningar och en ökad standardisering.[220] Detta talar också för att kravet bör vara sammankopplat med auktorisationssystem för elektronisk identifiering. Vi anser därmed sammanfattningsvis att den statliga e-legitimationen bör anmälas till föreslaget auktorisationssystem och att det ska införas krav om att använda de tjänster för elektronisk identifiering som tillhandahålls genom auktorisationssystemen.

Vad gäller frågan om i vilken lag som det övergripande kravet ska placeras så saknas med undantag för lagen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering en befintlig lag som rör e-legitimationer. Det kan inte anses lämpligt att placera bestämmelsen i denna lag då bestämmelsen saknar direkt koppling till eIDAS-förordningen. Vad gäller andra författningar har vi bara identifierat en lag som potentiellt skulle kunna innehålla det nu aktuella kravet och det är den ovan nämnda DOS-lagen. DOS-lagen genomför Europaparlamentets och rådets direktiv (EU) 2016/2102 av den 26 oktober 2016 om tillgänglighet avseende offentliga myndigheters webbplatser och mobila applikationer i svensk rätt. Direktivet är ett minimidirektiv och medlemsstater kan således uppställa andra krav än som framgår av direktivet så länge som kraven inte underskrider de minimikrav som direktivet och dess genomförandeförordningar anger. Vid införandet valde Sverige att införa vissa bestämmelser som går utöver direktivet, bl.a. att de krav som uppställs även omfattar vissa privata utförare inom offentlig sektor. Eftersom kravet på att godta vissa e-legitimationer till stor del grundas i ett behov av att skapa en

[220] Prop. 2023/24:6 s. 16.

ökad tillgänglighet vore det i linje med författningens syfte om kravet framgick av denna lag. DOS-lagen är dock, till följd av det underliggande direktivets invecklade struktur, redan i dagsläget en tämligen svårtillgänglig lag. De aktörer som omfattas av DOS-lagens bestämmelser överensstämmer inte heller till fullo med den krets vi föreslår då den också omfattar offentligt styrda organ. Att introducera nya bestämmelser som delvis avviker från DOS-lagens systematik hade enligt vår bedömning kunnat leda till att lagen blev än mer svårtillgänglig. Mot denna bakgrund anser vi att den lämpligaste placeringen för lagbestämmelsen blir i den i avsnitt 7.1 föreslagna lagen om elektronisk identifiering.

När det gäller krav på anslutning till auktorisationssystem ska kravet framgå av förslag till lag om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post.

Som noterats i promemorian om auktorisationssystem för elektronisk identifiering och för digital post har Digg tagit fram flera olika valfrihetssystem i fråga om tjänster för elektronisk identifiering. Skälet till detta är att det har varit svårt att få gehör för delar av den kravställning som myndigheten har tagit fram, främst i fråga om det tekniska gränssnitt som ska gälla för anslutande leverantörer. De olika valfrihetssystemen syftar alltså delvis till att lösa olika behov, t.ex. för tillfälliga övergångslösningar och önskemål från särskilt viktiga leverantörer inom området. Valfrihetssystemen har varit delvis överlappande och anslutning till flera valfrihetssystem har varit nödvändig för den anslutande myndighet som har velat kunna ta emot samtliga erbjudna e-legitimationslösningar i sina digitala tjänster. Det kan även framöver uppstå behov av att inrätta parallella eller delvis överlappande auktorisationssystem. Exempelvis kan det inrättas auktorisationssystem som tar sikte på olika tillitsnivåer eller på olika tekniska lösningar som inte lämpar sig för att hanteras samlat inom ett och samma auktorisationssystem. Mot denna bakgrund föreslogs i promemorian att det bör finnas en möjlighet för Digg att meddela föreskrifter om dels vilka tjänster för elektronisk identifiering inom auktorisationssystemen som kravet på användning avser, dels hur skyldigheten att använda tjänsterna ska fullgöras. Berörda aktörer kan på det sättet ges närmare anvisning om hur kravet ska tillgodoses med hänsyn till myndigheternas olika förutsättningar. Av samma skäl som anges i

promemorian anser vi att Digg ska få rätt att meddela föreskrifter om vilka tjänster som kravet avser och om hur skyldigheten ska fullgöras.[221]

7.13.6 Undantag från kraven

Utredningens förslag: Regeringen eller den myndighet regeringen bestämmer ska få meddela undantag från kraven.

Skälen för utredningens förslag

Vid uppställande om krav på erkännande av vissa e-legitimationer och anslutning till auktorisationssystem bör det även övervägas om undantag från kraven bör meddelas. Utredningen om effektiv styrning av nationella digitala tjänster bedömde att det behövde finnas en möjlighet att undantas från skyldigheten att ansluta sig till valfrihetssystem. Ett sådant undantag kunde enligt utredningen beviljas om det fanns särskilda skäl. Utredningen bedömde att sådana särskilda skäl kan vara att den offentliga aktören är bunden av befintliga avtalsvillkor som gör att den inte kan ansluta sig till valfrihetssystem eller att den måste genomföra omfattande tekniska anpassningar av sina egna system innan den kan följa de villkor som gäller inom valfrihetssystem.[222]

I promemorian om auktorisationssystem för elektronisk identifiering och för digital post gjordes liknande överväganden. I promemorian anfördes följande.

> För att kunna uppnå syftet och så snabbt som möjligt kunna realisera nyttorna med en samlad anskaffning av tjänsterna bör kravet gälla generellt från ikraftträdandet av regleringen och inte bara vid nyanskaffning av tjänster. Det ger också större möjligheter till kontroll och uppföljning av reformen. Eftersom de statliga myndigheterna har anskaffat tjänster för elektronisk identifiering på olika sätt, finns det stora skillnader i löpande avtalstider. Flera statliga myndigheter kommer att vara bundna av avtal som löper längre än det tilltänkta ikraftträdandedatumet för förordningen. Det går inte heller att utesluta att myndigheter kan komma att teckna avtal utanför existerande valfrihetssystem fram till dess. För att myndigheter inte ska hamna i en situation där tidigare ingångna avtal löper parallellt med kravet på användning av tjänster för elektronisk identifiering inom auktorisationssystemen bör det finnas en möjlighet att

[221] *Promemoria om auktorisationssystem för elektronisk identifiering och för digital post*, s. 44 f.
[222] *reboot – omstart för den digitala förvaltningen* (SOU 2017:114), s. 235.

> bevilja tidsbegränsade undantag från kravet. Till skillnad från vad utredningen föreslår bör Myndigheten för digital förvaltning få besluta om sådana undantag. Som Lantmäteriet anför bör undantag enbart beviljas för så lång tid som det krävs för att myndigheten i fråga ska kunna avsluta befintliga avtal och på ett ordnat sätt ansluta sig till auktorisationssystem. Undantag bör beviljas med stor restriktivitet. Ett exempel på en situation där undantag bör kunna beviljas är när avtalsrättsliga förpliktelser gentemot tredje part förhindrar en övergång till auktorisationssystem och ett upphörande i förtid skulle leda till orimliga konsekvenser för myndigheten i fråga. Det faktum att en enskild myndighet inte är nöjd med de tjänster som erbjuds inom inrättade auktorisationssystem bör inte vara grund för undantag. Förutom i direkt anslutning till ikraftträdandet bör undantag inte förekomma annat än i undantagsfall. Det skulle kunna vara fallet om de godkända leverantörerna i auktorisationssystemet enbart representerar en begränsad krets av användare, t.ex. om de största leverantörerna inte ansluter sig. Myndigheten för digital förvaltning kan då komma att behöva meddela ett generellt undantag som gäller för samtliga myndigheter. På så sätt kan det undvikas att det uppstår en situation där statliga myndigheter blir skyldiga att använda tjänster i auktorisationssystem som inte innefattar de största leverantörerna.[223]

Vi ansluter oss till de skäl för undantag som anfördes i promemorian. Vi ser därtill anledning att det med hänsyn till rikets säkerhet även kan behöva tas hänsyn till vissa myndigheters verksamhet och föreslår därmed att regeringen eller den myndighet regeringen bestämmer ska bemyndigas att meddela föreskrifter om undantag från kravet om att statliga myndigheter, kommuner, regioner och sammanslutningar av dessa aktörer samt vissa privata utförare av offentlig service att godta identifiering med de e-legitimationer som förslaget omfattar. Möjligheten till undantag bör föras in i både den föreslagna lagen om elektronisk identifiering och den föreslagna lagen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post.

I tidigare remissvar har framförts att myndigheter ska kunna fatta beslut om att undanta sig själva om de bedömer att tillräcklig säkerhet inte kan garanteras. Vi ser ingen anledning till att införa någon sådan möjlighet. De e-legitimationer som omfattas av kravet är godkända enligt Diggs tillitsramverk och en löpande uppföljning rörande efterlevnaden av ramverkets krav utförs även av myndigheten. För det fall en e-legitimation som omfattas av kravet har brister som utgör en risk för berörda myndigheter har Digg möjlighet att agera för att hantera en sådan situation. Regeringen har även i propositionen om auktorisa-

[223] *Promemoria om auktorisationssystem för elektronisk identifiering och för digital post*, s. 44.

tionssystem betonat att det är angeläget att de auktorisationssystem som inrättas tillgodoser de behov som de offentliga aktörerna har av tjänsterna och att risker beträffande säkerheten minimeras vad gäller skydd för personuppgifter, informationssäkerhet och säkerhetsskydd. Regeringen framförde även att Digg ska samråda med andra relevanta expertmyndigheter i samband med att krav och villkor utformas.[224]

[224] Prop. 2023/24:6 s. 24.

8 Ikraftträdande- och övergångsbestämmelser

Utredningens förslag: Författningsförslagen ska träda i kraft den 1 mars 2026.

Utredningens bedömning: Det saknas anledning att införa några särskilda övergångsbestämmelser.

Skälen för utredningens bedömning och förslag

Det är angeläget att Sverige kan anmäla en e-legitimation på tillitsnivå hög enligt eIDAS-förordningen inom föreskriven tid (se avsnitt 6.2). Enligt det kompromissförslag som antogs av rådet i slutet av 2022 ska en genomförandeperiod om 24 månader räknas från det att vissa genomförandeakter enligt den reviderade förordningen har antagits.[1] Dessa genomförandeakter ska i sin tur antas senast sex månader efter antagandet av den reviderade eIDAS-förordningen. Om dessa tidsramar inte förändras under återstoden av förhandlingarna får den totala tidsåtgången uppgå till högst 30 månader.

En statlig e-legitimation är efterfrågad. Vid sidan av ovan redovisade formella krav är det utifrån i kapitel 6 angivna skäl angeläget att en statlig e-legitimation kan tillhandahållas så snart som möjligt. Detta motiveras bl.a. av behovet av att staten tillgodoser sitt ansvar för att utfärda en e-legitimation till grupper i samhället som i dagsläget saknar förutsättningar att få någon av de befintliga.

Myndigheten för digital förvaltning har anfört att, givet nödvändiga beslut fattats om författningsreglering, finansiering och annan myn-

[1] Ständiga representanternas kommitté (Coreper I), den 25 november 2022, 14959/22, Förslag till Europaparlamentets och rådets förordning om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av en ram för europeisk digital identitet – Allmän riktlinje.

dighetsstyrning, utvecklingstiden för en statlig e-legitimation är minst 24 månader.

Vi gör bedömningen att förslagen till ny reglering kan träda i kraft tidigast den 1 mars 2026. Det saknas anledning att införa några särskilda övergångsbestämmelser.

Med beaktande av den tekniska anpassning som aktörer kan behöva genomföra med anledning av den föreslagna regleringen om krav på att godta vissa e-legitimationer anser vi att även dessa bestämmelser bör träda i kraft den 1 mars 2026. Inte heller för detta förslag föreligger skäl att införa några särskilda övergångsbestämmelser.

9 Konsekvenser

9.1 Inledning

I delbetänkandet redovisas våra förslag kopplade till hur en kostnadseffektiv statlig e-legitimation på högsta tillitsnivå enligt eIDAS-förordningen kan utformas och tillhandahållas av en statlig myndighet. Att en sådan e-legitimation ska utfärdas på den högsta tillitsnivån och att den ska utfärdas av Myndigheten för digital förvaltning (Digg) följer redan av våra utredningsdirektiv.

I detta avsnitt redogör vi för förslagens effekter i den omfattning som bedömts lämpligt och med beaktande av relevanta delar av kommittéförordningen (1998:1474) och förordningen (2007:1244) om konsekvensutredning vid regelgivning. För den integritetsanalys som vi enligt våra direktiv ska göra och de konsekvenser som förslagen bedöms få för den personliga integriteten hänvisas till avsnitt 7.11. I enlighet med direktiven har vi också analyserat risker för informationssäkerheten och risker med identitetsrelaterad brottslighet. Våra bedömningar i dessa delar finns i avsnitten 6.5, 7.2.6 och 7.4.4 respektive 6.7 och 9.10.

9.2 Bakgrund till och syfte med förslagen

I kapitel 6 redogör vi för problem- och behovsbilden bakom våra förslag. Som redovisas där finns det i dagsläget inte någon svensk e-legitimation för privatpersoner som tillhandahålls på tillitsnivå hög enligt eIDAS-förordningen och som är anmäld för gränsöverskridande användning enligt förordningens föreskrivna förfarande.[1]

[1] Genom Försäkringskassans tjänst E-identitet för offentlig sektor (Efos) tillhandahålls e-legitimationer. Efos är visserligen anmäld för gränsöverskridande användning på nivå hög enligt eIDAS-förordningen, men det är fråga om en e-tjänstelegitimation (se avsnitt 3.6, jämför e-legitimation för privat bruk, avsnitt 3.5). Efos möjliggör att anslutna organisationer kan autentisera, kryptera och signera så väl inom som mellan organisationer.

Av de befintliga e-legitimationer som utfärdas av kommersiella aktörer har BankID och Freja+ genomgått EU:s sakkunnighetsbedömning inom ramen för eIDAS-förordningen (en. peer review). Av dessa två har Freja+ även genomgått en formell anmälan till EU och kan därmed användas för gränsöverskridande användning på nivå väsentlig enligt eIDAS-förordningen.[2] Den e-legitimation som AB Svenska Pass tillhandahåller på Skatteverkets identitetskort för folkbokförda är godkänd enligt det svenska tillitsramverket på nivå 4, men är inte föranmäld för gränsöverskridande användning.

Det finns i dagsläget inga indikationer på att någon e-legitimation på nivå hög enligt eIDAS-förordningen som även anmäls för gränsöverskridande användning kommer att erbjudas inom överskådlig tid av privata aktörer. Som konstateras i våra direktiv har staten begränsade möjligheter till insyn och påverkan på sådana aktörer.

Sverige måste uppfylla det krav som förväntas följa av den reviderade eIDAS-förordningen om att varje medlemsstat ska anmäla en e-legitimation på den högsta tillitsnivån (se vidare avsnitt 9.3). Det kan för övrigt konstateras att Sverige är en av få medlemsstater som helt saknar en statlig e-legitimation.

Avsaknaden av en anmäld svensk e-legitimation för privat bruk på tillitsnivå hög enligt eIDAS-förordningen innebär också att svenskar kan utestängas från vissa digitala tjänster i andra medlemsstater, om de inte har tillgång till en e-legitimation på tillitsnivå hög från något annat land.

Ytterligare problem med den nuvarande situationen är att det för vissa grupper i Sverige är svårt eller uteslutet att få tillgång till befintliga e-legitimationer. Något förenklat kan sägas att det är äldre personer, personer med funktionsvariationer och personer utan svenskt personnummer som inte har tillgång till en e-legitimation i samma utsträckning som den övriga befolkningen. Omfattningen framgår av avsnitt 6.6.2. Detta medför att de inte kan identifiera sig digitalt och inte heller nyttja samhällets digitala tjänster för att ta till vara sina intressen och medborgerliga rättigheter. Det gäller även för personer som bara tillfälligt vistas i Sverige, exempelvis för högre studier eller arbete.

En översikt över e-legitimationsmarknaden i Sverige redovisas i kapitel 4. Att det finns få aktörer, varav en klart marknadsledande, innebär inte bara en risk ur ett konkurrensperspektiv; marknadssituationen får konsekvenser också vad gäller säkerhet och redundans. E-legitima-

[2] Europeiska unionens officiella tidning, 18/2/2022 L 257/73.

tioner utgör en viktig infrastruktur som behöver fungera också om samhället utsätts för en stor påfrestning och ytterst även i krig. Störningar i e-legitimationssystem kan snabbt få kännbara effekter för näringsliv, banker, offentlig sektor och inte minst för enskilda även under i övrigt normala förhållanden.

Vårt förslag om att en statlig myndighet ska utfärda en e-legitimation avser att utgöra ett komplement till befintliga alternativ och att därmed stärka samhällets säkerhet och robusthet. En statlig e-legitimation på den högsta tillitsnivån möjliggör dessutom id-växling till e-legitimationer på samma eller lägre tillitsnivå, vilket kan bidra till att nya, kommersiella aktörer etablerar sig på marknaden (se avsnitt 9.8). Med fler e-legitimationer finns förutsättningar för bättre redundans om en typ av e-legitimation av någon anledning inte fungerar under kortare eller längre tid.

Ytterligare önskvärda effekter med den föreslagna e-legitimationen, och som även lyfts fram i våra direktiv, är att den ska bidra till att dels motverka bedrägerier som begås med hjälp av e-legitimationer, dels öka tillgängligheten till en säker e-legitimation och således minska det digitala utanförskapet. Under arbetets gång har det blivit allt tydligare att dessa mål i vissa avseenden är svåra att förena med varandra om man eftersträvar maximal uppfyllelse av båda. Sådana intentioner torde inte heller kunna åstadkommas fullt ut inom ramen för vårt uppdrag. En e-legitimation omgärdad av så höga säkerhetsanordningar att bedrägeribrottslighet förhindras skulle sannolikt bli svåranvänd för många och innebära omotiverade integritetsintrång. Därtill kommer att utformningen av e-legitimationen i sig inte helt kan undanröja de risker som finns vid användningen av den. Förslaget omfattar därför möjlighet för den utfärdande myndigheten att meddela vissa föreskrifter om villkor för hur e-legitimationen får användas.

Vi bedömer att våra förslag kan bidra till att uppnå angiva syften men att ytterligare åtgärder kommer att vara nödvändiga (se t.ex. avsnitt 9.9). Eftersom den ökade digitaliseringen gör det allt svårare att klara sig i samhället utan tillgång till en e-legitimation har den främsta utgångspunkten för förslagen varit att så många som möjligt ska kunna skaffa en säker e-legitimation.

9.3 Nollalternativ

En beskrivning av nollalternativ innefattar en bedömning av vad som händer om de föreslagna åtgärderna inte genomförs.

Nollalternativ utifrån vårt uppdrag innebär att det inte tas fram en statlig e-legitimation. Det utesluter i och för sig inte att en e-legitimation på tillitsnivå hög tas fram på annat sätt, t.ex. av andra aktörer, och anmäls enligt reglerna i eIDAS-förordningen.

Den e-legitimation som finns på Skatteverkets identitetskort för folkbokförda i Sverige utfärdas inte av myndigheten utan av AB Svenska Pass. E-legitimationen är, som framgått, godkänd för nivå 4 enligt det svenska tillitsramverket, men den är inte anmäld för gränsöverskridande användning. För BankID och Freja+ är tillitsnivån inte hög utan väsentlig. Som anförts har staten begränsad påverkan på de kommersiella aktörer som utfärdar befintliga svenska e-legitimationer. Med beaktande av de föreslagna kraven enligt den reviderade eIDAS-förordningen, och tidsramarna för att uppfylla dessa (se avsnitt 4.2.7), är det inte ett alternativ att invänta att befintliga utfärdare eller någon ny aktör eventuellt agerar i frågan. Om en statlig e-legitimation på den högsta tillitsnivån inte blir verklighet och anmäls, alternativt försenas, riskerar Sverige att ett överträdelseförfarande inleds vilket kan leda till vite.

Användningen av digitala tjänster och e-legitimationer ökar i samhället vilket innebär att utanförskapet för den som saknar en e-legitimation riskerar att bli alltmer påtagligt. Utan en statlig e-legitimation kan de problem som tillgång till en e-legitimation avser att omhänderta, inte minst tillgänglighetsproblematiken, riskera att kvarstå eller öka.

Att samhällets beroende av e-legitimationer växer i takt med digitaliseringen medför också ett ökat beroende av befintliga e-legitimationsutfärdare. Samhällets sårbarhet vid säkerhetsincidenter riskerar som en konsekvens därav att bli än större. Utan möjligheten att använda en statlig e-legitimation som grund för id-växling kan ifrågavarande beroende bestå eftersom förutsättningarna för nya, kommersiella aktörer att kunna etablera sig på den svenska marknaden, begränsas.

9.4 Vilka berörs av förslagen?

Vårt förslag om en statlig e-legitimation medför konsekvenser primärt för de ansvariga myndigheterna; den utfärdande och den identitetskontrollerande. I avsnitten 9.5 respektive 9.6 beskrivs dessa konsekvenser närmare. I viss utsträckning kommer även allmänna förvaltningsdomstolar att beröras genom att beslut om statlig e-legitimation får överklagas dit (se avsnitt 9.7.2).

