**RP 133/2022 rd**

**Regeringens proposition till riksdagen med förslag till lagstiftning om digital identitet**

## PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås det att det stiftas en lag om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata samt en lag om e-legitimation. Dessutom föreslås det ändringar i lagen om stark autentisering och betrodda elektroniska tjänster, lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata, lagen om behandling av personuppgifter i polisens verksamhet, lagen om identitetskort, passlagen och lagen om förvaltningens gemensamma stödtjänster för e-tjänster.

Propositionen syftar till att göra det möjligt att producera och använda e-legitimationer samt e-tjänstverktyg för utlänningar. Det är fråga om nya mobilapplikationer till stöd för uträttandet av ärenden digitalt. Applikationerna ska produceras av polisen och Myndigheten för digitalisering och befolkningsdata för uppvisande av bestyrkta personuppgifter. E-legitimationen ska även fungera som en identitetshandling på motsvarande sätt som pass och identitetskort, och den ska ha en egenskap för stark autentisering. Den föreslagna lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata innehåller bestämmelser om ett informationssystem för digital identitet, som ska ligga till grund för e-legitimationen och för e-tjänstverktyget för utlänningar. De föreslagna bestämmelserna gäller utöver myndigheternas uppgifter bland annat också kraven på och informationssäkerheten i informationssystemet samt behandlingen av personuppgifter.

Enligt propositionen ska det dessutom vara möjligt för personer som inte vill eller kan använda mobilapplikationen att använda ett alternativt identifieringsverktyg. Identifieringsverktyget ska kunna användas för att uträtta ärenden elektroniskt inom den offentliga sektorn, och verktyget ska beviljas av Myndigheten för digitalisering och befolkningsdata.

Propositionen hänför sig till budgetpropositionen för 2023 och avses bli behandlad i samband med den. Lagarna avses träda i kraft den 1 september 2023.

---

**INNEHÅLL**

## MOTIVERING

# 1 Bakgrund och beredning

## 1.1 Bakgrund

I statsminister Marins regeringsprogram (https://valtioneuvosto.fi/sv/marin/regeringsprogrammet, s. 113) har det satts som mål att Finland är känt som ett föregångarland där de möjligheter som digitaliseringen och den tekniska utvecklingen medför utvecklas och tillvaratas över förvaltnings- och sektorsgränserna. Målet är att höja teknik- och digitaliseringsberedskapen hos den offentliga sektorn och utveckla samarbetet mellan den offentliga sektorn och den privata sektorn. I regeringsprogrammet har det bland annat satts som mål att finska medborgare och alla som bor i Finland ska ges möjlighet till elektronisk identifiering samt att främja utvecklingen av fungerande identifieringslösningar. I regeringsprogrammet har dessutom lyfts fram både individens möjlighet att kontrollera sina egna uppgifter inom den offentliga servicen och tillräckliga stödtjänster i anslutning till offentlig tjänster i syfte att säkerställa jämlikheten mellan medborgarna.

I syfte att nå målen i regeringsprogrammet har finansministeriet tillsatt ett projekt för att utveckla den digitala identiteten och sätten att använda den. I samband med projektet har finansministeriet tillsatt en lagstiftningsarbetsgrupp för den digitala identiteten samt en underarbetsgrupp för konsekvensbedömningen i syfte att bereda förslag till lagstiftning som gör det möjligt att skapa digitala identitetshandlingar och använda dem i samhällets tjänster för att styrka identiteten och visa bestyrkta personuppgifter.

Bakom regeringens proposition ligger också utvecklingen av digitala identitetslösningar i EU. Europeiska kommissionen överlämnande den 3 juni 2021 sitt förslag COM (2021)281 till ändring av Europaparlamentets och rådets förordning (EU) nr 910/2014. Detta förslag och den egentliga ändringsförordning som överlämnas senare kommer att avsevärt påverka den digitala identiteten och produktionen av tjänster i anslutning till den i Finland.

## 1.2 Beredning

Bakom den föreslagna lagstiftningen om digital identitet ligger en längre tids utveckling på området för identitet och digitala tjänster. Under det senaste decenniet har det inom ramen för flera olika projekt gjorts utredningar om hantering och användning av personers officiella identitet. Som den mest heltäckande utredningen kan betraktas den slutrapport om identitetsprogrammet som inrikesministeriet publicerade i december 2010 (Projekt rörande skapande av identitet (identitetsprogrammet). Arbetsgruppens slutrapport. Inrikesministeriets publikationer 32/2010, https://julkaisut.valtioneuvosto.fi/handle/10024/79876), där man beskriver de utvecklingsbehov som då riktade sig mot skapandet, hanteringen och användning av en av myndigheterna producerad identitet. En del av förslagen i rapporten har genomförts efter publiceringen.

Hösten 2018 bad finansministeriet att den dåvarande Befolkningsregistercentralen skulle göra en förstudie om alternativen i fråga om elektronisk identifiering (https://julkaisut.valtioneuvosto.fi/handle/10024/161432), som skulle svara på de problempunkter som hänför sig till den nuvarande modellen i förhållande till de sätt på vilka det antas att digital identitet kommer att användas i framtiden. Målet med studien var att hitta en eller flera alternativa modeller för att hantera elektronisk identifiering och digital identitet som hela befolkningen har tillgång till i så stor utsträckning som möjligt utan diskriminering och oavsett personens ålder eller fysiska begränsningar. Förutom finska medborgare borde det också vara möjligt att identifiera utlänningar som uträttar ärenden i Finland. Arbetet utvärderades av en av finansministeriet tillsatt

styrgrupp, som ändå inte var enhällig i sina slutsatser. Avvikande mening lämnades av kommunikationsministeriet, Konkurrens- och konsumentverket samt Transport- och kommunikationsverket Traficom. Styrkande och verifiering av identiteten har dessutom beskrivits i flera regeringspropositioner som gäller elektronisk identifiering.

Vid sidan av studierna som gäller elektronisk identifiering behandlade den arbetsgrupp som finansministeriet tillsatt för att utreda förnyande av personbeteckningen i sin slutrapport som publicerades i april 2020 (Slutrapport om förnyandet av personbeteckningen (Finansministeriets publikationer – 2020:42, https://julkaisut.valtioneuvosto.fi/handle/10024/162231) behoven av ändringar i de registreringsuppgifter och registreringsförfaranden som behövs för att identifiera personer.

Finansministeriet tillsatte den 8 oktober 2020 ett projekt för att utveckla den digitala identiteten och sätten att använda den (https://vm.fi/hanke?tunnus=VM161:00/2020). Mandatperioden för projektet är 8 oktober 2020–30 juni 2023. För projektet tillsattes en styrgrupp, som bestod av företrädare för finansministeriet, inrikesministeriet, kommunikationsministeriet, social- och hälsovårdsministeriet, undervisnings- och kulturministeriet samt arbets- och näringsministeriet. Styrgruppens arbete stöddes av ett sekretariat som bestod av företrädare för finansministeriet, Myndigheten för digitalisering och befolkningsdata samt Polisstyrelsen och som beredde de