Vidare berörs sådana offentliga aktörer som omfattas av det föreslagna kravet på att i sina digitala tjänster godta identifiering med vissa e-legitimationer (se avsnitten 9.7.3 och 9.8.1). Med offentliga aktörer avses i detta sammanhang statliga myndigheter, kommuner och regioner samt även vissa privata utförare som yrkesmässigt bedriver offentligfinansierad verksamhet inom skolområdet, hälso- och sjukvårdsområdet samt socialtjänstområdet (se avsnitt 7.13.4). Förslaget kommer även att påverka vissa företag som i dagsläget erbjuder integrationstjänster inom området elektronisk identifiering (se avsnitt 9.8.1). Vi gör också bedömningen att det kommer att finnas intresse av att använda den statliga e-legitimationen för id-växling, vilket kan gynna konkurrenssituationen på marknaden för e-legitimationer och skapa förutsättningar för befintliga företag att växa eller nya att etablera sig (se avsnitt 9.8.2).

Slutligen kan förslaget potentiellt påverka alla, i eller utanför landet, som har ett svenskt personnummer alternativt ett samordningsnummer för personer med styrkt identitet, från och med det kalenderår de fyller nio år. Vi bedömer dock att det initialt kommer att vara främst den senare kategorin som ansöker om att tillhandahållas den statliga e-legitimationen. Med anledning av förväntad reglering av den digitala identitetsplånboken för gränsöverskridande identifiering inom EU torde på sikt även personer som i dagsläget redan har tillgång till befintliga e-legitimationer i större utsträckning vilja anskaffa den statliga e-legitimationen och således beröras av förslagen (se vidare avsnitt 9.9).

9.5 Förslaget om ansvar för utfärdande av en statlig e-legitimation

Vi har anslutit oss till Diggs förslag om ansöknings- och utgivningsprocess. Förslaget innebär att den statliga e-legitimationen tillhandahålls genom att Digg bifaller en ansökan, som ska göras hos en identitetskontrollerande myndighet vilken också lämnar ut e-legitimationen till sökanden. E-legitimationen ska aktiveras, på plats vid utgivningsstället via en självservicetjänst eller inom viss tid därefter av innehavaren via Diggs webbplats eller av myndigheten tillhandahållen mobilapplikation (se avsnitt 7.4.2). Supportbehov bedöms föreligga vid ansökan och, i förekommande fall, aktiveringen, såväl som vid användning av e-legitimationen. Det ankommer på den identitetskontrollerande myndigheten att tillgodose tillgänglighetsbehov och tillhandahålla nödvändig service åt enskilda i samband med ansökan. För erforderlig användarsupport ansvarar Digg.

Digg har gjort följande huvudsakliga bedömning av de kostnader som beräknas uppstå för myndigheten i egenskap av utfärdare av den statliga e-legitimationen:

> Digg bedömer att de sammantagna utvecklings- och uppbyggnadskostnaderna för Digg uppgår till cirka 80–100 miljoner kronor (mnkr). Dessa fördelar sig på kostnader för utveckling av system och programvara om cirka 50–70 mnkr och uppbyggnad av verksamheten vid Digg om cirka 30 mnkr. Digg bedömer vidare att de årliga kostnaderna för verksamheten vid Digg uppgår till 63–71 mnkr. Dessa fördelar sig på kostnader för förvaltning om cirka 8–11 mnkr, kostnader för drift cirka 30 mnkr och Diggs kostnader för utgivningsprocessen till 25–30 mnkr. Baserat på utgivningsvolymerna kommer det över tid vara nödvändigt att se över beräkningarna. […] Kostnadsanalysen bygger på uppskattningar av resursåtgång för respektive kostnadskategori. Försäkringskassan och Polismyndigheten har bistått Digg i att få en bild av uppskattade kostnader för drift och förvaltning samt för utgivningsprocessen.[3]

Digg har angett att beräkningarna endast är en grundnivå för hanteringen och att nivån kommer att ändras vid större förändringar av volymerna av utgivna e-legitimationer.

[3] Myndigheten för digital förvaltning, *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, s. 81.

Tabell 9.1 Av Digg uppskattade totala årliga kostnader exklusive uppstart och utvecklingskostnader

Miljoner kronor

	År 1	År 2	År 3
Totalkostnader	**63–71**	**63–71**	**63–71**[4]

Källa: Myndigheten för digital förvaltning, Digg.

Vi instämmer i allt väsentligt i Diggs kostnadsbedömningar. Våra förslag skiljer sig emellertid i vissa avseenden från förslagen i Diggs rapport, vilket medför tillkommande kostnader om totalt 52,7–56,7 mnkr för första året, 41,1–45,1 mnkr för andra året och 42,2–46,2 mnkr för tredje året. Vår bedömning är att våra förslag om lagring av fingeravtryck och ansiktsbild (se avsnitt 7.2.6) inte påverkar Diggs utvecklings- och uppbyggnadskostnader. De tillkommande kostnaderna är hänförliga till våra egna bedömningar och förslag enligt redogörelsen nedan.

Säker och feltolerant drift

Säkra och feltoleranta system och register behöver vara tillgängliga för att den statliga e-legitimationen ska kunna utfärdas och användas.

Vi har inte kunnat inhämta säkerställda uppgifter om kostnader för säker IT-drift. Till utredningen av myndighetsrepresentanter lämnad information motiverar dock bedömningen att kostnaden kan förväntas motsvara 16 mnkr per år.

Säkert nät mellan Digg och den identitetskontrollerande myndigheten

Det är nödvändigt att kommunikationen mellan myndigheterna är säker, bl.a. för att statlig e-legitimation ska kunna utfärdas och att Diggs register ska kunna uppdateras.

Kostnaden uppskattas till 3 mnkr första året och därefter 2,5 mnkr per år samt baseras på användning av dels SGSI (Swedish Government

[4] Digg har uppskattat kostnaderna på två år. Vi har antagit att kostnaden år 3 är densamma som år 2. En osäkerhetsfaktor i detta är att ökade volymer användning kan ställa ökande krav på supportkostnader.

Secure Intranet)[5], dels kommersiella datatjänster för redundans och diversitet samt ökad feltolerans.

Ytterligare kostnader för bäraren av den statliga e-legitimationen

Våra tillkommande förslag om att bäraren ska möjliggöra innehåll av biometriska data och kunna vara en anordning för att skapa kvalificerade elektroniska underskrifter innebär merkostnader. Därutöver kan krav på leveranskedjan medföra färre möjliga leverantörer av bärare, vilket kan vara kostnadsdrivande.

Digg har bedömt styckkostnaden för kortämnen till tjugotalet kronor, men denna kostnadspost saknas i Diggs sammanställning. Vi bedömer att merkostnaderna uppgår till 100 kronor per kortämne. Sammantaget medför det en totalkostnad på 130 kronor per kortämne.

Säkerhetsgranskning och penetrationstester

Vi bedömer att säkerhetsgranskning om 600 timmar och penetrationstest om 600 timmar behöver utföras vartannat år och att uppföljning av de båda kräver 300 timmar vartannat år.

Kostnaderna beräknas på ett timpris om 1 750 kronor/timme, enligt tidigare ramavtal och uppräknat för inflation.

Informationsinsatser

I samband med lansering och därefter årligen om än i mindre omfattning behövs insatser för att informera om den statliga e-legitimationen och om t.ex. säkert handhavande.

Vi uppskattar kostnaden till 15 mnkr första året och därefter 5 mnkr årligen.

[5] SGSI (Swedish Government Secure Intranet) är ett intranät, skiljt från internet, för säker och krypterad kommunikation mellan användare i Sverige och i Europa som tillhandahålls av Myndigheten för samhällsskydd och beredskap (MSB).

Ytterligare behov av support

Kostnaderna för support är särskilt svårbedömda eftersom de är helt avhängiga av hur många personer med särskilda behov som kommer att skaffa en statlig e-legitimation. De personer som i dag saknar en e-legitimation kan emellertid – till följd av bristande datorvana, kognitiva svårigheter, språkbarriärer, begränsad kunskap om olika samhällsfunktioner eller på grund av fysiska funktionsnedsättningar – förväntas ha ett förhållandevis stort behov av support. Enligt uppgift från Finansiell ID-Teknik BID AB (Finansiell ID-Teknik), ägare och förvaltare av BankID, besvarade BankID:s supporttjänst i mars 2023 omkring 20 000 samtal med en genomsnittlig samtalstid om cirka fem minuter. Bolaget uppskattar att så många som 90 procent av samtalen kommer från de 10 procent av användarna som har minst datorvana.

BankID har totalt sett ett långt större antal innehavare än vad den statliga e-legitimationen initialt förväntas få. Statistiken från Finansiell ID-Teknik om tillhandahållen support, som dessutom avser endast en viss månad, kan därför inte tas till intäkt för supportbehovet för den statliga e-legitimationen. Vi kan dock konstatera att flertalet innehavare av den statliga e-legitimationen sannolikt kommer att ha ett motsvarande supportbehov som de tio procent av BankID-innehavarna som har minst datorvana. Behovet av support kan mot den bakgrunden förväntas uppgå till liknande nivåer och kräva anpassningar för att uppfylla de tillgänglighetskrav som ställs på myndigheter.

Vi bedömer att supportbehovet kommer att kvarstå under hela tiden som en e-legitimation kan användas. Support behöver därför finnas tillgänglig på fysiska besöksplatser och på distans, samt innehålla funktioner som säkerställer användbarhet för personer med funktionsnedsättningar. Beroende på hur den utfärdande myndigheten väljer att organisera support på fysiska besöksplatser kan samordningsvinster uppnås, exempelvis om lokaler och personal på befintliga offentliga serviceställen kan användas. Den ökade volymen till dessa platser kommer givetvis oavsett att innebära en merkostnad.

Digg har uppskattat kostnader för stöd till användare (kundservice, administration, första linjens support, hantering av frågor från allmänheten, informationsmaterial och webb) till 9 mnkr och andra linjens support (ärenden från användare, förlitande parter och identitetskontrollerande myndighet som skickas vidare från första linjen) till 4,5–6 mnkr.[6]

[6] A.a. s. 86.

I samband med utredningens öppna möten om Diggs rapport som anordnades under våren 2023 var det intressenter som angav att Digg underskattat kostnaden för support. Med tanke på detta och BankID:s kostnader gör vi bedömningen att kostnaden för support är någonstans i spannet 9–14 mnkr. Digg uppskattar kostnaden till 9 mnkr per år det gör att den uppskattade merkostnaden utifrån vår bedömning är 1–5 mnkr per år.

Tabell 9.2 Av utredningen uppskattade tillkommande kostnader för Digg

Miljoner kronor

	År 1	År 2	År 3
Redundanta och feltoleranta drifttjänster	16	16	16
Bärare: (i) kortämnen, (ii) biometriska uppgifter, (iii) kvalificerade elektroniska underskrifter	15,6	15,6	15,6
Säkert nät mellan Digg och grundidentifierande myndighet	3	2,5	2,5
Säkerhetsgranskning och penetrationstester	2,1	1	2,1
Information vid lansering och återkommande informationsinsatser	15	5	5
Supportkostnader	1–5	1–5	1–5
Summa kostnader	**52,7–56,7**	**41,1–45,1**	**42,2–46,2**

9.5.1 Finansiering för utfärdande

Digg har föreslagit att kostnader för utveckling av system och programvara samt uppbyggnad av verksamheten vid Digg ska finansieras genom ett tillfälligt förstärkt förvaltningsanslag under utvecklings- och uppbyggnadsfasen. Regeringen har i budgetpropositionen för 2024 föreslagit ett utökat anslag till Digg avseende statlig e-legitimation med 40 mnkr år 2024 och 40 mnkr år 2025.[7] De årliga kostnaderna ska enligt Digg finansieras genom en permanent höjning av samma anslagspost.[8] Vi delar Diggs bedömning om anslagsfinansiering av verksamheten.

[7] Prop. 2023/24:1 Utgiftsområde 22, s. 118.
[8] A.a. s. 89.

9.6 Förslaget om ansvar för grundidentifiering

9.6.1 Utgångspunkter

Utredningen har upphandlat konsultstöd för att inhämta och analysera kostnaderna för grundidentifieringen beroende på om, å ena sidan Polismyndigheten och, å andra sidan Skatteverket tillsammans med Statens Servicecenter, skulle ansvara för denna uppgift. Uppdraget har utförts av Governo AB (Governo) som har tagit fram antaganden och frågeställningar till berörda myndigheter.

Utöver att identifiera vilka kostnader som uppkommer vid utförandet av grundidentifieringen för respektive myndighet, omfattade Governos uppdrag en analys av vilka samhällsekonomiska kostnader och intäkter som kan förväntas beroende på valt alternativ.

Såväl Skatteverket som Polismyndigheten har framfört att det är svårt att göra efterfrågade kostnadsuppskattningar och att det därmed finns vissa osäkerhetsfaktorer i de svar som lämnats av myndigheterna.

Skatteverket har lämnat sina svar med utgångspunkt i den identitetskortsverksamhet som bedrivs av myndigheten. Polismyndigheten har påpekat att framtagna kostnader baserats på det tillställda underlaget, men att sådan information som krävs för att fånga samtliga kostnadsposter och att göra mer exakta uppskattningar saknats, varför av myndigheten redovisade uppskattningar ska tolkas med stor försiktighet.

Premisser för kostnadsberäkningarna

Kostnadsberäkningarna påverkas av flera olika faktorer, såsom ansökningsvolym, handläggningstid, behov av stöd vid ansökan och aktivering, samt antal platser på vilka det ska vara möjligt att ansöka om en statlig e-legitimation.

Det har inte varit möjligt att inhämta några säkerställda uppgifter i dessa avseenden. I avsaknad av sådana uppgifter har Governo angett följande premisser för myndigheternas uppgiftslämnande:[9]

– att ansökan och utfärdande av en statlig e-legitimation sker vid ett och samma tillfälle,

[9] För detaljerad beskrivning, se Governo AB, Rapport 2023-08-17 *Utfärdandet av en statlig e-legitimation Analys av ekonomiska konsekvenser,* (dnr I202204/2023/403A).

– att utfärdandet hanteras på ett eget nätverk med personal som har säkerhetsprövats i säkerhetsklass 3 enligt säkerhetsskyddslagen (2018:585),
– att ansökan och utfärdande av den statliga e-legitimationen görs av den sökande fysiskt på plats (personlig inställelse) efter tidsbokning,
– att det ska vara möjligt att ansöka om statlig e-legitimation i hela landet. Fasta kontor kan eventuellt kombineras med ambulerande tillfälliga möjligheter att söka på vissa geografiska platser,
– att den statliga e-legitimationen är förenad med en ansökningsavgift om 400 kronor,
– att kundservice och teknisk support för användning av e-legitimationen erbjuds av Digg,
– att en slussningsfunktion mellan den identitetskontrollerande myndigheten och Digg behövs gällande kundservice och teknisk support,
– att målgruppen är personer som är folkbokförda i Sverige, alternativt har tilldelats ett samordningsnummer för personer med styrkt identitet, och
– att den identitetskontrollerande myndigheten ansvarar för stöd i samband med ansökan och, i förekommande fall, aktivering av den statliga e-legitimationen i dess fysiska lokaler.

Utöver angivna förutsättningar har Polismyndigheten i sitt underlag gjort följande bedömningar och antaganden:

– att ansökan om statlig e-legitimation ryms i befintlig verksamhet och i de befintliga besöksflödena.
– att besökstiden för ansökan om statlig e-legitimation beräknas till 10 minuter[10], med reservation för att olika målgrupper kan ha olika behov som kräver olika handläggningstider. De uppskattade kostnaderna för support i samband med ansökan och aktivering är inkluderade i kostnadsuppskattningarna som lämnats. Utifrån de angivna ansökningsvolymerna och målgrupperna antas behovet av support vara lågt.

[10] Samtidigt lyfter myndigheten att tidsbokning för personer som för närvarande saknar e-legitimation behöver ske per telefon (via 114 14), vilket kommer att medföra en merkostnad.

– att utrustning som krävs för support tillhandahålls av Digg. Det framgår inte vad som krävs av Polismyndigheten för att tillhandahålla en självservicetjänst, varför detta inte har kunnat beräknas. Supporttjänsten, det vill säga hjälp vid besöket med ansökan och aktivering, antas kunna vara i drift vid ett införande av uppgiften om statlig e-legitimation.

9.6.2 Kostnadsberäkningar för grundidentifiering

Skatteverket och Polismyndigheten har i dag olika utbredd närvaro i samhället (se avsnitt 7.6.2) och antalet nya kontor som var och en av myndigheterna kan behöva etablera skiljer sig åt. För att kunna göra en jämförelse i kostnadshänseende mellan myndigheterna har vi utgått från premissen att ansökan och utgivning av den statliga e-legitimationen kan göras vid 50 kontor. Ansökningsvolymerna har uppskattats i två olika scenarier, alternativ 1 med minskande volymer och alternativ 2 med ökande volymer (se tabell 9.3 nedan). Det underlag som funnits tillgängligt för utredningen har inte medgett någon exakt bedömning av kostnaden för att etablera ett tillkommande kontor.

Tabell 9.3 Scenarier för volymer av ansökningar de första tre åren

	År 1	År 2	År 3
Alternativ 1	110 000	100 000	90 000
Alternativ 2	100 000	180 000	270 000

Polismyndighetens redovisade utgångspunkter för sina kostnadsuppskattningar

Polismyndigheten har redovisat i huvudsak följande utgångspunkter för sina kostnadsuppskattningar.

De ansökningsvolymer som angetts i de två alternativen är förhållandevis små i jämförelse med de volymer av ansökningar och besök som Polismyndigheten redan hanterar. Förväntade ansökningsvolymer kan därför förväntas rymmas inom ramen för polisens befintliga verksamhet.

Eftersom processen för statlig e-legitimation är snarlik den för pass och nationella identitetskort förutspås inte behov av några större verk-

samhetsanpassningar. Med hänsyn tagen till myndighetens redan höga geografiska tillgänglighet redovisas inga kostnader för att tillhandahålla statlig e-legitimation vid nytillkomna receptioner. Inte heller bedöms det finnas behov av ambulerande kontor för att säkra den geografiska tillgängligheten.

Oavsett alternativ bedöms uppstartskostnaden motsvara 24 mnkr. I kostnaden ingår lönekostnader för uppstarts- och införandeorganisation. De arbetsuppgifter som utförs bedöms vara motsvarande de som redan utförs för pass och nationellt identitetskort, varför inget omfattande arbete som ställer krav på en större införandeorganisation krävs. Vidare ingår utbildningskostnader för polisens nationella telefonväxel, kostnader för säkerhet och förvaring av kort, kostnader för kassasystem och utrustning, kostnader för tidsbokningssystem, kostnader för rekrytering av personal och kostnader för framtagande och genomförande av utbildning.

Driftskostnader har uppskattats per år i förhållande till ansökningsvolymer i angivna scenarier. Enligt myndigheten uppgår de sammanlagda driftkostnaderna för alla tre år till 118 mnkr (38–41 mnkr per år) för alternativ 1, respektive 186 mnkr (40–83 mnkr per år) för alternativ 2. I uppskattningarna ingår ökade driftskostnader för handläggning, kassasystem, den nationella televäxeln, rekrytering, utbildning, säkerhetsprövning, lokalkostnader och overheadkostnader. I dessa kostnader ingår även de av polisen uppskattade kostnaderna för support i samband med ansökan och aktivering. Polismyndigheten anger att utifrån de angivna ansökningsvolymerna och målgrupperna antas behovet av support vara lågt. De anger, att uppskatta och beräkna detta separat påverkar inte behovet av resurser och blir därför inte i sammanhanget meningsfullt.

Osäkerhetsfaktorn bedöms vara hög gällande framtagna uppskattningar, både såvitt avser kostnader för uppstart som för drift. Exempelvis har inga årliga prisuppräkningar gjorts utifrån att syftet enbart varit att få en uppfattning av omfattningen av kostnaderna.

Uppgiften att genomföra grundidentifiering för en statlig e-legitimation bedöms rymmas inom polisens befintliga verksamhet för kontor som utfärdar pass och nationella identitetskort. En säker bedömning kräver dock vidare analys i fråga om vilka expeditioner som kan vara aktuella.

Om fotografering och lagring av ansiktsbild ska ingå i processen kan den uppskattade tiden för ansökan påverkas. Längre besökstider

medför ökade kostnader vilket kan påverka de framtagna kostnadsuppskattningarna. Vidare kan användningen av biometriska data i processen ställa krav på tillgång till biometristationer vid ansökan och utlämning. Detta kan enligt polisen innebära behov av mer utrustning, vilket skulle öka uppskattade kostnader.

Tabell 9.4 Av Polismyndigheten uppskattade kostnader för de tre första åren

Miljoner kronor

	År 1	År 2	År 3
Volymer enligt alternativ 1	41	40	38
Volymer enligt alternativ 2	40	63	83

Källa: Polismyndigheten.

Utredningens bedömning av tillkommande kostnader för Polismyndigheten

Polismyndigheten har, utifrån befintlig information angett sig inte kunna uppskatta kostnaden för att etablera ett säkert nätverk med Digg. Vi bedömer att kostnaden för att etablera ett säkert nätverk för Polismyndigheten motsvarar kostnaden som i det avseendet anges för Digg (se avsnitt 9.5). Vi delar i övrigt Polismyndighetens bedömningar avseende uppstartskostnad och driftskostnader. Mot den bakgrunden finns det inte skäl för att, på samma sätt som för Skatteverket (se nedan), ange ytterligare kostnader för support eller säkerhetsprövning.

Tabell 9.5 Av utredningen uppskattade tillkommande kostnader för Polismyndigheten

Miljoner kronor

	År 1	År 2	År 3
Säkert nät mellan Polismyndigheten och Digg	3	2,5	2,5

Skatteverkets redovisade utgångspunkter för sina kostnadsuppskattningar

Skatteverket har i sitt underlag bedömt att ett utökat antal kontor med behov av personal och utrustning som t.ex. kameror, fingeravtrycksskanner, säkerhetsskåp för förvaring av kortämnen utgör den huvud-

sakliga kostnadsdrivaren, och inte ökade volymerna i föreslagna scenarier.

Identitetskort för folkbokförda i Sverige utfärdas för närvarande på 33 servicekontor och därutöver så lämnas korten ut på ytterligare 17 kontor.[11] Som framgått har Skatteverket lämnat sina svar med utgångspunkt i den identitetskortsverksamhet som bedrivs av myndigheten. Kostnaden för denna verksamhet uppgick till drygt 110 miljoner för 2022.[12] Enligt myndigheten skulle ett ökat antal kontor, från nuvarande 33 till 50, enligt ett grovt antagande innebära en kostnadsökning motsvarande minst 50 procent av kostnaden för identitetskortsverksamheten.

Skatteverket har vidare bedömt att det finns svårigheter förknippade med att bedriva verksamhet från ambulerande kontor. Med ambulerande kontor enligt Statens servicecenter (SSC) avses s.k. ”pop-upkontor”. De kommer alltså inte ha fasta lokaler där man kan förvara kortämnena och utrustningen. Öppettider för dessa kontor kan också komma att vara obestämd. Tanken är att SSC endast kommer att ha med sig en bärbar dator till den plats som bokats och där endast svara på enklare frågor. För att säkerställa att säkerhetskrav kan uppfyllas eller att grundidentifieringen kan hanteras behöver vidare utredning ske om ambulerande kontor skulle kunna utgöra ett alternativ och vilka konsekvenser det skulle få.

Tabell 9.6 Av Skatteverket uppskattade kostnader för de tre första åren

Miljoner kronor

	År 1	År 2	År 3
Volymer enligt alternativ 1	55	55	55
Volymer enligt alternativ 2	55	55	55

Källa: Skatteverket.

[11] Enligt uppgift från Skatteverkets hemsida finns det 34 kontor, jfr www.skatteverket.se/omoss/kontaktaoss/besokservicekontor.4.515a6be615c637b9aa4acd5.html?filter=idcards, (hämtad 2023-09-20).
[12] Skatteverket, Årsredovisning 2022 (Dnr 8-2211089), s. 85.

Utredningens bedömning av tillkommande kostnader för Skatteverket

I Skatteverkets uppskattningar ingår inte kostnader för säkerhetsklassning av personal, säkert nätverk mellan Digg, Statens servicecenter och Skatteverket eller kostnaden för support och stöd vid ansökan om och aktivering av statlig e-legitimation. Vi bedömer att de som kommer att ansöka om en statlig e-legitimation kommer att ha supportbehov vid ansökan och aktivering och att detta kan påverka behovet av antalet arbetade timmar för personalen vid kontoren. Denna beräkning bygger på en uppskattning av personalkostnad om 1 miljon kronor per år och att det behövs 0,2 årsarbetskrafter per kontor, vilket för 50 kontor ger en totalkostnad på 10 mnkr per år.

Vi bedömer att kostnaden för säkert nätverk är densamma om den ska upprättas mellan Skatteverket och Digg som mellan Polismyndigheten och Digg (se avsnitt 9.5 avseende hur kostnaden beräknats).

Vi bedömer att kostnaden för säkerhetsprövningar hos Skatteverket motsvarar de kostnader som Domarnämnden har för säkerhetsprövningar. Domarnämnden har en uppskattad kostnad för säkerhetsprövning om 1 mnkr om året.[13] De genomför ett 70-tal nya och uppföljande säkerhetsprövningar per år som då skulle ge en beräknad kostnad om cirka 15 000 kronor per säkerhetsprövad person[14]. Av underlaget från Skatteverket går det inte att utläsa hur många personer som kan behöva säkerhetsprövas per år. Vår bedömning är dock att kostnaderna för säkerhetsprövning inte överskrider 1 mnkr per år.

Tabell 9.7 Av utredningen uppskattade tillkommande kostnader för Skatteverket

Miljoner kronor

	År 1	År 2	År 3
Support vid ansökan och aktivering	10	10	10
Säkert nät mellan Skatteverket och Digg	3	2,5	2,5
Säkerhetsprövning av personal	1	1	1

[13] Prop. 2020/21:11 s. 17.
[14] Ibid.

Finansiering för grundidentifieringen

Polismyndigheten har i sitt underlag angett en uppstartskostnad om cirka 24 mnkr och att den behöver finansieras genom anslag. Regeringen anger i budgetpropositionen för 2024 att

> Regeringskansliet bereder förslagen om nya regler om svenska identitetshandlingar som lämnats i betänkandet Ett säkert statligt ID-kort – med e-legitimation (SOU 2019:14). Det huvudsakliga syftet med förslagen är att försvåra identitetsmissbruk och att motverka bedrägerier och andra brott som begås med hjälp av oriktiga id-handlingar. Enligt betänkandet ska staten framöver bara utfärda två allmängiltiga id-handlingar: ett nytt statligt identitetskort och det vanliga passet. Regeringen förstärker Polismyndigheten för att förslagen innebär förändringar för främst myndighetens verksamhet med utfärdande av id-handlingar. Det är också viktigt att så många som möjligt ska få tillgång till en säker e-legitimation. Regeringen avser därför även att utveckla en statlig e-legitimation (utg.omr. 22 avsnitt 4.5).[15]

I samband med detta föreslås ett utökat anslag till Polismyndigheten avseende säkra identitetshandlingar med 25 mnkr år 2024, 34 mnkr år 2025 och 46 mnkr år 2026.[16] Enligt Polismyndigheten kan driftskostnaderna dock antas täckas av avgiften för ansökan, på samma sätt som gäller för utfärdande av pass- och nationella identitetskort.

Skatteverket har i sitt underlag inte angett någon uppstartskostnad. Myndigheten har inte heller angett hur de anser att kostnaden för grundidentifieringen bör finansieras. Som tidigare angetts har dock Skatteverket för sina svar utgått från den egna identitetskortsverksamheten. För den verksamheten finansieras cirka 50 procent av driftkostnaderna via statligt anslag och 50 procent via avgifterna för att få ett identitetskort för folkbokförda i Sverige. Vi bedömer de totala kostnaderna för Skatteverket till 69 mnkr för det första året och 68,5 mnkr per år för år två och tre och om samma fördelning mellan anslag och avgiftsfinansiering för den statliga e-legitimationen som för id-kortsverksamheten skulle anslagsbehovet vara cirka 34,5 mnkr det första året och 34,25 mnkr de två nästföljande åren.

Vi delar Polismyndighetens bedömning att om de får i uppdrag att hantera grundidentifieringen så behöver uppstartskostnaden anslagsfinansieras, men att driftskostnaderna kan täckas av ansökningsavgifterna.

[15] Prop. 2023/24:1 Utgiftsområde 4, s. 51.
[16] Prop. 2023/24:1 Utgiftsområde 4, s. 55.

Vi har inte tillräckliga underlag från Skatteverket för att göra en mer precis bedömning men vi bedömer att det kommer att behövas en kombination av anslagsfinansiering och avgiftsfinansiering för driften om Skatteverket får i uppdrag att hantera grundidentifieringen.

9.6.3 Slutsatser utifrån uppskattade kostnader och finansieringsmöjligheter

Polismyndigheten har till skillnad från Skatteverket uppgivit en uppstartkostnad. Uppstartskostnaden uppgår till 24 mnkr. Polismyndigheten anger att antalet ansökningsställen för statlig e-legitimation inte i stort är kostnadsdrivande med tanke på omfattningen av antalet passexpeditioner. Skatteverket anger att antalet ansökningsställen är kostnadsdrivande i högre utsträckning än för Polismyndigheten. Utgångspunkten för beräkningarna har varit att grundidentifiering ska kunna ske på 50 kontor. Pass och nationellt identitetskort utfärdas av Polismyndigheten på omkring 110 platser, medan ansökan om identitetskort för folkbokförda i Sverige som utfärdas av Skatteverket kan göras på 34 olika servicekontor.[17] Om antalet ansökningsställen överstiger detta blir det en större kostnad för Skatteverket än för Polismyndigheten sett till antalet befintliga kontor.

Polismyndigheten anger att processen för ansökan och registrering av statlig e-legitimation kan göras enklare genom att koppla denna till Polismyndighetens ärendesystem för handläggning av pass och nationella identitetskort. En sådan integrering med handläggningssystemet kan spara tid vid ansökningstillfället och ger därmed förutsättningar för en mer kostnadseffektiv handläggning. I den mån de biometriska uppgifterna i systemet kan och får användas som stöd vid identifiering av den sökande kan en något högre säkerhet för vissa av målgrupperna uppnås.

[17] Enligt uppgift från Skatteverkets hemsida finns det 34 kontor, jfr www.skatteverket.se/omoss/kontaktaoss/besokservicekontor.4.515a6be615c637b9aa4acd5.html?filter=idcards, (hämtad 2023-09-20).

Tabell 9.8 Av utredningen uppskattad driftkostnad för de tre första åren

Miljoner kronor

	År 1	År 2	År 3
Polismyndigheten	43–45	42,5–65,5	40,5–85.5
Skatteverket	69	68,5	68,5

9.6.4 Kostnader för att utfärda statlig e-legitimation till personer bosatta utomlands

Ansökningar från svenska medborgare bosatta utomlands ska enligt vårt förslag hanteras av utlandsmyndigheterna (avsnitt 7.6.2). Digg har uppskattat kostnaderna för dessa ansökningar enligt följande:

> I nuläget bor närmare 700 000 svenskar utomlands. Digg uppskattar att cirka 10–20 procent av dessa personer skulle kunna vara intresserade av en statlig e-legitimation för att kunna utföra vissa ärenden. Givet samma antaganden rörande tidsåtgång som för Polismyndigheten med justering för en genomsnittslön baserat på de lönekostnader som framräknats av Statskontoret, skulle utlandsmyndigheternas administrativa kostnader för utfärdande av den statliga e-legitimationen ligga på cirka 4 årsarbetskrafter det första året, och 7 årsarbetskrafter år två. Detta motsvarar en tillkommande kostnad på ungefär 6 mnkr det första året, och 8 mnkr år två. Digg bedömer att siffrorna kan komma att behöva revideras baserat på hur många av utlandsmyndigheterna som kommer att utfärda den statliga e-legitimationen.[18]

Vi ansluter oss till Diggs uppskattning av kostnaderna för utlandsmyndigheterna. Vår bedömning är att viss del av kostnaderna kan täckas av avgifter men att det kommer behöva kompletteras med anslagsfinansiering. Anslaget kan antingen ske direkt till utlandsmyndigheterna eller i enlighet med vad Utrikesdepartementet framfört till Digg:[19]

> Utrikesdepartementet har gällande utlandsmyndigheterna uttryckt en önskan att hantera kostnaden för utfärdande av den statliga e-legitimationen via en kostnadsdelning i likhet med den som i dag finns mellan utlandsmyndigheterna och Migrationsverket gällande migrationsverksamheten. Det skulle innebära en användning av befintligt tidsmätningssystem för att mäta den tid det tar att handlägga ett utgivningsärende och i efterhand fakturera denna kostnad för tidsåtgång till ansvarig förvaltningsmyndighet, i detta fallet Digg. För att minimera administrationen, vore

[18] Myndigheten för digital förvaltning, *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, s. 88.
[19] Myndigheten för digital förvaltning, *En säker och tillgänglig statlig e-legitimation – Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*, s. 89 f.

det lämpligt att i ett sådant fall undersöka förutsättningarna för att Migrationsverket, i likhet med den befintliga överenskommelsen, hanterar den tillkommande administrationen för fakturering mellan myndigheter.

9.7 Konsekvenser för offentlig sektor i övrigt

9.7.1 Förslaget om kravet att vissa e-legitimationer ska godtas för identifiering i digitala tjänster

Ett obligatorium för offentlig förvaltning och vissa privata utförare av offentligfinansierad verksamhet att erkänna vissa e-legitimationer innebär en anpassningskostnad (se avsnitt 7.13). Den anpassningskostnaden följer av hanteringen av ytterligare e-legitimationstyper. En motsvarighet till denna anpassningskostnad har tidigare beräknats i det lämnade förslaget om krav på att statliga myndigheter ska använda tjänster för elektronisk identifiering som tillhandahålls inom auktorisationssystem. Sedan förslaget lämnats kan det antas att något fler statliga myndigheter har stöd för fler än en e-legitimationstyp samtidigt kan antalet som har stöd för en e-legitimationstyp nog ses som representativt då även andra offentliga aktörer och privata utförare av offentligt finansierad verksamhet räknas med. I promemorian där förslaget lämnas görs följande bedömning.

Kostnaderna för teknisk anslutning hänförliga till användningen av de tjänster som tillhandahålls inom nuvarande valfrihetssystem varierar mellan statliga myndigheter och beror på deras befintliga lösning. Det bedöms att drygt hälften av de offentliga aktörerna endast har stöd för en e-legitimationstyp i dag. Dessa myndigheter behöver möjliggöra inloggning med fler e-legitimationer, under förutsättning att de nya auktorisationssystemen har ungefär samma leverantörssammansättning och krav som nuvarande valfrihetssystem. Vidare bedöms att de myndigheter som tar emot en e-legitimation i dag får en startkostnad på cirka 25 000 kronor, de som tar emot två e-legitimationer får en startkostnad på cirka 10 000 kronor och de som redan i dag erbjuder stöd för tre eller fler e-legitimationstyper inte kommer att öka sina startkostnader. Den fasta månadskostnaden antas öka med fem procent per verksamhet till följd av att tjänsteleverantörer administrerar fler typer av e-legitimationer samt, teoretiskt sett, fler transaktioner. En stor del av de myndigheter som behöver göra tekniska anpassningar av sina system för att kunna ta emot nya leverantörer av tjänster för elektronisk identifiering kommer ändå att behöva göra motsvarande anpassningar för att kunna ta emot utländska e-legitimationer, vilket är en skyldighet enligt EU:s förordning om elektronisk identifiering. Sammantaget bedöms därför kostnaderna för teknisk anpassning bli marginella, under förutsättning att den tekniska kravställningen för nya

> e-legitimationsutfärdare hålls snarlik den kravställning som görs för anslutning till förbindelsepunkterna för gränsöverskridande elektronisk identifiering.[20]

Vi bedömer att de ovan redovisade kostnaderna för anslutning kan användas som utgångspunkt även för det nu aktuella förslaget. Det har till utredningen framförts att de organisationer som har använt egen infrastruktur eller externa systemintegratörer kan ha betydligt högre anpassningskostnader än ovan nämnda. Den exakta kostnaden för respektive aktör är dock svår att beräkna eftersom de har olika förutsättningar.

Om den myndighet som ansvarar för utfärdandet av den statliga e-legitimationen tillhandahåller en identifieringstjänst och förlitandetjänst i enlighet med avsnitt 7.4.3 kommer det troligen att minska svårigheterna och kostnaderna för aktörernas anpassning för att acceptera den statliga e-legitimationen.

Finansiering av de ekonomiska konsekvenserna

Ett av de grundläggande syftena med förslaget att godta identifiering med vissa e-legitimationer är att öka tillgängligheten till digital offentlig service. En av de grundläggande principerna inom svensk funktionshinderspolitik är den s.k. ansvars- och finansieringsprincipen. Den innebär att varje sektor i samhället ska utforma och bedriva sin verksamhet så att den blir tillgänglig för alla medborgare, inklusive personer med funktionsnedsättning.[21] Regeringen har därtill uttalat att utgångspunkten för finansieringen av en åtgärd för tillgänglighet bör, i linje med ansvars- och finansieringsprincipen, som är fastslagen av riksdagen, vara att kostnader ska täckas inom ramen för den ordinarie verksamheten. Principen innebär vidare att miljöer och verksamheter ska utformas och bedrivas så att de blir tillgängliga för alla människor, samtidigt som kostnaderna för anpassningsåtgärderna ses som en självklar del av de totala kostnaderna för verksamheten. Undantag från principen kan ske när andra lösningar anses vara effektivare. Det gäller t.ex. när kostnaderna anses vara stora i förhållande till huvudmannens ekonomiska möjligheter.[22] I budgetpropositionen för 2022 konstaterar regeringen att ansvars- och finansieringsprincipen är en

[20] *Auktorisationssystem för elektronisk identifiering och för digital post*, s. 51 f.
[21] Prop. 1999/2000:79 s. 16 f.
[22] Prop. 2013/14:198 s. 111.

viktig utgångspunkt för att nå det nationella målet för funktionshinderspolitiken.[23]

Utgångspunkten för finansieringen av en åtgärd för tillgänglighet bör utifrån ansvars- och finansieringsprincipen vara att kostnaderna ska täckas inom den ordinarie verksamheten. Mot bakgrund av redan gällande lagstadgade krav på tillgänglighet som åligger de flesta offentliga aktörer (se avsnitt 6.6.4), ansvars- och finansieringsprincipen samt den naturliga verksamhetsutveckling som tillgänglighetsanpassning innebär så ska de kostnader som kan uppstå till följd av förslaget finansieras inom den ordinarie verksamheten. Möjligheten till undantag från kraven kan även motverka att ökade kostnader uppstår till följd av ingångna avtal (se avsnitt 7.13.6).

9.7.2 Konsekvenser för domstolarna

Beslut som rör den statliga e-legitimationen får enligt vårt förslag överklagas till allmän förvaltningsdomstol. Under åren 2018–2021 registrerades omkring 150 mål rörande pass och nationellt identitetskort. För 2022 var motsvarande siffra 200 mål vilket sannolikt beror på för det året ökade ansökningsvolymer. Enligt uppgift från Polismyndigheten gjordes drygt 3 670 000 ansökningar om pass och nationella identitetskort 2022 (se avsnitt 7.6.2). Mot bakgrund av den statistiken och att förväntade ansökningsvolymer för den statliga e-legitimationen väsentligen understiger de för pass och nationella identitetskort, gör vi bedömningen att beslut om den statliga e-legitimationen inte kommer att generera någon större mängd mål för domstolarna. Förslaget bedöms därför inte få några konsekvenser för de allmänna förvaltningsdomstolarna som måste finansieras i särskild ordning.

9.7.3 Kommuner och regioner

Den kommunala självstyrelsen

I 14 kap. 3 § regeringsformen anges att en inskränkning i den kommunala självstyrelsen inte bör gå utöver vad som är nödvändigt med hänsyn till de ändamål som föranlett den. En lagstiftning som ställer

[23] Prop. 2021/22:1 Utgiftsområde 9, s. 114 f.

upp krav för en kommunal verksamhet minskar generellt sett kommunernas möjligheter att själva göra prioriteringar i sin verksamhet.

Förslagen om att regioner och kommuner i sina digitala tjänster ska godta identifiering med vissa e-legitimationer och ansluta till föreslaget auktorisationssystem innebär nya åligganden för regionerna och kommunerna. Förslagen är emellertid inte enbart riktade mot regioner och kommuner utan omfattar även statliga myndigheter och, vad gäller det förstnämnda kravet, vissa privata utförare inom offentligfinansierad verksamhet. Utredningens förslag som här är aktuella omfattar varken statlig eller kommunal verksamhet, dvs. kärnverksamhet eller kommunala angelägenheter.

Ett av syftena med kravet om att godta identifiering med vissa e-legitimationer är att öka tillgängligheten till digital offentlig service. Kommunerna omfattas redan i dag av generella krav på tillgänglighet som följer av annan lagstiftning och är således ålagda att verka för att deras tjänster ska vara tillgängliga (se avsnitt 6.6.4). Påverkan på den kommunala självstyrelsen får mot denna bakgrund anses begränsad vad gäller detta förslag. Ett ytterligare syfte med det föreslagna kravet är att skapa redundans och därmed öka samhällets robusthet mot antagonistiska angrepp. Den inskränkning som förslaget innebär får med beaktande av dessa syften anses vara proportionerlig.

Det föreslagna kravet om att regioner och kommuner ska ansluta till det föreslaget auktorisationssystem motiveras huvudsakligen med att kravet i lag om att godta identifiering med vissa e-legitimationer medför upphandlingsrättsliga problem samt att föreslaget auktorisationssystem har en befintlig teknisk infrastruktur och ett system för ersättning som kan användas för att på ett enklare och effektivare sätt realisera förslaget. Det får således anses utgöra en praktisk förutsättning för att genomföra förslaget om krav om att godta identifiering med vissa e-legitimationer. Det innebär även att berörda e-legitimationsutfärdare på lika villkor kan användas i anslutna aktörers digitala tjänster. Mot denna bakgrund anser vi att förslaget inte går utöver vad som är nödvändigt med hänsyn till de ändamål som föranlett det.

Kommunala finansieringsprincipen

Kommunala finansieringsprincipen innebär att om staten inför nya eller ändrade föreskrifter som ändrar skyldigheter för kommunerna och regionerna kan detta påverka dessas kostnader. För att hantera sådana konsekvenser har i samförstånd mellan staten, kommunerna och regionerna en finansieringsordning utvecklats, den s.k. kommunala finansieringsprincipen. Principen och dess tillämpning är inte lagfäst, men har godkänts av riksdagen.[24] Den kommunala finansieringsprincipen omfattar enbart statligt beslutade åtgärder som tar sikte på verksamheter. Principen innebär att staten inte bör införa nya obligatoriska uppgifter för kommuner och regioner, göra tidigare frivilliga uppgifter obligatoriska, ändra ambitionsnivån på befintliga uppgifter eller göra regeländringar som påverkar kommuners möjligheter att ta ut avgifter utan medföljande finansiering, t.ex. i form av höjda statsbidrag. En förändring som leder till sänkta kostnader för kommunerna och regionerna ska på motsvarande sätt innebära minskade bidrag.

Förslagen om att regioner och kommuner i sina digitala tjänster ska godta identifiering med vissa e-legitimationer och ansluta till det föreslaget auktorisationssystem kommer att leda till ökade kostnader, framför allt för regioner och kommuner som inte redan är anslutna till befintliga valfrihetssystem (se avsnitt 9.7.1). Beträffande den kommunala sektorn gäller även att den kommunala finansieringsprincipen ska tillämpas under vissa förutsättningar. Principen innebär att när staten beslutar om nya åtaganden och skyldigheter för kommunerna och regionerna ska de ges möjlighet att finansiera dessa med annat än höjda skatter.

Riktlinjerna för tillämpningen av den kommunala finansieringsprincipen har godkänts av riksdagen.[25] Den kommunala finansieringsprincipen omfattar enbart statligt beslutade åtgärder som direkt tar sikte på den kommunala verksamheten. Principen omfattar inte statliga beslut om åtgärder som inte direkt tar sikte på, men som ändå får direkta ekonomiska effekter för kommunsektorn, vilket bedöms vara fallet med nu aktuella lagförslag. Effekterna av sådana åtgärder ska däremot beaktas vid den bedömning som görs av det skattefinansierade

[24] Prop. 1993/94:150 bil. 7 avsnitt 2.5.1, bet. 1993/94:FiU19, rskr. 1993/94:442.
[25] Prop. 1993/94:150 bilaga 7 s. 30 f., bet. 1993/94 FiU19, rskr. 1993/94:442.

utrymmet i samband med fastställandet av statsbidragsramen, vilket årligen görs i budgetpropositionen.

9.8 Konsekvenser för företag

9.8.1 Krav om att godta vissa utpekade e-legitimationer

De företag som träffas av krav på att godta vissa utpekade e-legitimationer är sådana som yrkesmässigt bedriver verksamhet som till någon del är offentligt finansierad inom förskola, skola, hälso- och sjukvård samt omsorg (se vidare avsnitt 7.13.4). Statistiska uppgifter från perioden 2015–2020 visar att 17 till 19 procent av verksamheten inom välfärdssektorn utfördes av privata utförare. Högst andel finns inom omsorgen, följt av hälso- och sjukvård och därefter privata utförare och inom utbildning.[26]

Vad gäller hälso- och sjukvård samt omsorgsverksamhet utgörs de privata utförarna av närmare 15 600 vård- och omsorgsföretag. Det är en småföretagarbransch; inom sektorn har 94 procent av företagen färre än 20 anställda.[27]

Friskolesektorn domineras av för-, grund- och gymnasieskolor (skolenheter) vars huvudmän är aktiebolag. Detta gäller särskilt gymnasieskolorna, av vilka nästan 90 procent drivs av aktiebolag. Inom grundskolan är motsvarande andel cirka 60 procent. Av de fristående förskolenheterna drivs cirka 45 procent i bolagsform.[28]

Det är emellertid förenat med vissa svårigheter att få fram uppgifter om hur många bolag det är fråga om och deras storlek. Det finns drygt 4 000 fristående skolenheter i Sverige, varav drygt 2 600 är förskolor. Inom förskolan och grundskolan har 98 respektive 95 procent av huvudmännen en eller två enheter. För gymnasiet är motsvarande andel 84 procent. Att majoriteten av de fristående huvudmännen driver få, och inte sällan relativt sett små, enheter innebär dock inte nödvändigtvis att dessa definitionsmässigt utgör småföretag.

[26] Statistiknyhet från Statistiska centralbyrån (SCB), www.scb.se/hitta-statistik/statistik-efter-amne/offentlig-ekonomi/finanser-for-den-kommunala-sektorn/finansiarer-och-utforare-inom-varden-skolan-och-omsorgen/pong/statistiknyhet/finansiarer-och-utforare-inom-vard-skola-och-omsorg-20202/ (hämtad 2023-09-12).
[27] Almega, Vårdföretagarna, *Privat vårdfakta*, Fakta och statistik om den privat drivna vård- och omsorgsbranschen, 2022, s. 15.
[28] Friskolornas riksförbund, Rapport, *Fakta om friskolor 2023*, s. 32. Begreppet ”huvudman” används inte för förskolan, varför statistik om antal varumärken/ägare bör betraktas som osäker, se a.a. s. 30.

Ett bolag kan äga flera huvudmän med både en, två och flera enheter. Friskolornas Riksförbunds lista över de största friskoleägarna i februari 2023 visar att de 19 största ägarna svarar för cirka 600 skolenheter på grundskole- och gymnasienivå, motsvarande drygt 40 procent av alla fristående skolor. För förskolor är ägarkoncentrationen lägst: 0,7 procent av antalet ”förskolehuvudmän” äger knappt 20 procent av förskolenheterna.[29] Enligt muntliga uppgifter från Friskolornas riksförbund uppgår antalet medlemmar till cirka 500, varav 80 procent av dessa är aktiebolag. Även om samtliga fristående skolhuvudmän inte är medlemmar i förbundet ger dock denna uppgift, liksom övrig redovisad information, en indikation om antalet företag och deras storlek.

Det föreslagna kravet omfattar även enskilda utbildningsanordnare med tillstånd att utfärda examina enligt lagen om tillstånd att utfärda vissa examina, och som till största delen har statsbidrag som finansiering av högskoleutbildning på grundnivå eller avancerad nivå eller för utbildning på forskarnivå. Den senast kända uppgiften är att sådana företag uppgår till 14 (maj 2018).[30]

Av de företag som i och för sig omfattas av det föreslagna kravet erbjuder inte samtliga sådana digitala tjänster där inloggning krävs med e-legitimation.

Kostnaderna för de berörda företagen bedöms främst bestå av utvecklings- och anpassningskostnader för att hantera de utpekade e-legitimationerna. Kostnaderna bedöms vara i nivå med de uppskattade kostnaderna för de statliga aktörerna i avsnitt 9.7.1. Anpassningen och utvecklingen kan medföra begränsade administrativa kostnader.

Andra företag som kommer att beröras av förslaget är de som i dagsläget erbjuder sådana integrationstjänster som innebär att de agerar mellanhand mellan en förlitande part och en e-legitimationsutfärdare. Detta gäller exempelvis de företag som ingår i Kammarkollegiets ramavtalsområden inom programvaror och tjänster (se avsnitt 4.6). Om förslaget genomförs kommer de inte längre att kunna sälja sådana tjänster till de aktörer som enligt förslaget ska anslutas till auktorisationssystem.[31] Sammantaget finns det cirka 20 leverantörer som erbjuder olika former av tjänster för elektronisk identifiering och integrationstjänster på den svenska marknaden. Ett fåtal tjänste-

[29] A.a. s. 81 ff. respektive s. 31.
[30] Prop. 2017/18:299 s. 80.
[31] Prop. 2023/24:6. Ny reglering av auktorisationssystem för elektronisk identifiering och för digital post föreslås träda i kraft den 1 januari 2024.

leverantörer har dock betydande delar av marknaden. Dessa leverantörer är av varierande storlek. Vissa företag ingår i större it-koncerner, men det finns ett fåtal mikroföretag som också verkar på marknaden.[32]

9.8.2 Id-växling från den statliga e-legitimationen

Om den statliga e-legitimationen når stora volymer kan förutsättningar för mer omfattande id-växling till kommersiella e-legitimationer skapas. Det gäller de nuvarande kommersiella e-legitimationerna men det skapar även ökade möjligheter för att nya aktörer etablerar sig på marknaden då kostnaderna för den initiala identifieringen sänks (se avsnitt 7.10.1). Det beror på att tiden och kostnaden för en tillhandahållare att identifiera individer till vilka de utfärdar e-legitimation är mycket omfattande, troligen de mest kostsamma för en e-legitimation utfärdare.

Id-växling kan även bidra till att antalet utfärdare och olika e-legitimationer blir fler, vilket ökar redundansen och minskar sårbarheten för samhället om en enskild e-legitimations utfärdare drabbas av säkerhetsincidenter eller omfattande sårbarheter.

9.9 Konsekvenser för individer och hushåll

Vi föreslår att den statliga e-legitimationen ska kunna utfärdas till individer från det år de fyller nio under förutsättning att de är svenska medborgare eller har ett samordningsnummer med styrkt identitet. Det kommer således vara möjligt för personer från andra länder som arbetar eller studerar i Sverige och för svenska medborgare bosatta utomlands att skaffa den statliga e-legitimationen.

De krav som vi föreslår ska gälla för att få en statlig e-legitimation är nödvändiga av säkerhetsskäl och kommer i huvudsak att motsvara de som befintliga aktörer ställer. Våra förslag kommer därför inte medföra att fler personer på grund av en ändrad kravställning kan få en e-legitimation. För att fullt ut inkludera de individer som saknar e-legitimation behöver i stället ytterligare åtgärder vidtas, exempelvis genom att ställföreträdare ges möjlighet att bistå sina huvudmän eller att

[32] *Promemoria om auktorisationssystem för elektronisk identifiering och för digital post*, s. 52.

anpassade lösningar i användningsskedet införs. För att gruppen äldre ska inkluderas behövs, utöver bistånd från ställföreträdare, omfattande informationskampanjer för att utbilda i användarförmåga och säkerhetskunskap. Utan erforderliga åtgärder i dessa avseenden riskerar tillgång till en e-legitimation leda till att redan utsatta grupper drabbas av identitetsrelaterad brottslighet i större omfattning än vad som redan är fallet. Sammanfattningsvis kan vi konstatera att de förslag vi presenterar skapar förutsättningar för att minska det digitala utanförskapet men att ytterligare åtgärder kommer krävas för att med bibehållen säkerhetsnivå nå ännu fler.

Personer med samordningsnummer som inte når upp till nivån styrkt kommer inte kunna skaffa en statlig e-legitimation till följd av våra förslag. Det är enligt vår bedömning inte möjligt att, med erforderlig säkerhet, utfärda en statlig e-legitimation på högsta tillitsnivån till dessa personer. Eftersom inte heller privata aktörer på marknaden godtar samordningsnummer med lägre identitetsnivå än styrkt kommer dessa personer fortsatt stå utan tillgång till väsentliga samhällsfunktioner.

Vårt uppdrag har inte omfattat att utreda om en statlig e-legitimation kan tillhandahållas på en lägre tillitsnivå. Vi menar dock att det kan finnas skäl för att i särskild ordning utreda om en statlig e-legitimation på en lägre tillitsnivå bör införas för att tillgodose behovet för personer med samordningsnummer med lägre identitetsnivå än styrkt att kunna legitimera sig elektroniskt.

Som en del i finansieringen av den statliga e-legitimationen föreslår vi att en avgift om 400 kronor ska tas ut från den som vill ansöka om en statlig e-legitimation. Detta kommer att innebära en ökad kostnad för hushållen och individen. För en familj med två barn motsvarar kostnaden 1 600 kronor fördelat på fem år således 26 kronor per månad.[33] Vi anser att kostnaden är adekvat och berättigad för att tydliggöra e-legitimationens status som en värdehandling. Enligt våra bedömningar skulle det emellertid vara en fördel om den statliga e-legitimationen framöver tillhandahålls på en befintlig fysisk id-handling. I sådant fall bör samordningsvinster kunna medföra en lägre kostnad.

Enligt våra förslag kommer det inte vara möjligt att ansöka om en statlig e-legitimation genom bud vilket sannolikt får en begränsande

[33] Exemplet utgår från att e-legitimationen placeras på ett kontaktlöst kort och inte en befintlig id-handling. Vid placering på en fysisk ID-handling kan kostnaden öka om giltighetstiden för minderåriga bestäms till en kortare tid än fem år.

effekt för individer med olika funktionsnedsättningar. Även om det blir en uppgift för det allmänna att skapa förutsättningar exempelvis genom möjlighet till färdtjänst, anpassade lokaler och eventuell ambulerande verksamhet kan begränsningen leda till att vissa personer inte kan skaffa en statlig e-legitimation.

9.10 Konsekvenser för brottsligheten och det brottsförebyggande arbetet

Vi föreslår att en statlig e-legitimation utfärdas på den högsta tillitsnivån vilket medför ett krav på personlig inställelse i samband med ansökan. Kravet på personlig inställelse är en grundläggande förutsättning för att motverka den identitetsrelaterade brottsligheten som beskrivs i avsnitt 6.7. De förslag vi lämnar i avsnitt 7.11 som innebär att den utfärdande myndigheten ska få lagra och utföra jämförande sökningar på biometriska uppgifter vid ansökan kan enligt vår bedömning förväntas bidra till möjligheten att motverka identitetsrelaterad brottslighet.

Den identitetsrelaterade brottsligheten är omfattande och ett betydande samhällsproblem. Som framgår i avsnitt 6.7 har BankID beskrivits som en ”dörröppnare för kriminella aktörer”. En risk med att bereda en redan utsatt del av befolkningen tillgång till en e-legitimation är att kriminella aktörer får ytterligare verktyg för att begå brott. Även om vi bedömer att de förslag vi lämnar – så långt det är möjligt – säkerställer en säker utgivningsprocess och utformning är användningsskedet av avgörande betydelse. En korrekt utfärdad e-legitimation kan i fel användares hand användas för att begå brott. Således finns det – som en följd av en ökad användning av e-legitimationer – en risk för att den identitetsrelaterade brottsligheten ökar till följd av våra förslag. För att motverka en sådan utveckling kommer bl.a. lättillgänglig support samt tydlig och omfattande information att behövas. Någon exakt statistik över den brottslighet som begås med användande av just e-legitimationer har vi inte kunnat finna varför en närmare beräkning av kostnaderna inte låter sig göras. Som redovisas i avsnitt 6.7.5 uppgick dock brottsvinsterna för bedrägeribrottsligheten till 5,8 miljarder kronor 2022. Det finns mot den bakgrunden anledning att utgå ifrån att kostnaderna för brottslighet som begås med användning av e-legitimationer är betydande.

För den enskilde som drabbas av att någon obehörigt använder sig av dennes e-legitimation kan bedrägeribrotten få allvarliga konsekvenser, om förutsättningarna för återställande av kontot inte föreligger. Även om den enskilde enligt reglerna i lagen (2010:751) om betaltjänster helt eller delvis undgår betalningsansvar, drabbas hon eller han åtminstone kortvarigt av likviditetsproblem som i sin tur kan komma att påverka ekonomin allvarligt (se avsnitt 7.8). Alldeles oavsett påverkas den enskilde av att bedrägeriet medför olägenhet och obehag.

De ekonomiska konsekvenserna drabbar även näringslivet, inte minst kreditinstituten som alltså har en skyldighet att återställa bedragna kontoinnehavare under vissa förutsättningar. Därutöver drabbas staten, och i förlängningen allmänheten, av den ökande brottslighet som är riktad mot välfärdssystemen.

Givet att Polismyndigheten ges i uppdrag att vara identitetskontrollerande myndighet i samband med utfärdande av e-legitimationer skulle myndigheten kunna dra nytta av de erfarenheter som myndigheten har i den brottsbekämpande verksamheten. Ett sådant ansvar hos en och samma myndighet ökar förutsättningarna för att bedriva ett mer effektivt brottsförebyggande arbete.

9.11 Konsekvenser för sysselsättningen och offentlig service i olika delar av landet

Avsikten med de förslag vi lämnar är att fler personer ska ges tillgång till en e-legitimation. Därigenom kan tillgången till digital offentlig service i hela landet förväntas öka.

Vi bedömer att våra förslag inte kommer att få några nämnvärda konsekvenser för sysselsättningen.

9.12 Konsekvenser för jämställdheten mellan kvinnor och män samt flickor och pojkar

Andelen kvinnor i åldersgruppen 16–85 år som använder mobilt BankID eller BankID med kortläsare vid legitimering på internet är 84 procent. Motsvarande andel män är 86 procent.[34] Även kvinnors och mäns respektive användning av myndigheters webbsidor eller appar är i stort sett likvärdig för åldersgruppen 16–85 år. Exempelvis har 68 procent av männen och 71 procent av kvinnorna e-deklarerat själva samt 66 procent av kvinnorna och 63 procent av männen hämtat information.[35] Detta talar för att kvinnor och män har likartade förutsättningar för att använda en statlig e-legitimation. Förslagen bedöms därför inte få några konsekvenser för jämställdheten mellan män och kvinnor.

9.13 Konsekvenser för att nå de integrationspolitiska målen

Att ha tillgång till en e-legitimation är i många avseenden en förutsättning för att delta i olika samhällsfunktioner och därmed också viktigt för ökad integration. Således begränsar avsaknaden av e-legitimation, som beskrivs i avsnitt 6.6.2, möjligheten för asylsökande och nyanlända att integreras. De förslag vi lämnar tillgodoser inte detta behov fullt ut men innebär i vart fall att individer med samordningsnummer för personer med styrkt identitet kan få den statliga e-legitimationen, vilket kan bidra till att nå de integrationspolitiska målen. I förhållande till den ordning som nu gäller får förslagen enligt vår bedömning inte några negativa konsekvenser för att nå de integrationspolitiska målen.

[34] Statistiska centralbyrån, Statistikdatabasen, Legitimering vid användning av internet efter legitimeringssätt, kön och redovisningsgrupp. År 2020.
[35] Statistiska centralbyrån, Statistikdatabasen, Användning av myndigheters webbsidor eller appar efter användningsområde, kön och redovisningsgrupp. År 2021–2022.

9.14 Tidpunkten för ikraftträdande och behov av speciella informationsinsatser

Vi gör bedömningen att förslagen kan genomföras tidigast den 1 mars 2026 (se kapitel 8).

Det finns visst behov av informationsinsatser från främst den utfärdande myndighetens sida i anslutning till att de nya och ändrade reglerna träder i kraft (se avsnitt 9.5).

10 Författningskommentar

10.1 Förslaget till lag om elektronisk identifiering

Lagens innehåll och förhållande till annan reglering

1 § Denna lag innehåller bestämmelser om medel för elektronisk identifiering som utfärdas av staten samt krav på erkännande av vissa medel för elektronisk identifiering.

Bestämmelser om medel för elektronisk identifiering finns också i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, här benämnd EU:s förordning om elektronisk identifiering samt, i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

Av paragrafen framgår lagens innehåll. Lagen kompletteras med föreskrifter meddelade av regeringen eller den myndighet som regeringen bestämmer. Övervägandena finns i avsnitten 7.1 och 7.11.3.

Vad som avses med elektronisk identifiering och med medel för elektronisk identifiering följer av 2 §. Enligt vad som anges i kommentaren till det lagrummet används som synonym för medel för elektronisk identifiering uttrycket e-legitimation.

Av *första stycket* framgår att lagens bestämmelser gäller för en sådan e-legitimation som utfärdas av staten, och inte av privata aktörer. I 26 § finns emellertid en bestämmelse som är tillämplig även på sådana e-legitimationer som tillhandahålls av en leverantör som är godkänd i enlighet med den föreslagna lagen om auktorisationssystem för elektronisk identifiering och för elektronisk post (prop. 2023/24:6).

Andra stycket innehåller en upplysningsbestämmelse. I den däri nämnda svenska författningen finns bestämmelser om bl.a. granskning av kvalificerade tillhandahållare av betrodda tjänster och om certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter m.m., samt om tillsyn och om offentliga organs skyldig-

het att ansluta sina nättjänster till den svenska noden för inkommande gränsöverskridande elektronisk identifiering. De hänvisningar till EU:s förordning om elektronisk identifiering (eIDAS-förordningen) som finns i lagen är dynamiska. Det innebär att hänvisningarna avser eIDAS-förordningen i dess vid varje tidpunkt gällande lydelse.

Ord och uttryck i lagen

2 § Med elektronisk identifiering, medel för elektronisk identifiering, nättjänst och autentisering avses i denna lag detsamma som i EU:s förordning om elektronisk identifiering.

Paragrafen innehåller definitioner av vissa begrepp genom hänvisningar till eIDAS-förordningen. Övervägandena finns i avsnitt 7.1

Medel för elektronisk identifiering är det uttryck som även i nationella författningar används i stället för den i vardagligt tal och allmänt accepterade benämningen e-legitimation, se avsnitt 3.5.

Av artikel 3.1 i nämnda förordning framgår att med elektronisk identifiering avses ”en process inom vilken personidentifieringsuppgifter i elektronisk form, som unikt avser en fysisk eller juridisk person eller en fysisk person som företräder en juridisk person, används”.

I artikel 3.2 i samma förordning anges att medel för elektronisk identifiering avser ”en materiell och/eller immateriell enhet som innehåller personidentifieringsuppgifter och som används för autentisering för nättjänster.”

Nättjänster eller digitala tjänster är sådana tjänster som en aktör tillhandahåller på elektronisk väg, t.ex. självbetjäningstjänster via internet, och som gör det möjligt för användare att hantera sina ärenden hos aktören på elektronisk väg (jfr prop. 2012/13:123 s. 65.). I eIDAS-förordningen används uttrycket med denna betydelse, men det ingår inte bland definitionerna i artikel 3.

Enligt artikel 3.5 i eIDAS-förordningen avses med autentisering ”en elektronisk process som gör det möjligt att bekräfta den elektroniska identifieringen för en fysisk eller juridisk person, eller ursprunget för och integriteten hos uppgifter i elektronisk form.”

3 § Med en offentlig aktör avses i denna lag

1. en statlig eller kommunal myndighet, eller en beslutande församling i en kommun eller region,

2. en sammanslutning som inrättats särskilt för att tillgodose behov i det allmännas intresse, under förutsättning att behovet inte är av industriell eller kommersiell karaktär, och som består av en eller flera myndigheter eller församlingar som anges i 1,

3. en privat aktör som yrkesmässigt bedriver verksamhet som till någon del är offentligt finansierad och som

a) aktören bedriver i egenskap av enskild huvudman inom skolväsendet eller huvudman för en sådan internationell skola som avses i 24 kap. skollagen (2010:800),

b) utgör hälso- och sjukvård enligt hälso- och sjukvårdslagen (2017:30) eller tandvård enligt tandvårdslagen (1985:125),

c) bedrivs enligt socialtjänstlagen (2001:453), lagen (1988:870) om vård av missbrukare i vissa fall, lagen (1990:52) med särskilda bestämmelser om vård av unga eller lagen (1993:387) om stöd och service till vissa funktionshindrade, eller

d) utgör personlig assistans som utförs med assistansersättning enligt 51 kap. socialförsäkringsbalken, eller

4. en enskild utbildningsanordnare med tillstånd att utfärda examina enligt lagen (1993:792) om tillstånd att utfärda vissa examina, och som till största delen har statsbidrag som finansiering av högskoleutbildning på grundnivå eller avancerad nivå eller av utbildning på forskarnivå.

I paragrafen anges vad som vid tillämpningen av denna lag avses med benämningen offentlig aktör. Genom definitionen tydliggörs vilka offentliga aktörer som omfattas av kravet om att för sina digitala tjänster godkänna identifiering med den statliga e-legitimationen som finns i 26 §. Övervägandena finns i avsnitt 7.13.4.

Paragrafen motsvarar 4 § lagen (2018:1937) om tillgänglighet till digital offentlig service frånsett att förevarande bestämmelse inte omfattar offentligt styrda organ. I berörda delar har paragraferna samma innebörd, se prop. 2017/18:299 s. 30 ff. och 86 ff.

Ansökan om och utfärdande av statligt medel för elektronisk identifiering

4 § Statligt medel för elektronisk identifiering får, efter ansökan, utfärdas av den myndighet som regeringen bestämmer (utfärdande myndighet).

Paragrafen innehåller ett bemyndigande för regeringen att föreskriva vilken myndighet som ska utfärda den statliga e-legitimationen. Den myndighet som ansvarar för uppgiften framgår av 2 § i den föreslagna förordningen om elektronisk identifiering. Övervägandena finns i avsnitten 7.4.2 och 7.6.3.

Av bestämmelsen framgår även att utfärdande av en statlig e-legitimation ska ske efter ansökan, vilket är ett krav för tillitsnivå hög enligt Kommissionens genomförandeförordning (EU) 2015/1502 av den 8 september 2015 om fastställande av tekniska minimispecifikationer och förfaranden för tillitsnivåer för medel för elektronisk identifiering i enlighet med artikel 8.3 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden, härefter genomförandeförordningen (EU) 2015/1502.

Den utfärdande myndigheten ska se till att även övriga krav enligt nämnda rättsakter är uppfyllda, exempelvis kontroll av att uppgifterna i ansökan är fullständiga och att de stämmer överens med uppgifter i ett officiellt register.

5 § Statligt medel för elektronisk identifiering får utfärdas till en person som innevarande kalenderår är eller ska fylla nio år och som har antingen ett svenskt personnummer enligt folkbokföringslagen (1991:481) eller ett sådant samordningsnummer som tilldelats personer som styrkt sin identitet enligt lagen (2022:1697) om samordningsnummer, som inte är förklarat vilande.

För den som är under arton år krävs vårdnadshavares skriftliga medgivande.

Paragrafen reglerar till vem den statliga e-legitimationen får utfärdas. Övervägandena finns i avsnitt 7.4.2.

Av första stycket framgår att personer som är folkbokförda i landet, dvs. såväl svenska som icke svenska medborgare, vilka därmed har ett personnummer, kan ansöka och få en statlig e-legitimation, förutsatt att ålderskravet är uppfyllt. Den statliga e-legitimationen kan utfärdas även till personer utomlands, om de uppfyller angivna krav.

Utöver individer med personnummer kan statlig e-legitimation utfärdas till alla som på egen eller en myndighets begäran tilldelats ett samordningsnummer med styrkt identitet (2 kap. 2–4 §§ lagen om samordningsnummer), exempelvis personer som äger en fastighet, eller personer som vistas i landet för att arbeta, bedriva näringsverksamhet eller studera vid högskola eller universitet (som har rätt att utfärda vissa examina). Ett sådant samordningsnummer får inte ha förklarats vilande (3 kap. 2 § nämnda lag). Även personer med ett sådant samordningsnummer måste uppfylla ålderskravet.

I *andra stycket* föreskrivs krav på vårdnadshavares medgivande när sökanden är minderårig. Enligt 5 § i den föreslagna förordningen om

elektronisk identifiering får undantag från kravet medges, om det föreligger synnerliga skäl att ändå utfärda e-legitimationen. Bestämmelserna motsvarar vad som gäller för pass och vissa statliga identitetshandlingar (7 § passlagen [1978:302], 3 § förordningen [2005:661] om nationellt identitetskort och 5 § förordningen [2015:904] om identitetskort för folkbokförda).

6 § Den sökande är skyldig att styrka sin identitet och övriga personuppgifter.

I paragrafen regleras skyldigheten för sökanden att vid ansökan styrka sin identitet. Motsvarande bestämmelser finns i passlagen, förordningen om nationellt identitetskort och lagen om identitetskort för folkbokförda i Sverige. Övervägandena finns i avsnitt 7.5.

Att sökandens identitet säkerställs är av central betydelse för att garantera att utfärdandet av de statliga e-legitimationerna sker på en hög säkerhetsnivå. Detaljreglering av hur detta ska ske finns i föreskrifter som meddelas enligt 11 § andra stycket 1.

7 § Kontroll av att sökandens identitet är styrkt ska göras av den eller de myndigheter som regeringen bestämmer (identitetskontrollerande myndighet).

Paragrafen innehåller ett bemyndigande för regeringen att föreskriva vilken eller vilka myndigheter som ska ansvara för uppgiften att kontrollera identiteten hos den som ansöker om den statliga e-legitimationen. Övervägandena finns i avsnitt 7.6.2.

8 § I samband med ansökan är sökanden skyldig att låta den identitetskontrollerande myndigheten ta ett fingeravtryck och en ansiktsbild i digitalt format.

Paragrafen reglerar att fingeravtryck och ansiktsbild ska tas vid ansökan om statlig e-legitimation. Övervägandena finns i avsnitt 7.5.

Paragrafen motsvarar 6 § andra stycket 1 passlagen, 3 § andra stycket 1 förordningen om nationellt identitetskort och (delvis) 2 § 1 lagen om identitetskort för folkbokförda i Sverige. Syftet är att fingeravtrycken och ansiktsbilden ska sparas i ett lagringsmedium i bäraren av den statliga e-legitimationen. Detta framgår av 9 § förevarande lag. Fingeravtrycken och ansiktsbilden får också användas för att jämföra med, i förekommande fall, motsvarigheter på eller i den

identitetshandling som sökanden uppvisar vid ansökan. Detta framgår av 7 § i den föreslagna förordningen om elektronisk identifiering.

9 § Fingeravtrycken och ansiktsbilden enligt 8 § ska sparas i ett lagringsmedium i bäraren av det statliga medlet för elektronisk identifiering.

Fingeravtrycken och de biometriska data som tas fram ur dessa ska omedelbart förstöras när det statliga medlet för elektronisk identifiering har lämnats ut eller en ansökan om sådant medel har återkallats eller avslagits.

Paragrafen föreskriver att fingeravtryck och ansiktsbild ska finnas i ett lagringsmedium i bäraren av den statliga e-legitimationen. Övervägandena finns i avsnitten 7.2.6 och 7.11.7.

Bestämmelsen i *första stycket* motsvarar det som gäller för pass och nationella identitetskort. Av 8 § i den föreslagna förordningen om elektronisk identifiering framgår att bäraren av den statliga e-legitimationen är ett kontaktlöst kort.

Bestämmelsen i *andra stycket* är delvis utformad efter förebild i 6 a § passlagen och 4 § andra stycket förordningen om nationellt identitetskort. Av bestämmelsen följer att fingeravtryck och de biometriska uppgifter som kan tas fram ur dessa endast får behandlas under tiden handläggningen av sökandens ansökan pågår, och ska därefter tas bort. Syftet med den tillfälliga lagringen är att den identitetskontrollerande myndigheten ska kunna göra en kvalitetskontroll av uppgifterna som finns i lagringsutrymmet på bäraren av den statliga e-legitimationen i samband med att kortet lämnas ut. Fingeravtrycken får inte sparas i den databas som ska föras enligt 16 § utan endast lagras tillfälligt i den utfärdande myndighetens ärendehanteringssystem.

10 § En ansökan ska avslås om förutsättningarna i 5 och 6 §§ inte är uppfyllda. Detsamma gäller om det som anges i 8 § eller som föreskrivits i enlighet med 11 § andra stycket 1 inte har iakttagits, och sökanden inte har följt en uppmaning att avhjälpa bristen.

I paragrafen anges när en ansökan ska avslås. Övervägandena finns i avsnitt 7.4.2.

Paragrafen motsvarar i sak 4 § lagen om identitetskort för folkbokförda i Sverige och 8 § förordningen om nationellt identitetskort. Bestämmelsen innebär att ansökan om statlig e-legitimation ska avslås om de grundläggande förutsättningarna för e-legitimationens utfärdande inte är uppfyllda. Detsamma gäller om det som föreskrivits i

fråga om ansökan eller utlämnande inte har iakttagits och sökanden inte följt en uppmaning att avhjälpa bristen.

I bestämmelsen anges att även underlåtelse att iaktta föreskrifter som meddelats i anslutning till lagen ska leda till avslag. Det innebär att föreskrifter som har meddelats med stöd av delegationsbestämmelser i lagen såväl som föreskrifter som har meddelats med stöd av regeringens restkompetens eller i form av verkställighetsföreskrifter enligt 8 kap. 7 § regeringsformen omfattas.

11 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om undantag från skyldigheten att lämna fingeravtryck när det gäller minderåriga och personer som av fysiska skäl är permanent förhindrade att lämna fingeravtryck.

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om

1. ansökan om samt utfärdande och utlämnande av ett statligt medel för elektronisk identifiering, och
2. utformningen av det statliga medlet för elektronisk identifiering..

Paragrafens *första stycke* innehåller ett föreskriftsbemyndigande beträffande undantag från skyldigheten att lämna fingeravtryck, se även 6 och 12 §§ i den föreslagna förordningen om elektronisk identifiering. Bestämmelsen i förevarande paragraf är utformad efter förebild i (delvis) 6 § tredje stycket passlagen. Övervägandena finns i avsnitt 7.5.

I *andra stycket* finns en upplysningsbestämmelse om föreskriftsrätt vad gäller bl.a. tillämpningsbestämmelser av administrativ och teknisk karaktär. Övervägandena finns i avsnitten 7.4.2, 7.5 och 7.7.1 (*punkten 1*) respektive 7.2.2 och 7.3 (*punkten 2*).

Bestämmelser på förordningsnivå eller i myndighetsföreskrifter reglerar giltighetstid och fastställer exempelvis tekniska krav och detaljreglera utgivnings- och aktiveringsprocesser så att det säkerställs att den statliga e-legitimationen uppfyller eIDAS-regelverkets villkor för tillitsnivå hög, se bl.a. 8 § i den föreslagna förordningen om medel för elektronisk identifiering. Av den paragrafen framgår att den statliga e-legitimationen ska ha ett kontaktlöst kort som fysisk bärare och uppfylla kraven för tillitsnivå hög enligt eIDAS-regelverket. Föreskriftsrätten avseende utformningen av e-legitimationen omfattar också dess innehåll.

Återkallelse och spärr av statligt medel för elektronisk identifiering

12 § Ett statligt medel för elektronisk identifiering ska återkallas och spärras om

1. det fanns hinder mot att utfärda ett sådant medel vid tiden för utfärdandet och hindret fortfarande består,
2. någon väsentlig uppgift som ett sådant medel innehåller är felaktig eller inte längre gäller,
3. det är nödvändigt av säkerhetsskäl för att någon annan än den som ett sådant medel är utställt till kan misstänkas obehörigt förfoga över det, eller om innehavaren av medlet på annat sätt förlorat kontrollen över det,
4. ett sådant medel inte har aktiverats inom sex månader efter att ansökan gjordes, eller
5. innehavaren av ett sådant medel har avlidit.

På begäran av innehavaren får ett statligt medel för elektronisk identifiering återkallas och spärras.

Paragrafen reglerar grunderna för återkallelse och spärr av den statliga e-legitimationen. Övervägandena finns i avsnitt 7.7.2. Paragrafen är utformad delvis efter förebild i 6 § lagen om identitetskort för folkbokförda och 9 § förordningen om nationellt identitetskort.

Av *första stycket* framgår grunderna för en återkallelse. En bestämmelse motsvarande den i *första punkten* finns även i 12 § passlagen. Den har motiverats av att det inte anses vara rimligt att ett pass eller en identitetshandling ska fortsätta att gälla om det i efterhand visat sig att förutsättningarna för att utfärda det inte var uppfyllda, t.ex. att en person fått handlingen i någon annans namn.

Det som anges i styckets *andra punkt,* om en väsentlig uppgift i e-legitimationen är felaktig eller inte längre gäller, omfattar både rena felskrivningar och ändringar av personuppgifter, t.ex. om ett samordningsnummer får ändrad identitetsnivå och inte längre når upp till nivån styrkt, om innehavaren har bytt namn eller fått nytt personnummer efter att e-legitimationen utfärdats. Av lydelsen följer att en felaktighet av mindre betydelse inte behöver leda till återkallelse och spärr av e-legitimationen.

Exempel på situationer som omfattas av *tredje punkten* är när bedräglig användning av e-legitimationen rör ett stort antal användare, liksom när det är fråga om att en enskild e-legitimation används på ett sätt som gör att misstanke om bedräglig användning uppstår.

Av 25 § första stycket 3 förvaltningslagen (2017:900) framgår att en myndighets beslut får meddelas omedelbart utan föregående kom-

munikation med parten om ett väsentligt allmänt eller enskilt intresse kräver det. Ett beslut om återkallelse bör därför ofta kunna fattas utan att innehavaren av en statlig e-legitimation underrättas i förväg.

Att en e-legitimation inte aktiverats inom sex månader efter ansökan eller att innehavaren är avliden utgör också grund för återkallelse enligt *punkterna fyra* och *fem*.

En statlig e-legitimation som har återkallats ska inte längre kunna användas och ska därför spärras elektroniskt.

Om en innehavare inte längre vill använda den statliga e-legitimationen ska e-legitimationen, upphöra att gälla och spärras. Detta följer av *andra stycket*.

Det är inte möjligt att aktivera en tidigare återkallad och spärrad statlig e-legitimation på nytt. Om innehavaren önskar återfå en statlig e-legitimation måste ett nytt ansökningsförfarande initieras.

13 § Om ett statligt medel för elektronisk identifiering tidigare har utfärdats till sökanden ska det spärras senast i samband med att ett nytt sådant medel utfärdas.

I paragrafen uppställs krav på att en tidigare utfärdad statlig e-legitimation ska spärras innan en ny får utfärdas. Övervägandena finns i avsnitt 7.7.2.

14 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om förfarandet vid spärr av statligt medel för elektronisk identifiering.

Paragrafen innehåller en upplysningsbestämmelse om föreskriftsrätt. Övervägandena finns i avsnitten 7.1 och 7.7.2.

Behandling av personuppgifter

15 § Bestämmelserna i 16, 17, 19–23 och 25 §§ samt föreskrifter som meddelats enligt 18 och 24 §§ i denna lag kompletterar Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), här benämnd EU:s dataskyddsförordning.

Vid behandling av personuppgifter enligt denna lag gäller lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning och före-

skrifter som har meddelats i anslutning till den lagen, om inte annat följer av 16–25 §§ eller föreskrifter som meddelats i anslutning till dessa paragrafer.

I paragrafen anges hur däri hänvisade lagrum förhåller sig till EU:s dataskyddsförordning och lagen med kompletterande bestämmelser till EU:s dataskyddsförordning samt föreskrifter som meddelats i anslutning till sistnämnda författning. Övervägandena finns i avsnitten 7.11.1 och 7.11.3.

EU:s dataskyddsförordning är direkt tillämplig i varje medlemsstat. Det innebär att den automatiskt är en del av den svenska rättsordningen. I vissa avseenden förutsätter eller tillåter dataskyddsförordningen emellertid att medlemsstaterna inför bestämmelser som kompletterar förordningen, antingen i form av preciseringar eller i form av undantag.

I 16–25 §§ eller i föreskrifter som meddelats i anslutning till dessa paragrafer finns bestämmelser som kompletterar dataskyddsförordningen när den utfärdande myndigheten och de identitetskontrollerande myndigheterna behandlar personuppgifter i verksamheten med den statliga e-legitimationen. Vad som avses med behandling av personuppgifter framgår av artikel 2 i EU:s dataskyddsförordning. De hänvisningar till dataskyddsförordningen som finns i lagen är dynamiska. Det innebär att hänvisningarna avser dataskyddsförordningen i dess vid varje tidpunkt gällande lydelse.

Databas över statligt medel för elektronisk identifiering

16 § Den utfärdande myndigheten ska med hjälp av automatiserad behandling föra en databas med en samling uppgifter om statliga medel för elektronisk identifiering som myndigheten har utfärdat.

Bestämmelsen är utformad efter förebild i 8 § lagen om identitetskort för folkbokförda i Sverige och, i sak, 14 § förordningen om nationellt identitetskort. Övervägandena finns i avsnitt 7.11.5.

17 § En kopia av den ansiktsbild som enligt 9 § ska finnas i ett lagringsmedium i bäraren av det statliga medlet för elektronisk identifiering, och de biometriska uppgifter som tas fram ur ansiktsbilden får behandlas i databasen.

Av paragrafen följer att den ansiktsbild som ska finnas i lagringsmediet i bäraren av den statliga e-legitimationen och de biometriska uppgifter som tas fram ur bilden får lagras i databasen. Bestämmelsen motsvarar delvis 14 § lagen om identitetskort för folkbokförda i Sverige och 16 § 3 förordningen om nationellt identitetskort som anger att ansiktsbilden får sparas. Övervägandena finns i avsnitten 7.11.5 och 7.11.7.

De fingeravtryck som enligt 8 § också ska tas i samband med ansökan, eller de biometriska uppgifter som tas fram ur dessa, får däremot inte sparas i databasen. Dessa uppgifter får enligt 9 § andra stycket bara behandlas tillfälligt. Att ansiktsbilden och de biometriska uppgifterna får behandlas i jämförande syfte i samband med en ny ansökan framgår av 21 och 22 §§ (se även 7 § i den föreslagna förordningen om elektronisk identifiering).

Med biometriska uppgifter avses enligt definitionen i artikel 4.14 i EU:s dataskyddsförordning personuppgifter som erhållits genom en särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar identifieringen av denna fysiska person, såsom ansiktsbilder eller fingeravtrycksuppgifter. Behandling av fotografier anses dock inte utgöra behandling av biometriska uppgifter annat än när de behandlas med särskild teknik som möjliggör identifiering eller autentisering av en fysisk person, exempelvis i ett ansiktsigenkänningsprogram. Genom bestämmelsen om att biometriska uppgifter som kan tas fram ur ansiktsbilden ska sparas i databasen möjliggörs sökning på de ansiktsbilder som finns i där.

18 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om

1. vilka uppgifter databasen ska eller får innehålla, och
2. den längsta tid som personuppgifter får behandlas i databasen.

Paragrafen innehåller en upplysningsbestämmelse om föreskriftsrätt avseende vilka ytterligare uppgifter som ska finnas i den utfärdande myndighetens databas och hur länge som personuppgifter däri får behandlas. Övervägandena finns i avsnitten 7.11.5 och 7.11.8.

Sådana föreskrifter finns i 14–16 §§ i den föreslagna förordningen om elektronisk identifiering.

Personuppgiftsansvar

19 § Den utfärdande myndigheten är personuppgiftsansvarig för den behandling av personuppgifter som sker i samband med ansökan om och utfärdandet av ett statligt medel för elektronisk identifiering.

Den identitetskontrollerande myndigheten är personuppgiftsansvarig för den behandling av personuppgifter som sker i samband med att myndigheten kontrollerar att sökandes identitet är styrkt enligt 7 §.

Paragrafen innehåller bestämmelser om personuppgiftsansvar. Övervägandena finns i avsnitt 7.11.2.

Av *första stycket* framgår att den myndighet som enligt 16 § för en databas över statliga e-legitimationer är personuppgiftsansvarig för behandlingen av personuppgifter i databasen. Vilken myndighet som ska utfärda den statliga e-legitimationen samt föra databasen över dessa och därmed ha personuppgiftsansvaret, bestäms enligt 4 § av regeringen . Som framgår av 2 § i den föreslagna förordningen om elektronisk identifiering är Myndigheten för digital förvaltning ansvarig för denna myndighetsuppgift.

Personuppgiftsansvaret innebär ett ansvar för att behandlingen stämmer överens med dataskyddsförordningen och de kompletterande bestämmelser till denna som finns i nationell rätt, dvs. i den generella regleringen i dataskyddslagen, i denna lag och i föreskrifter som meddelats med stöd av dessa lagar.

I *andra stycket* anges att den identitetskontrollerande myndigheten är personuppgiftsansvarig för den behandling av personuppgifter som krävs för kontrollen av att sökandens identitet är styrkt. Vilken eller vilka myndigheter som ska utföra den föreskriva identitetskontrollen, och därmed ha personuppgiftsansvaret, bestäms av regeringen enligt 7 § (se även 3 § i den föreslagna förordningen om elektronisk identifiering).

Varje myndighet ansvarar alltså själv för den behandling av personuppgifter som sker inom ramen för myndighetens verksamhet. Bestämmelsen gäller bl.a. för behandlingen av fingeravtryck, eftersom den inte sker i databasen över e-legitimationerna.

Den identitetskontrollerande myndigheten ska dock även samla in och för den utfärdande myndighetens räkning registrera nödvändiga uppgifter om sökanden i samband med ansökan om e-legitimation. För denna behandling är den identitetskontrollerande myndigheten personuppgiftsbiträde åt den utfärdande myndigheten.

Ändamål

20 § Personuppgifter får behandlas av den utfärdande myndigheten om det är nödvändigt för att

1. handlägga ärenden om statligt medel för elektronisk identifiering
2. administrera en databas över innehavare av statliga medel för elektronisk identifiering, och
3. möjliggöra en säker användning av statliga medel för elektronisk identifiering.

Personuppgifter får behandlas av den identitetskontrollerande myndigheten om det är nödvändigt för att, i samband med ansökan, kunna kontrollera den sökandes identitet.

Personuppgifter som har samlats in enligt första stycket får också behandlas av den utfärdande myndigheten

1. om det är nödvändigt för att tillhandahålla information som behövs i Polismyndighetens verksamhet för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa uppbörd eller upprätthålla allmän ordning och säkerhet,
2. om det är nödvändigt för att fullgöra uppgiftsutlämnande som sker i överensstämmelse med lag eller förordning, och
3. för andra ändamål, under förutsättning att uppgifterna inte behandlas på ett sätt som är oförenligt med det ändamål för vilket uppgifterna samlades in.

I paragrafen anges de ändamål för vilka personuppgifter får behandlas. Ändamålsbestämmelsen omfattar all behandling av personuppgifter i verksamheten med tillhandahållandet av en statlig e-legitimation, och inte endast den som sker i den databas som den utfärdande myndigheten har rätt att föra enligt 16 §. Övervägandena finns i avsnitt 7.11.4.

Det huvudsakliga ändamålet med behandlingen är, som framgår av *första stycket*, att den är nödvändig i den utfärdande myndighetens verksamhet för utfärdande av en statlig e-legitimation, och för att möjliggöra en säker användning av sådan e-legitimation. Detta är de primära ändamålen. Personuppgifter får både samlas in och vidarebehandlas för dessa ändamål. Bestämmelsen motsvarar det som gäller för befintliga identitetshandlingar enligt (delvis) 12 § första stycket lagen om identitetskort för folkbokförda i Sverige respektive 15 § förordningen om nationellt identitetskort.

Andra stycket innehåller en ändamålsbestämmelse för den identitetskontrollerande myndighetens behandling av personuppgifter.

Att behandlingen ska vara nödvändig för ändamålet innebär inte ett krav på att behandlingsåtgärden ska vara oundgänglig för ändamålet. Det unionsrättsliga begreppet nödvändig har inte en så strikt inne-

börd. Behandlingen kan anses nödvändig, och därmed tillåten, om behandlingen leder till effektivitetsvinster. Att behandlingen skulle kunna ske manuellt, dvs. utan tekniska hjälpmedel, medför därför normalt inte att automatisk behandling inte anses nödvändig.

I *tredje stycket* regleras de sekundära ändamålen för behandling av personuppgifterna. Endast sådana uppgifter som redan har samlats in för de ändamål som anges i första och andra styckena får behandlas för dessa ändamål. Det är alltså inte tillåtet att samla in personuppgifter för dessa ändamål.

Personuppgifter som behandlas i verksamheten med den statliga e-legitimationen får enligt *första punkten* även behandlas för att tillhandahålla Polismyndigheten information om det är nödvändigt för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa uppbörd eller upprätthålla allmän ordning och säkerhet. Ändamålen motsvarar 1 kap. 1 § lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område. Vid den fortsatta behandlingen för dessa ändamål gäller den lagen och brottsdatalagen (2018:1177).

För de myndigheter som jämte Polismyndigheten har ansvar för brottsbekämpningen, kan det också finnas behov av att ta del av uppgifter i databasen för statliga e-legitimationer. Dessa myndigheter kan i förekommande fall få del av uppgifterna med stöd av *andra punkten* som föreskriver att de får vidarebehandlas, om det behövs för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning, se även avsnitt 7.12. Bestämmelsen motsvarar 12 § andra stycket lagen om identitetskort för folkbokförda i Sverige.

Att uppgiftslämnandet ska ske i överensstämmelse med lag eller förordning innebär att det ska ske med stöd av bestämmelser som antingen påbjuder eller tillåter utlämnande. Bestämmelser om uppgiftslämnande finns t.ex. i 6 kap. 5 § offentlighets- och sekretesslagen (2009:400). I bestämmelsen finns en allmän skyldighet för en myndighet att på begäran av en annan myndighet lämna ut uppgifter som inte omfattas av sekretess, om det inte skulle hindra arbetets behöriga gång.

I *tredje punkten* erinras om att finalitetsprincipen därutöver gäller vid behandling av personuppgifter enligt lagen. Principen innebär att personuppgifter inte får behandlas på ett sätt som är oförenligt med de ändamål för vilka uppgifterna samlades in. Bestämmelsen är utformad i nära anslutning till artikel 5.1 b i dataskyddsförordningen

och ska ges en tolkning som har stöd i förordningen. Det innebär bl.a. att behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 i förordningen inte ska anses vara oförenlig med insamlingsändamålen.

Behandling av känsliga personuppgifter

21 § Personuppgifter som avses i artikel 9.1 i EU:s dataskyddsförordning (känsliga personuppgifter) får behandlas endast om det är absolut nödvändigt för ändamålet med behandlingen.

Känsliga personuppgifter får dock behandlas

1. i databasen när det är tillåtet enligt 17 § och föreskrifter som meddelats enligt 18 §, och
2. vid sökning som är tillåten enligt 22 §.

Paragrafen, som reglerar när känsliga personuppgifter får behandlas, är utformad efter förebild i motsvarande förslag till ny passdatalag i promemorian Ds 2019:5. Övervägandena finns i avsnitt 7.11.7. Känsliga personuppgifter får enligt dataskyddsförordningen inte behandlas. Undantag från förbudet kan dock tillåtas om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse. Förevarande paragraf utgör en kompletterande bestämmelse till dataskyddsförordningen (se 15 §).

Med känsliga personuppgifter avses sådana särskilda kategorier av personuppgifter som anges i artikel 9.1 i dataskyddsförordningen, dvs. personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning. Med hänsyn till den restriktivitet som ligger i uttrycket ”absolut nödvändigt” måste behovet av att behandla uppgifterna prövas noggrant i varje enskilt fall.

I vissa fall kan bestämmelserna i förevarande lag (t.ex. 8 §) medföra att uppgifter som avslöjar ras eller etniskt ursprung behandlas, eftersom en kombination av t.ex. ansiktsbild samt uppgifter om namn kan anses avslöja en persons ras eller etniska ursprung. Vidare behöver biometriska uppgifter som tas fram ur fingeravtryck och ansiktsbilder behandlas. Behandlingen av nämnda uppgifter är tillåten

enligt *första stycket* under förutsättning att behandlingen är absolut nödvändig för ändamålet.

Uppgifter som avslöjar politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i en fackförening, genetiska uppgifter och uppgifter om en persons sexualliv eller sexuella läggning får däremot inte behandlas i verksamheten. Sådana uppgifter är inte nödvändiga för att ärenden om statlig e-legitimation ska kunna handläggas och får därför inte samlas in med stöd av föreskrifter som meddelats enligt 18 § första stycket 1. Om en enskild ändå lämnar in sådana uppgifter får de behandlas bara på de sätt som är absolut nödvändiga.

Av *andra stycket* framgår att känsliga personuppgifter i vissa fall får behandlas utan någon prövning av om behandlingen är absolut nödvändig för ändamålet. Enligt *första punkten* får känsliga personuppgifter alltid behandlas när det är tillåtet enligt 17 § och föreskrifter som meddelats enligt 18 § 1, dvs. bestämmelser som reglerar innehållet i databasen. Av 14 § i den föreslagna förordningen om elektronisk identifiering följer bl.a. att databasen ska innehålla sådana biometriska uppgifter som har tagits fram ur ansiktsbilder. Enligt *andra punkten* får känsliga personuppgifter alltid behandlas vid sökningar som är tillåtna enligt 22 § förevarande lag, dvs. i samband med ansökan om en statlig e-legitimation och endast för att kontrollera sökandens identitet och eventuell tidigare förekomst i databasen.

Integritetshöjande och säkerhetshöjande åtgärder

22 § Det är förbjudet att använda ansiktsbilder samt biometriska uppgifter som har tagits fram ur sådana bilder som sökbegrepp. Trots förbudet får den ansiktsbild som tas enligt 8 §, och de biometriska uppgifter som tas fram ur ansiktsbilden, användas vid sökning i databasen i samband med ansökan om medel för elektronisk identifiering. Sökning är då tillåten endast för att kontrollera sökandens identitet och innehav av sådant medel.

Sådana övriga känsliga personuppgifter som avses i 21 § och uppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden får inte användas som sökbegrepp.

I paragrafen föreskrivs begränsningar och förbud för att som sökbegrepp i databasen använda ansiktsbilden, biometriska uppgifter som tagits fram ur den samt känsliga personuppgifter och vissa uppgifter kopplade till lagöverträdelser och liknande. Motsvarande reg-

lering i detta avseende finns i 17 § lagen om identitetskort för folkbokförda i Sverige. Övervägandena finns i avsnitt 7.11.7.

Bestämmelsen i *första stycket* innebär att ansiktsbilder och biometriska uppgifter som tagits ur sådan bild inte får användas som sökbegrepp vid sökning med hjälp av automatiserad behandling i databasen. Detta förbud är dock inte absolut enligt förevarande paragraf. Sådan sökning bland ansiktsbilderna i databasen är tillåten i samband med att en ansökan om statlig e-legitimation görs, men endast i detta fall. En jämförelse kan på så sätt göras mellan sökanden och en bild som tagits tidigare av henne eller honom och som finns i databasen. Ansiktsbilderna fyller således en viktig funktion i den identitetsbedömning som görs i samband med utfärdande av e-legitimationen. Genom att jämföra sökanden med ansiktsbilden som finns i databasen kan en bedömning göras av om det är samma person. Att sökandens ansikte jämförs med samtliga ansiktsbilder i databasen kan även förhindra att samma person skaffar sig flera identitetshandlingar med olika identiteter.

Någon motsvarande begränsning att använda fingeravtryck som sökbegrepp krävs inte eftersom det av 9 § andra stycket framgår att fingeravtryck överhuvudtaget inte får behandlas i databasen.

Bestämmelsen i *andra stycket* innebär ett förbud mot att använda andra känsliga personuppgifter än de som avses i första stycket, och uppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden som sökbegrepp vid sökning i databasen.

23 § Tillgången till personuppgifter ska begränsas till det som var och en behöver för att kunna fullgöra sina arbetsuppgifter.

I paragrafen regleras tillgången till personuppgifter inom såväl den utfärdande som den identitetskontrollerande myndigheten. Övervägandena finns i avsnitt 7.11.10.

Anställda och andra personer som deltar i verksamheten ska enligt bestämmelsen inte ges tillgång till andra eller fler personuppgifter än vad som behövs med hänsyn till deras arbete. Det är respektive myndighet som i egenskap av personuppgiftsansvarig ansvarar för att avgöra vilka personuppgifter varje person behöver ha tillgång till för att kunna fullgöra sina arbetsuppgifter. Tillgången till personuppgifter kan begränsas genom tekniska och organisatoriska åtgärder

24 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela

1. närmare föreskrifter om tillgången till personuppgifter, och
2. ytterligare föreskrifter om säkerhetsåtgärder till skydd för personuppgifter.

Paragrafen innehåller en upplysningsbestämmelse om föreskriftsrätt i form av verkställighetsföreskrifter. I bestämmelsen anges också att regeringen eller den myndighet som regeringen bestämmer kan meddela ytterligare föreskrifter om säkerhetsåtgärder till skydd för personuppgifter. Det finns alltså ett utrymme för regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om andra säkerhetsåtgärder än den som framgår av 23 §.

Övervägandena finns i avsnitt 7.11.10.

Rätten att göra invändningar

25 § Artikel 21.1 i EU:s dataskyddsförordning om rätten att göra invändningar gäller inte vid sådan behandling som är tillåten enligt denna lag eller föreskrifter som har meddelats i anslutning till lagen.

Paragrafen innehåller en begränsning av den registrerades rätt att göra invändningar enligt artikel 21.1 i EU:s dataskyddsförordning, som är gjord med stöd av artikel 23 i samma förordning. Bestämmelsen är utformad efter förebild i 18 § lagen om identitetskort för folkbokförda i Sverige. Övervägandena finns i avsnitt 7.11.11.

Vid sådan behandling av personuppgifter som är tillåten enligt lagen eller föreskrifter som har meddelats i anslutning till den gäller alltså inte rätten att göra invändningar enligt dataskyddsförordningen. Bestämmelsen omfattar all behandling av personuppgifter som är tillåten enligt lagen eller föreskrifter som meddelats i anslutning till den och inte endast den som sker i databasen för statliga e-legitimationer.

Krav på erkännande av vissa medel för elektronisk identifiering

26 § När medel för elektronisk identifiering krävs för att få tillgång till en nättjänst som tillhandahålls av en offentlig aktör, och tjänsten helt eller delvis riktar sig till privatpersoner, ska medel erkännas för autentisering för tjänsten om

1. medlet för elektronisk identifiering tillhandahålls av leverantör som är godkänd i enlighet med lagen (20XX:XXX) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post, och
2. tillitsnivån för medlet för elektronisk identifiering motsvarar en tillitsnivå som är lika hög eller högre än den tillitsnivå som den offentliga aktören kräver för åtkomst till nättjänsten.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om
1. vilka typer av tjänster för elektronisk identifiering som kravet i första stycket avser,
2. hur skyldigheten ska fullgöras, och
3. undantag från kravet.

I paragrafen uppställs krav om att de offentliga aktörer som definieras i 4 § i sina nättjänster ska erkänna vissa medel för elektronisk identifiering. Övervägandena finns i avsnitten 7.13.4–7.13.6.

Bestämmelsen i *första stycket* innebär att när e-legitimation krävs för att få tillgång till en digital tjänst som tillhandahålls av en offentlig aktör, och tjänsten helt eller delvis riktar sig till privatpersoner, ska en e-legitimation erkännas för autentisering för tjänsten, om de angivna rekvisiten är uppfyllda. Att tjänsten riktar sig helt eller delvis till privatpersoner innebär att kravet inte omfattar digitala tjänster som avses att användas av personer inom ramen för deras yrkesutövning eller för tjänster inom utbildningsområdet där identifiering uteslutande sker med särskilda e-legitimationer som utfärdas till elever eller studenter. Endast sådana digitala tjänster där autentisering med e-legitimationer krävs omfattas av kravet.

Det som anges i första styckets *första punkt* innebär att kravet endast omfattar de e-legitimationer som tillhandahålls av leverantör som är godkänd i enlighet med den föreslagna lagen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post.

Av första styckets *andra punkt* följer att kravet på erkännande endast gäller om tillitsnivån för e-legitimationen motsvarar en tillitsnivå som är lika hög eller högre än den tillitsnivå som den offentliga aktören kräver för åtkomst till den digitala tjänsten. Kravet gäller vidare endast sådana digitala tjänster där identifiering sker med e-legitimation.

Av *andra stycket* framgår att regeringen eller den myndighet som regeringen bestämmer kan meddela ytterligare föreskrifter om vilka typer av tjänster för elektronisk identifiering som kravet i första stycket avser, hur skyldigheten ska fullgöras samt besluta om undantag från

kravet. En omständighet som kan medföra att undantag från kravet aktualiseras är exempelvis att det för en viss myndighets verksamhet är påkallat med hänsyn till rikets säkerhet.

Användning av statligt medel för elektronisk identifiering

27 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om villkor för när och hur ett statligt medel för elektronisk identifiering får användas.

Paragrafen innehåller ett bemyndigande för regeringen eller den myndighet regeringen bestämmer att föreskriva villkor för användningen av den statliga e-legitimationen. Övervägandena finns i avsnitt 7.8.

De krav som avses är t.ex. sådana som kan behövas för att säkerställa att den statliga e-legitimationen inte används i oseriösa sammanhang och att biometriska uppgifter får eller ska användas som extra kontroll i samband med id-växling eller vid betalningstransaktioner över visst belopp. Det kan också vara fråga om att uppställa krav på innehavare av en statlig e-legitimation att skydda e-legitimationen och dess tillhörande behörighetsfunktioner.

Övriga bestämmelser

28 § Beslut enligt denna lag får överklagas till allmän förvaltningsdomstol. Prövningstillstånd krävs vid överklagande till kammarrätten.

I paragrafen föreskrivs att beslut enligt lagen får överklagas till allmän förvaltningsdomstol och att det krävs prövningstillstånd vid överklagande till kammarrätten. Övervägandena finns i avsnitt 7.4.2. Paragrafen motsvarar 19 § lagen om identitetskort för folkbokförda i Sverige och 22 § förordningen om nationellt identitetskort, i vilken det hänvisas till bestämmelsen om överklagande i 40 § förvaltningslagen.

29 § Beslut enligt denna lag gäller omedelbart, om inte något annat anges i beslutet.

Paragrafen motsvarar 20 § lagen om identitetskort för folkbokförda i Sverige och i sak 23 § förordningen om nationellt identitetskort. Övervägandena finns i avsnitt 7.4.2.

Ikraftträdande

Denna lag träder i kraft den 1 mars 2026.

Bestämmelsen föreskriver när lagen ska träda i kraft. Övervägandena finns i kapitel 8.

10.2 Förslaget till lag om ändring i förslag till lag om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post

2 §

Med ett *auktorisationssystem* avses i denna lag ett system där

1. den myndighet som tillhandahåller systemet godkänner att leverantörer av tjänster för elektronisk identifiering av enskilda eller för digital post får ingå ett avtal inom systemet och ingår avtal med var och en av de godkända leverantörerna om utförande av sådana tjänster,
2. en enskild har rätt att välja den leverantör som ska utföra tjänsterna för den enskildes räkning,
3. en *sådan* offentlig aktör *som avses i 4 § första stycket 1–3 a ska* använda tjänsterna *för elektronisk identifiering och kan använda tjänsterna för digital post* i sin verksamhet enligt avtal med den tillhandahållande myndigheten, *och*
4. *en sådan offentlig aktör som avses i 4 § första stycket 3 b–5 och andra stycket kan använda tjänsterna i sin verksamhet enligt avtal med den tillhandahållande myndigheten*.

I paragrafen anges vad som avses med ett auktorisationssystem.

I tredje punkten anges att en sådan offentlig aktör som avses i 4 § första stycket 1–3 a ska använda tjänsterna för elektronisk identifiering i sin verksamhet. Övervägandena finns i avsnitten 7.13.4 och 7.13.5.

23 §

Regeringen eller den myndighet som regeringen bestämmer får besluta om undantag från skyldigheten i 2 § 3.

I paragrafen bemyndigas regeringen eller den myndighet som regeringen bestämmer att få besluta om undantag från skyldigheten i 2 § 3. Övervägandena finns i avsnitt 7.13.6.

Vad gäller situationer då undantag från kravet kan aktualiseras kan detta exempelvis föranledas av att vissa myndigheter bör undantas med hänsyn till rikets säkerhet. Det kan även ske för att berörda aktörer inte ska hamna i en situation där tidigare ingångna avtal löper parallellt med kravet. Det kan vidare bli aktuellt om de godkända leverantörerna i auktorisationssystemen enbart representerar en begränsad krets av användare.

Ikraftträdande

Denna lag träder i kraft den 1 mars 2026.

Bestämmelsen föreskriver när lagen ska träda i kraft. Övervägandena finns i kapitel 8.

10.3 Förslaget till förordning om elektronisk identifiering

Förordningens innehåll

1 § Denna förordning innehåller bestämmelser som kompletterar lagen (20XX:XXX) om elektronisk identifiering.

Ord och uttryck som används i denna förordning har samma betydelse som i lagen.

Övervägandena finns i avsnitt 7.1.

Utfärdande och identitetskontrollerande myndigheter

2 § Myndigheten för digital förvaltning är utfärdande myndighet av statligt medel för elektronisk identifiering.

Övervägandena finns i avsnitt 7.6.3.

3 § Myndigheten X är identitetskontrollerande myndighet för ansökningar om statligt medel för elektronisk identifiering som görs inom riket.

Regeringskansliet får besluta i vilken utsträckning beskickningar och karriärkonsulat ska fullgöra uppgifter som identitetskontrollerande myndighet i fråga om ansökningar om statligt medel för elektronisk identifiering

som görs utom riket. Regeringskansliet får också besluta att ett honorärkonsulat i begränsad utsträckning ska fullgöra sådana uppgifter.

Övervägandena finns i avsnitt 7.6.2.

Ansökan om och utfärdande av statligt medel för elektronisk identifiering

4 § Ansökan om statligt medel för elektronisk identifiering ska göras hos en identitetskontrollerande myndighet.

Den identitetskontrollerande myndigheten ska registrera nödvändiga uppgifter i den databas för statliga medel för elektronisk identifiering som den utfärdande myndigheten har rätt att föra enligt lagen (20XX:XXX) om elektronisk identifiering.

Övervägandena finns i avsnitten 7.4.2 och 7.11.5.

5 § Sökanden är skyldig att inställa sig personligen.

Om sökanden är under arton år ska sökanden ge in ett skriftligt medgivande från hans eller hennes vårdnadshavare, om det inte finns synnerliga skäl att ändå utfärda ett statligt medel för elektronisk identifiering.

I fråga om barn som är under arton år ska en handling som styrker uppgift om vem som är vårdnadshavare uppvisas, om denna uppgift inte framgår av för den identitetskontrollerande myndighetens tillgängliga uppgifter.

Övervägandena finns i avsnitten 7.4.2 och 7.5.

6 § För personer som av fysiska skäl är permanent förhindrade att lämna fingeravtryck gäller undantag från skyldigheten i 8 § lagen (20XX:XXX) om elektronisk identifiering att låta den identitetskontrollerande myndigheten ta den sökandes fingeravtryck.

Övervägandena finns i avsnitt 7.5.

7 § Om en sökande för att styrka sin identitet uppvisar en identitetshandling som är försedd med ett fotografi av innehavarens ansikte eller innehåller ett lagringsmedium där fingeravtryck eller ansiktsbild är sparade, får den identitetskontrollerande myndigheten kontrollera att dessa motsvarar fingeravtryck och ansiktsbild som enligt 8 § lagen (20XX:XXX) ska tas av sökanden vid ansökningstillfället.

När en kontroll enligt första stycket har genomförts, ska fingeravtrycken och de biometriska data som då har tagits fram omedelbart förstöras.

Övervägandena finns i avsnitten 7.5 och 7.11.7.

8 § Ett statligt medel för elektronisk identifiering ska finnas på ett kontaktlöst kort och ska utfärdas på tillitsnivå hög enligt artikel 8.2 c i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, här benämnd EU:s förordning om elektronisk identifiering.

Ett kort enligt första stycket ska antingen vara en certifierad anordning för skapande av kvalificerade elektroniska underskrifter som avses i artikel 3.12 i EU:s förordning om elektronisk identifiering, eller kunna certifieras som en sådan anordning.

Ett medel för elektronisk identifiering ska innehålla efternamn, förnamn, namn som visas för användaren, och personnummer enligt folkbokföringslagen (1991:481), alternativt samordningsnummer för personer med styrkt identitet enligt lagen (2022:1697) om samordningsnummer.

Övervägandena såvitt avser *första* och *tredje styckena* finns i avsnitten 7.2.2 och 7.4.1 respektive 7.2.3, samt i avsnitt 7.3 såvitt avser *andra stycket*.

9 § Myndigheten X får, efter att ha hört Regeringskansliet (Utrikesdepartementet), meddela de ytterligare föreskrifter som behövs för verkställigheten av kontrollen att en sökande har styrkt sin identitet enligt 6 § lagen (20XX:XXX) om medel för elektronisk identifiering när det gäller ansökan om sådant medel som görs inom riket.

Regeringskansliet får, efter att ha hört Myndigheten X, meddela motsvarande föreskrifter för sådana identitetskontrollerande myndigheter utom riket som avses enligt denna förordning.

Myndigheten för digital förvaltning får med stöd av 8 kap. 7 § regeringsformen meddela de ytterligare föreskrifter som behövs för verkställigheten av denna förordning.

Övervägandena finns i avsnitten 7.4.2 och 7.5.

Utlämnande av statligt medel för elektronisk identifiering

10 § Om ansökan bifalls av den utfärdande myndigheten, ska den identitetskontrollerande myndigheten skyndsamt lämna ut medlet för elektronisk identifiering till sökanden personligen.

Övervägandena finns i avsnitt 7.4.2.

Giltighetstid samt återkallelse och spärr

11 § Ett statligt medel för elektronisk identifiering ska utfärdas med en giltighetstid av högst fem år.

12 § För sökande som av fysiska skäl är tillfälligt förhindrade att lämna fingeravtryck ska det statliga medlet för elektronisk identifiering ges giltighet endast så lång tid som det fysiska hindret förväntas bestå. Giltighetstiden får dock inte överstiga sju månader.

13 § Myndigheten för digital förvaltning får meddela ytterligare föreskrifter om begränsning av giltighetstiden i särskilt angivna fall.

Övervägandena till 11–13 §§ finns i avsnitt 7.7.1.

Behandling av personuppgifter

14 § Den databas som Myndigheten för digital förvaltning ska föra enligt lagen (20XX:XXX) om elektronisk identifiering ska innehålla

1. sökandens fullständiga namn, personnummer alternativt samordningsnummer, födelsetid, och behövliga kontaktuppgifter,
2. kopia av den ansiktsbild som tagits vid ansökan och biometriska uppgifter som tagits fram ur ansiktsbilderna,
3. dagen för utfärdandet av det statliga medlet för elektronisk identifiering samt dess giltighetstid och status,
4. unik identifierare för det statliga medlet för elektronisk identifiering och dess serienummer,
5. aktiveringskod,
6. kondensat av innehavarens personliga kod,
7. uppgift om hur sökanden har styrkt sin identitet,
8. uppgift om att ansökan har avslagits och skälen för detta beslut, och
9. uppgift om att det statliga medlet för elektronisk identifiering har återkallats och spärrats, samt vad som har utgjort skäl för återkallelsen.

En handling som har kommit in eller upprättats i ett ärende får behandlas i databasen.

Övervägandena finns i avsnitt 7.11.5.

15 § Databasen som avses i 14 § får tillföras sådana uppgifter från Skatteverkets folkbokföringsdatabas som anges i 14 § första stycket 1.

Övervägandena finns i avsnitten 7.4.2 och 7.11.5.

16 § Uppgifter och handlingar vilka finns i databasen som avses i 14 § ska gallras senast tio år efter utgången av det kalenderår då det ärende som uppgifterna eller handlingarna hänför sig till avslutades.

Riksarkivet får, efter att ha inhämtat synpunkter från Myndigheten för digital förvaltning, meddela föreskrifter om

1. att uppgifter och handlingar får bevaras för arkivändamål av allmänt intresse eller vetenskapliga, statistiska eller historiska ändamål under längre tid än som anges första stycket, och

2. avskiljande och begränsningar av åtkomsten till uppgifter och handlingar som bevaras för sådana ändamål som anges i 1.

Övervägandena finns i avsnitt 7.11.8.

17 § En innehavare av ett statligt medel för elektronisk identifiering har rätt att hos den identitetskontrollerande myndigheten kontrollera den information som har sparats i lagringsmediet på bäraren av det medlet för elektronisk identifiering.

Övervägandena finns i avsnitt 7.2.6.

18 § Myndigheten för digital förvaltning får meddela närmare föreskrifter om

1. tillgången till personuppgifter inom myndigheten, och

2. andra säkerhetsåtgärder till skydd för personuppgifter inom myndigheten.

Myndigheten X får meddela närmare föreskrifter om

1. tillgången till personuppgifter inom myndigheten, och

2. andra säkerhetsåtgärder till skydd för personuppgifter inom myndigheten.

Regeringskansliet (Utrikesdepartementet) får meddela närmare föreskrifter om

1. tillgången till personuppgifter inom sådana identitetskontrollerande myndigheter utom riket som avses enligt denna förordning, och

2. andra säkerhetsåtgärder till skydd för personuppgifter inom sådana identitetskontrollerande myndigheter utom riket som avses enligt denna förordning.

Övervägandena finns i avsnitt 7.11.10.

Krav på erkännande av vissa medel för elektronisk identifiering

19 § Myndigheten för digital förvaltning får meddela föreskrifter om
1. vilken typ av tjänster som kravet i 26 § första stycket lagen (20XX:XXX) om elektronisk identifiering avser,
2. hur skyldigheten ska fullgöras, och
3. undantag från kravet.

Övervägandena finns i avsnitten 7.13.5 och 7.13.6.

Ansökningsavgift

20 § För prövning av ansökan om statligt medel för elektronisk identifiering ska sökanden betala en ansökningsavgift på 400 kronor. Avgiften ska betalas i samband med ansökan. Om avgiften inte är betald då tillämpas bestämmelserna i 11 § avgiftsförordningen (1992:191). För prövning av ansökan tillämpas i övrigt bestämmelserna i 12–14 §§ avgiftsförordningen.

Övervägandena finns i avsnitt 7.9.

Ikraftträdande

Denna förordning träder i kraft den 1 mars 2026.

Bestämmelsen föreskriver när förordningen ska träda i kraft. Övervägandena finns i kapitel 8.

10.4 Förslaget till förordning om ändring i offentlighets- och sekretessförordningen (2009:641)

6 §

Sekretess gäller i nedan angiven verksamhet, som avser registrering av betydande del av befolkningen, för
1. uppgift om en enskilds personliga förhållanden, om det av särskild anledning kan antas att den enskilde eller någon närstående till honom eller henne lider men om uppgiften röjs, och
2. uppgift i form av fotografisk bild av den enskilde, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider men.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

Verksamheten avser
fastighetsregistret
kommunala fastighetsregister
Myndigheten för digital förvaltnings databas över statliga medel för elektronisk identifiering
passregister och register över nationella identitetskort
röstlängdsregister
Skatteverkets databas över identitetskort för folkbokförda i Sverige
Socialstyrelsens register över legitimerad hälso- och sjukvårdspersonal och personal med bevis om rätt att använda yrkestiteln undersköterska
Statens jordbruksverks register över hund- och kattägare
Statens tjänstepensionsverks pensionsregister
Totalförsvarets plikt- och prövningsverks register över totalförsvarets personal
Transportstyrelsens vägtrafikregister

Övervägandena finns i avsnitt 7.12.

Ikraftträdande

Denna förordning träder i kraft den 1 mars 2026.

Bestämmelsen föreskriver när förordningen ska träda i kraft. Övervägandena finns i kapitel 8.

10.5 Förslaget till förordning om ändring i förordningen (2014:115) med instruktion för utrikesrepresentationen

3 kap.

Identitetskontroll i ärende om statligt medel för elektronisk identifiering

10 b §

Beskickningar och konsulat ska utföra identitetskontroll enligt lagen (20XX:XXX) om elektronisk identifiering.

Övervägandena finns i avsnitt 7.6.2.

Ikraftträdande

Denna förordning träder i kraft den 1 mars 2026.

Bestämmelsen föreskriver när förordningen ska träda i kraft. Övervägandena finns i kapitel 8.

Särskilt yttrande av Ulf Palmgren, Försäkringskassan

Samhället har utmaningar med identiteter generellt och med ett missbruk som inte är försumbart. Detta försvårar för bland andra Försäkringskassan att utföra sitt uppdrag korrekt. Därför behövs en sammanhållen och tillförlitlig identitetsförvaltning. Frågan behöver dock utredas i ett bredare perspektiv.

En statlig utredning måste initieras utifrån ett samlat grepp för hela identitetskedjan: *grundregistrering*, *identifiering*, *verifiering* och *kontroll*. Det är Försäkringskassans uppfattning och i linje med det myndighetsgemensamma arbete som pågår inom ramen för MUR (Motståndskraft hos utbetalande och rättsvårdande myndigheter mot missbruk och brott i välfärden).

Allt syftar till att myndigheterna ska kunna utgå från att en person är den som hen utger sig för att vara.

Balans mellan tillgänglighet och säkerhet

Digital inkludering och tillgänglighet är viktigt för att fler ska kunna använda dagens och framtidens tjänster. Det kräver tillit till de digitala tjänsterna och vetskap om vem som är vem. Det behövs ett holistiskt perspektiv som inkluderar kopplingen mellan grundregistrering, digital identitet och verifiering, och att de hänger ihop så att det inte skapas sårbarheter.

Unika identiteter med biometri som grund

För att förbättra och förstärka den nationella förmågan till unika och tillförlitliga identiteter som kan verifieras måste det gå att koppla ihop den fysiska och den registrerade identiteten. Det behövs därför en nationell infrastruktur med biometriska uppgifter.

Utredning för en sammanhållen hantering baserad på unika identiteter

För att kunna skapa en tillförlitlig, sammanhållen och solid identitetsförvaltning behövs en statlig utredning som utifrån en helhetssyn klargör förutsättningarna för identitetshantering och därtill kopplad lagring och användning av biometriska data.

Nedan följer en kort beskrivning av dagens identitetsprocess för registrering, identifiering, verifiering och kontroll samt utmaningarna med den:

Grundregistrering

En identitet registreras i folkbokföringsregistret. Här är några exempel på hur identitetskontrollen görs vid en grundregistrering.

- Ett barn som föds i Sverige och har en svensk mor får ett personnummer. Hälso- och sjukvården utför identitetskontrollen.
- Ett barn som föds utomlands kan få ett samordningsnummer. En svensk utlandsmyndighet utför då identitetskontrollen.
- En person som får svenskt medborgarskap får ett personnummer. Migrationsverket utför identitetskontrollen.
- En person kan själv begära samordningsnummer av Skatteverket, som utför identitetskontrollen vid en personlig inställelse.
- En myndighet kan rekvirera ett samordningsnummer från Skatteverket. För att samordningsnumret ska få status ”styrkt identitet” måste personen besöka Skatteverket personligen för identitetskontroll.

Utmaningar

En utmaning är att en person kan ha falska id-handlingar och tilldelas flera identiteter i olika namn, vilket sedan kan nyttjas i brottsligt syfte. För att kunna motverka detta behöver biometriska data kunna användas, det vill säga lagrade biometriska uppgifter som kan användas inför grundregistreringen.

En större utmaning är att nummerserien för personnummer och samordningsnummer inte räcker till i dag. Många personer får ett annat datum i sina personnummer eller samordningsnummer än sitt faktiska födelsedatum. Antalet ökar stadigt i takt med att befolkningen ökar. Detta driver också på behovet av att se över hanteringen av hela identitetsområdet.

En annan utmaning är personer med utländsk identitet. Alla e-tjänster kräver inte att personen har svenskt personnummer eller samordningsnummer, utan de ska kunna användas baserat på den utländska identiteten.

Identifiering

För att få en id-handling utfärdad behöver personen kunna visa upp och styrka sin identitet. Detta steg brukar även benämnas *grundidentifiering*. Här krävs goda kunskaper om olika identitetshandlingar och deras säkerhetsdetaljer samt möjlighet att kontrollera giltigheten i register. Det blir dock problem för dem som tilldelats ett samordningsnummer och inte kan uppvisa en svensk id-handling. Många har giltiga utländska id-handlingar, men svårigheten är att med säkerhet fastställa att ett samordningsnummer verkligen tillhör personen som visar upp en utländsk id-handling.

Verifiering

En person ska kunna styrka sin identitet. I den analoga världen ska hen kunna visa upp en id-handling. Sverige saknar en instans som godkänner id-handlingar, så det är upp till berörda myndigheter att avgöra vilka som ska accepteras. Ett exempel är att Systembolaget nu accepterar ett av de två digitala id-kort som finns på marknaden. Bankerna accepterar endast pass och nationella id-kortet i dag. Övriga godtar

fler id-handlingar, till exempel körkort, vid utfärdande av id-handling eller pass.

För e-legitimationer är situationen bättre eftersom det finns en instans i Sverige som granskar och godkänner dessa id-handlingar. I den digitala världen benämns detta steg *autentisering*.

Kontroll

Även om personen har styrkt sin identitet kan den behöva kontrolleras mot olika register, där folkbokföringsregistret har en central roll. Det kan till exempel behövas om personen har status avliden eller avförd.

Särskilt yttrande av Johannes Holmström, Skatteverket

Utredningen Säker och tillgänglig digital identitet har haft i uppdrag att utreda och lämna förslag på hur staten kan utfärda en e-legitimation på högsta tillitsnivå. Syftet är att stärka samhällets säkerhet och robusthet, motverka bedrägerier som kan begås med hjälp av e-legitimationer och underlätta för så många som möjligt att få tillgång till en e-legitimation.

Skatteverket ser positivt på uppdraget och ser ett stort behov av att förstärka infrastrukturen och förutsättningarna för en identitetsförvaltning som stärker möjligheterna till digital inkludering samtidigt som säkerheten ökar. Skatteverket anser dock att ett helhetsperspektiv gällande identitet är en förutsättning för att kunna uppnå angivna effekter. En tillförlitlig, tillgänglig och säker e-legitimation kräver en tillförlitlig kedja av förutsättningar från etablerande av identitet, utfärdande av identitetshandling, verifiering av identitet till förvaltning och kontroll av dessa.

Skatteverket vill därför understryka att det finns flera närliggande frågor som har betydelse för att en sammanhållande infrastruktur för identitetsförvaltning ska fungera tillfredställande. Dessa bör utredas tillsammans med frågan om statlig e-legitimation på hög tillitsnivå.

Området karaktäriseras av en oerhört kraftig utvecklingsintensitet både nationellt och internationellt. Under pågående utredning och pågående arbete inom och i samverkan mellan myndigheter så har kunskapen och förutsättningarna för hur tekniken kan och bör användas hela tiden utvecklats. Det är därav av vikt att belysa att en reglering behöver vara hållbar över tid och ge förutsättningar att följa en hög säkerhets- och tillitsnivå i samklang med hög användarvänlighet.

Skatteverkets uppfattning är att en sådan identitetsförvaltning består av:

- *Etablerande av identitet/användare.* Grundregistreringen av en person och dennes identitet sker i samband med födelse eller flyttning till Sverige. Det förutsätter en hög grad av säkerhet, dvs. att registerhållaren av identiteten kan verifiera att personen är unik i Sverige. Det kan ske på olika sätt men ska registreringen förbli unik med ”en person en identitet” krävs användande av biometri.
- *Upprättande av ID-dokument*. Upprättande, utlämnande och förvaltning av såväl fysiska som digitala identitetsdokument behöver ske på ett tillförlitligt och förutsägbart sätt. Upprättade dokument bör bestå av digital lagring av biometriska kännetecken för unikt utfärdande och verifiering. Kraven på identitetskontroll bör harmoniseras oavsett om det avser en digital eller fysisk identitetshandling.
- *Autentisering- och verifiering av identitet.* För en stark tillit till vem jag interagerar med och att en enskild medborgare ska vara trygg med att deras uppgifter inte nyttjas av någon annan, krävs att tillförlitliga verifieringstjänster av såväl dokument som person, tillgängliggörs och nyttjas brett. Det innebär verifiering och koppling mellan den fysiska personen och identitetsdokumentet.
- *Förvaltning och registerhållning av identitet.* När missbruk, brott eller felaktiga uppgifter om identitet upptäcks krävs möjlighet att rätta, spärra och underrätta om missbruket på ett förenklat och tillgängligt sätt, brett i samhället. Det kräver ett utökat informationsutbyte och förutsättningar för att kunna behandla uppgifter i syfte att verifiera uppgifter, handlingar och biometriska kännetecken. Utöver det krävs tillräckligt med information för användare av identitetsuppgifterna för att bedöma behovet i den enskilda situationen. Vidare finns ett tydligt behov av att stödja brottsoffer som är drabbade av identitetsstöld eller bedrägerier med personuppgifter. Ett förbättrat stöd för en enskild som drabbas behöver det offentliga ta ett tydligare ansvar för.

De frågor som behöver behandlas är således upptagning och lagring av biometri i syfte att kontrollera och verifiera identitet både för privata och offentliga aktörer. Att utreda hur en behandling av biometriska kännetecken som en nationell resurs i syfte att stödja nationell infrastruktur för användande av unika identiteter digitala som analoga kan ske med ökat informationsägarskap, ökad trygghet samtidigt som det kan ske med en tydlig ansvarsfördelning mellan olika aktö-

rer på området. I det föreligger sannolikt behov av att utreda införande av en ny unik identitetskod som en persistent nyckel i ett nationellt identitetsindex i syfte att på ett tillförlitligt sätt separera lagring, användning och förvaltning.

Målet är en mer sammanhållen hantering av identiteter som bygger på unika identiteter och säker verifiering av dessa. Detta ger i sin tur trygghet för användarna att det enbart är jag själv som kan agera som mig såväl digitalt som analogt. En sådan nationell infrastruktur kräver utredning av ett samordnat nationellt identitetsindex i likhet med det som tas fram förslag på i myndighetssamverkan, vilket syftar till att skapa förutsättning för tjänster som bygger på tillit, behörighet, trygghet och säkerhet.

Skatteverkets uppfattning är att när enskilda frågor på identitetsområdet utreds utan ett samlat grepp finns risk för suboptimerade lösningar. Identitet och identifiering bygger på spårbarhet och kontinuitet i uppgifter vid etablering, utfärdande och verifiering. I dag bedöms risken för utnyttjade och kapade identiteter vara mer tongivande än renodlat falska uppgifter. Det medför att kopplingen mellan verifiering och etablering behöver stärkas. Ett införande av biometriska uppgifter som verifiering utan användning av referensdata riskerar att driva enkelhet framför säkerhet och trygghet.

Skatteverkets bedömning är att det föreligger ett tydligt behov av att utreda frågorna på ett mer sammanhållet sätt för att uppnå avsedda effekter. Med utgångspunkt i redan befintlig myndighetssamverkan anser Skatteverket att frågan bör utredas med en bra balans i kompetens avseende områden som juridik, arkitektur, säkerhet och integritet i syfte att nå en reglering som stödjer en hög grad av säkerhet, informationsägarskap, tillgänglighet och med en användarvänlighet som genererar drivkraft till utveckling.

Kommittédirektiv 2022:142

Säker och tillgänglig digital identitet

Beslut vid regeringssammanträde den 22 december 2022

Sammanfattning

En särskild utredare ska utreda och lämna förslag på hur staten kan utfärda en e-legitimation på högsta tillitsnivå. Utredaren ska också se över behovet av anpassningar som följer av den reviderade eIDAS-förordningen. Syftet är att stärka samhällets säkerhet och robusthet, motverka bedrägerier som begås med hjälp av e-legitimationer och underlätta för så många som möjligt att kunna få tillgång till en e-legitimation.

Utredaren ska bl.a.

- lämna förslag på hur en kostnadseffektiv statlig e-legitimation på högsta tillitsnivå kan utformas och tillhandahållas av en statlig myndighet,
- analysera och föreslå förändringar som följer av den reviderade eIDAS-förordningen, och
- lämna nödvändiga författningsförslag.

Uppdraget att föreslå hur staten kan utfärda en e-legitimation på högsta tillitsnivå ska delredovisas senast den 16 oktober 2023. Uppdraget ska slutredovisas senast den 31 maj 2024.

Säker och tillgänglig identifiering i ett digitaliserat samhälle

Den 3 juni 2021 presenterade Europeiska kommissionen ett förslag till Europaparlamentets och rådets förordning om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av en ram för europeisk digital identitet (den reviderade eIDAS-förordningen), COM (2021) 281. Det föreslås bl.a. att det ska bli obligatoriskt för varje medlemsstat att anmäla en e-legitimation på den högsta tillitsnivån enligt ett förfarande för gränsöverskridande identifiering och att varje medlemsstat ska utfärda en europeisk digital identitetsplånbok. Tillitsnivån på e-legitimationen avgör hur tillförlitligt det är att personen som identifierar sig är den man utger sig för att vara. Plånboken ska möjliggöra för fysiska och juridiska personer att på ett säkert sätt bl.a. begära, erhålla, lagra och använda personidentifieringsuppgifter och digitala bevis för autentisering online och off-line samt att skriva under med kvalificerade elektroniska underskrifter.

Den ökade digitaliseringen gör det allt svårare att klara sig i samhället utan tillgång till en e-legitimation. Det är därför viktigt att så många som möjligt ges möjlighet att skaffa en säker e-legitimation. En e-legitimation är i princip nödvändig för att få tillgång till viktiga digitala tjänster och samhällsfunktioner, t.ex. hantera bankärenden eller för att ha kontakt med det offentliga. E-legitimationer har också börjat användas för identifiering exempelvis via telefon eller vid besök. En e-legitimation är alltså viktig för att enskilda ska kunna nyttja samhällets digitala tjänster så att alla enskilda kan ta till vara sina intressen och medborgerliga rättigheter. Detta gäller även för personer som bara tillfälligt vistas i Sverige, exempelvis för arbete.

I dag är det endast privata aktörer som utfärdar e-legitimationer och staten har begränsade möjligheter till insyn och påverkan. Det finns även behov av att utreda alternativa lösningar för e-legitimation utifrån flera perspektiv, särskilt när det gäller säkerhet, redundans och tillgänglighet.

E-legitimationer utgör en samhällsviktig infrastruktur som behöver fungera också om samhället utsätts för en stor påfrestning och ytterst även i krig. Störningar i e-legitimationssystem kan snabbt få kännbara effekter för näringsliv, banker, offentlig sektor och inte minst för enskilda även under i övrigt normala förhållanden.

Uppdraget att föreslå hur staten kan utfärda en e-legitimation på högsta tillitsnivå

Förslagen i revisionen av eIDAS-förordningen ställer krav på medlemsstaterna att anmäla en e-legitimation på högsta tillitsnivå enligt ett särskilt anmälningsförfarande. En anmäld e-legitimation kan därefter användas i andra EU-länders e-tjänster.

Det är viktigt i ett digitalt samhälle att så många som möjligt ges möjlighet att identifiera sig. En säker elektronisk identifiering kan också bidra till att motverka den identitetsrelaterade brottsligheten. Med en säker grundidentifiering som görs av en myndighet vid ett personligt besök minskar risken för att fel person får tillgång till e-legitimationen. En utredning ska analysera vilka kontroller av identiteten som behöver vidtas och om omfattningen av kontrollen ska vara jämförbar med den kontroll som sker för andra identitetshandlingar.

Utgångspunkten är att utfärdande av e-legitimationer på den högsta tillitsnivån bör ske vid en statlig myndighet. En e-legitimation på högsta nivå kan användas för växling till en annan e-legitimation på samma nivå eller en e-legitimation på lägre nivå.

För att en e-legitimation ska kunna användas behövs en bakomliggande digital infrastruktur mot vilken e-legitimationen kan verifieras. En individ kan använda sin e-legitimation flera gånger om dagen. Infrastrukturen behöver därför hantera en stor mängd verifieringar. Myndigheten för digital förvaltning ansvarar för den offentliga förvaltningens tillgång till infrastruktur och tjänster för elektronisk identifiering och underskrift. Eftersom system för e-legitimationer och digital identifiering kräver särskild kompetens bör Myndigheten för digital förvaltning vara den myndighet som får ett eventuellt uppdrag att ta fram en statlig e-legitimation.

2017 års ID-kortsutredning föreslår i sitt betänkande Ett säkert statligt ID-kort – med e-legitimation (SOU 2019:14) att staten ska utfärda en e-legitimation på högsta tillitsnivå. Syftet med förslaget är att ge alla invånare möjlighet att skaffa en säker e-legitimation för att de ska få tillgång till viktiga samhällsfunktioner. Vidare menar utredningen att en säker elektronisk identifiering motverkar den identitetsrelaterade brottsligheten.

Utredningen föreslår att en statlig e-legitimation ska finnas på det statliga identitetskort som enligt förslaget ska utfärdas av Polismyndigheten. Vidare konstaterar utredningen att det inte är möjligt att

uppskatta kostnaderna för bl.a. utveckling och förvaltning av e-legitimationen och lämnar inte heller förslag på en ersättningsmodell för utfärdande och användande av en e-legitimation. Utredningen konstaterade att det finns ett stort behov av alternativa lösningar för e-legitimationer.

Utredningens förslag bereds inom Regeringskansliet. Det är dock tidskrävande att ta fram ett kombinerat id-kort och e-legitimation. Förslagen i den reviderade eIDAS-förordningen i kombination med ett förändrat säkerhetsläge kan medföra vissa krav på skyndsamhet. Det kan därför finnas behov av en alternativ lösning för en e-legitimation på högsta nivå.

En ny utredning bör också analysera hur en e-legitimation kan utformas så att så många som möjligt kan få tillgång till den, exempelvis personer från andra länder som arbetar eller studerar i Sverige. Grupper som särskilt bör beaktas när förslagen utformas är bl.a. äldre och personer med funktionsnedsättning.

En statlig aktör som ansvarar för en e-legitimation kommer att behandla stora mängder personuppgifter om användarna. Det är därför viktigt att skyddet för den personliga integriteten beaktas, både utifrån bestämmelsen i 2 kap. 6 § andra stycket regeringsformen och Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

En del svenska medborgare bor utomlands och utredaren behöver analysera om de ska ha rätt att få tillgång till en e-legitimation från utlandet. Om utredaren bedömer att det bör finnas en sådan möjlighet, ska utredaren föreslå hur ansvarig myndighet kan tillhandahålla den.

Slutligen bör utredningen ta ställning till om en e-legitimation på högsta tillitsnivå ska kunna användas för att framställa kvalificerade elektroniska underskrifter. eIDAS-förordningen skiljer på avancerad elektronisk underskrift och kvalificerad elektronisk underskrift. På den senare ställs det högre säkerhetskrav. De underskrifter som finns på den svenska marknaden i dag är framför allt avancerade elektroniska underskrifter medan det i resten av Europa är mer vanligt med kvalificerade underskrifter.

Myndigheten för digital förvaltning fick våren 2022 ett uppdrag att i samarbete med Polismyndigheten och Försäkringskassan före-

slå hur en statlig e-legitimation kan utformas (I2022/0135). Uppdraget ska redovisas senast den 31 januari 2023. Utredningen ska i sitt arbete beakta förslagen och de synpunkter som framkommit inom ramen för regeringsuppdraget.

Utredaren ska därför

- lämna förslag på hur en kostnadseffektiv e-legitimation på tillitsnivå hög enligt eIDAS-förordningen kan utformas och tillhandahållas av Myndigheten för digital förvaltning,
- lämna förslag på vilken eller vilka myndigheter som ska ansvara för grundidentifieringen vid utfärdandet av en statlig e-legitimation och vilka kontroller av identitet som ska genomföras vid en sådan grundidentifiering,
- analysera om det bör ställas krav på förlitande parter som tillhandahåller digitala tjänster inom offentlig sektor att acceptera alla e-legitimationsalternativ på marknaden förutsatt att de lever upp till den tillitsnivå som tjänsterna kräver,
- analysera om det för vissa grupper kan behövas särskilda lösningar för att de ska kunna identifiera sig digitalt,
- analysera och beräkna kostnader för att ta fram och förvalta en e-legitimation och lämna förslag på hur en ersättningsmodell kan utformas där bl.a. avgifter för att få tillgång till en e-legitimation ska övervägas,
- analysera om e-legitimationen ska kunna användas för att framställa kvalificerade elektroniska underskrifter, och
- lämna nödvändiga författningsförslag.

Uppdraget att analysera och föreslå förändringar som följer av revisionen av eIDAS-förordningen

Om de föreslagna ändringarna i eIDAS-förordningen träder i kraft, innebär det att en rad nya krav måste mötas. Sverige måste exempelvis inrätta ett bedömningsorgan som har till uppdrag att certifiera e-legitimationslösningar som uppnår tillitsnivåerna i förordningen. Vidare ska valideringsmekanismer som säkerställer den digitala plånbokens äkthet införas. Medlemsstaterna kan också komma att be-

höva utarbeta processer för rapportering vid eventuell förlust och eventuellt missbruk av digitala plånböcker samt för återkallandet av sådana plånböcker. Vidare krävs det att medlemsstaterna inrättar ett organ som ansvarar för register över förlitande parter, dvs. fysiska eller juridiska personer som förlitar sig på en elektronisk identifiering.

Enligt förslaget ska ett tillsynsorgan ansvara för frågor som berör tillhanda-hållare av kvalificerade och icke-kvalificerade betrodda tjänster. Organet ska undersöka om betrodda tjänsterna uppfyller kraven i eIDAS-förordningen och kraven i Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen och de krav som den pågående revideringen av det direktivet föranleder.

Medlemsstaterna behöver vidare inkludera en unik och bestående identifikationsbeteckning i minimiuppsättningen av personidentifieringsuppgifter för att kunna identifiera personen när identifiering krävs enligt lag.

De digitala plånböckerna ska enligt förslaget säkerställa att personidentifieringsuppgifter på ett unikt och beständigt sätt representerar den fysiska eller juridiska person som de är förbundna med. Plånböckerna ska tillhandahålla en mekanism som säkerställer att förlitande parter kan autentisera användaren och ta emot attributintyg. Det ska vidare säkerhetsställas att inte fler attribut än vad som är nödvändigt för tjänsten delas.

Myndigheten för digital förvaltning har i rapporten Digital plånbok (I2021/02470) föreslagit att svenska plånböcker ska utfärdas av en statlig myndighet och att även privata aktörer ska ges möjlighet till det. Syftet är att säkerställa att alla användare inkluderas, att systemet blir robust och att tillvarata innovation på området.

Utredaren ska därför

- utreda hur det kan säkerställas att en kostnadseffektiv digital identitetsplånbok i enlighet med den reviderade eIDAS-förordningen ska utfärdas,
- utreda hur en sådan digital plånbok kan användas ändamålsenligt för största möjliga nationella effektivitet och nytta,
- ta ställning till vilken myndighet som bör utses till tillsynsorgan med ansvar för ett register över förlitande parter enligt kraven i den reviderade eIDAS-förordningen,

- analysera den slutgiltiga versionen av förordningen i sin helhet och ge förslag på hur Sverige kan uppfylla tillkommande krav,
- föreslå de författningsändringar och andra åtgärder som krävs för att den föreslagna myndigheten ska kunna vidta de åtgärder som åläggs den enligt förordningen, samt
- lämna de författningsförslag i övrigt som är nödvändiga eller annars bedöms lämpliga för att komplettera förordningen.

Konsekvensbeskrivningar

Utredaren ska bedöma de ekonomiska konsekvenserna för myndigheter, regioner och kommuner av förslagen. Om förslagen kan förväntas leda till kostnadsökningar för ovan nämnda aktörer, ska utredaren föreslå hur dessa ska finansieras. Utredaren ska särskilt bedöma vilka organisatoriska och ekonomiska konsekvenser förslagen får för de myndigheter som berörs av förslagen. Utredaren ska också ange konsekvenser för enskilda och för företag i form av kostnader och ökade administrativa bördor samt om förslagen får några konsekvenser ur ett jämställdhetsperspektiv. Utredaren ska särskilt redovisa förslagens konsekvenser för den personliga integriteten och under arbetets gång göra en integritetsanalys. Utredaren ska också analysera eventuella risker för informationssäkerheten och risker med identitetsrelaterad brottslighet och redovisa konsekvenser för brottsbekämpningen och det brottsförebyggande arbetet.

Konsekvenserna ska redovisas enligt 14–15 a §§ kommittéförordningen (1998:1474) samt 6 och 7 §§ förordningen (2007:1244) om konsekvensutredning vid regelgivning.

Kontakter och redovisning av uppdraget

Utredaren ska hålla sig informerad om och beakta relevant arbete som bedrivs inom Regeringskansliet, utredningsväsendet och inom EU, exempelvis Europeiska kommissionens förslag till förordning och direktiv om digitalisering av rättsligt samarbete.

Under genomförandet av uppdraget ska utredaren ha en dialog med och inhämta upplysningar från Ekobrottsmyndigheten, Finansinspektionen, Försvarsmakten, Försäkringskassan, Integritetsskyddsmyndigheten, Migrationsverket, Myndigheten för digital förvaltning, Myndigheten för samhällsskydd och beredskap, Riksarkivet, Skatteverket, Säkerhetspolisen, Polismyndigheten, Post- och telestyrelsen, näringslivet samt, i den utsträckning som utredaren finner det behövligt, andra organisationer och myndigheter.

Följande uppdrag ska redovisas senast den 16 oktober 2023:

– Uppdraget att föreslå hur staten kan utfärda en e-legitimation på högsta tillitsnivå.

Följande uppdrag ska redovisas senast den 31 maj 2024:

– Uppdraget att analysera och föreslå förändringar som följer av revisionen av eIDAS-förordningen.

(Infrastrukturdepartementet)

Statens offentliga utredningar 2023

Kronologisk förteckning

1. Skärpta straff för flerfaldig brottslighet. Ju.
2. En inre marknad för digitala tjänster – ansvarsfördelning mellan myndigheter. Fi.
3. Nya regler om nödlidande kreditavtal och inkassoverksamhet. Ju.
4. Posttjänst för hela slanten. Finansieringsmodeller för framtidens samhällsomfattande posttjänst. Fi.
5. Från delar till helhet. Tvångsvården som en del av en sammanhållen och personcentrerad vårdkedja. S.
6. En lag om tilläggsskatt för företag i stora koncerner. Fi.
7. På egna ben. Utvecklad samverkan för individers etablering på arbetsmarknaden. A.
8. Arbetslivskriminalitet – arbetet i Sverige, en bedömning av omfattningen, lärdomar från Danmark och Finland. A.
9. Ett statligt huvudmannaskap för personlig assistans. Ökad likvärdighet, långsiktighet och kvalitet. S.
10. Tandvårdens stöd till våldsutsatta patienter. S.
11. Tillfälligt miljötillstånd för samhällsviktig verksamhet – för ökad försörjningsberedskap. KN.
12. Förstärkt skydd för demokratin och domstolarnas oberoende. Ju.
13. Patientöversikter inom EES och Sverige. S.
14. Organisera för hållbar utveckling. KN.
15. Förnybart i tanken. Ett styrmedelsförslag för en stärkt bioekonomi. LI.
16. Staten och betalningarna. Del 1 och 2. Fi.
17. En tydligare bestämmelse om hets mot folkgrupp. Ju.
18. Värdet av vinden. Kompensation, incitament och planering för en hållbar fortsatt utbyggnad av vindkraften. Del 1 och 2. KN.
19. Statlig forskningsfinansiering. Underlagsrapporter. U.
20. Förbud mot bottentrålning i marina skyddade områden. LI.
21. Informationsförsörjning på skolområdet. Skolverkets ansvar. U.
22. Datalagring och åtkomst till elektronisk information. Ju.
23. Ett modernare socialförsäkringsskydd för gravida. S.
24. Etablering för fler – jämställda möjligheter till integration. A.
25. Kunskapskrav för permanent uppehållstillstånd. Ju.
26. Översyn av entreprenörsansvaret. A.
27. Kamerabevakning för ett bättre djurskydd. LI.
28. Samhället mot skolattacker. U.
29. Varje rörelse räknas – hur skapar vi ett samhälle som främjar fysisk aktivitet? S.
30. Ett trygghetssystem för alla. Nytt regelverk för sjukpenninggrundande inkomst. S.
31. Framtidens yrkeshögskola – stabil, effektiv och hållbar. U.
32. Biometri – för en effektivare brottsbekämpning. Ju.
33. Ett förbättrat resegarantisystem. Fi.
34. Bolag och brott – några åtgärder mot oseriösa företag. Ju.
35. Nya regler om hållbarhetsredovisning. Ju.
36. Genomförande av minimilönedirektivet. A.

37. Förstärkt skydd för den personliga integriteten. Behovet av åtgärder mot oskuldskontroller, oskuldsintyg och oskuldsingrepp samt omvändelseförsök. Ju.
38. Ett förstärkt konsumentskydd mot riskfylld kreditgivning och överskuldsättning. Fi.
39. En inre marknad för digitala tjänster – kompletteringar och ändringar i svensk rätt. Fi.
40. Förbättrade möjligheter för barn att utkräva sina rättigheter enligt barnkonventionen. S.
41. Förutsättningarna för en ny kollektivavtalad arbetslöshetsförsäkring. A.
42. Ett modernare regelverk för legaliseringar, apostille och andra former av intyganden. UD.
43. En samordnad registerkontroll för upphandlande myndigheter och enheter. Fi.
44. En översyn av regleringen om frihetsberövande påföljder för unga. Ju.
45. Övergångsrestriktioner – ökat förtroende för offentlig verksamhet. Fi.
46. Jakt och fiske i renbetesland. LI.
47. En utvecklad arbetsgivardeklaration – åtgärder mot missbruk av välfärdssystemen. Fi.
48. Rätt förutsättningar för sjukskrivning. S.
49. Skyddet för EU:s finansiella intressen. Ändringar och kompletteringar i svensk rätt. Fi.
50. En modell för svensk försörjningsberedskap. Fö.
51. Signalspaning i försvarsunderrättelseverksamhet – frågor med anledning av Europadomstolens dom. Fö.
52. Ett stärkt och samlat skydd av välfärdssystemen. S.
53. En ändamålsenlig arbetsskadeförsäkring – för bättre ekonomisk trygghet, kunskap och rättssäkerhet. Volym 1 och 2. S.
54. Centraliseringen av administrativa tjänster till Statens servicecenter – en utvärdering. Fi.
55. Vem äger fastigheten. Ju.
56. Några smittskyddsfrågor inom socialtjänsten och socialförsäkringen. S.
57. Åtgärder för tryggare bostadsområden. Ju.
58. Kultursamhället – utvecklad samverkan mellan stat, region och kommun. Ku.
59. Ny myndighetsstruktur för finansiering av forskning och innovation. U.
60. Utökade möjligheter att använda preventiva tvångsmedel 2. Ju.
61. En säker och tillgänglig statlig e-legitimation. Fi.

Statens offentliga utredningar 2023

Systematisk förteckning

Vem äger fastigheten. [55]

Åtgärder för tryggare bostadsområden. [57]

Utökade möjligheter att använda preventiva tvångsmedel 2. [60]

Klimat- och näringslivsdepartementet

Tillfälligt miljötillstånd för samhällsviktig verksamhet – för ökad försörjningsberedskap. [11]

Organisera för hållbar utveckling. [14]

Värdet av vinden. Kompensation, incitament och planering för en hållbar fortsatt utbyggnad av vindkraften. Del 1 och 2. [18]

Kulturdepartementet

Kultursamhället – utvecklad samverkan mellan stat, region och kommun. [58]

Landsbygds- och infrastrukturdepartementet

Förnybart i tanken. Ett styrmedelsförslag för en stärkt bioekonomi. [15]

Förbud mot bottentrålning i marina skyddade områden. [20]

Kamerabevakning för ett bättre djurskydd. [27]

Jakt och fiske i renbetesland. [46]

Socialdepartementet

Från delar till helhet. Tvångsvården som en del av en sammanhållen och personcentrerad vårdkedja. [5]

Ett statligt huvudmannaskap för personlig assistans. Ökad likvärdighet, långsiktighet och kvalitet. [9]

Tandvårdens stöd till våldsutsatta patienter. [10]

Patientöversikter inom EES och Sverige. [13]

Ett modernare socialförsäkringsskydd för gravida. [23]

Varje rörelse räknas – hur skapar vi ett samhälle som främjar fysisk aktivitet? [29]

Ett trygghetssystem för alla. Nytt regelverk för sjukpenninggrundande inkomst. [30]

Förbättrade möjligheter för barn att utkräva sina rättigheter enligt barnkonventionen. [40]

Rätt förutsättningar för sjukskrivning. [48]

Ett stärkt och samlat skydd av välfärdssystemen. [52]

En ändamålsenlig arbetsskadeförsäkring – för bättre ekonomisk trygghet, kunskap och rättssäkerhet. Volym 1 och 2. [53]

Några smittskyddsfrågor inom socialtjänsten och socialförsäkringen. [56]

Utbildningsdepartementet

Statlig forskningsfinansiering. Underlagsrapporter. [19]

Informationsförsörjning på skolområdet. Skolverkets ansvar. [21]

Samhället mot skolattacker. [28]

Framtidens yrkeshögskola – stabil, effektiv och hållbar. [31]

Ny myndighetsstruktur för finansiering av forskning och innovation. [59]

Utrikesdepartementet

Ett modernare regelverk för legaliseringar, apostille och andra former av intygande. [42]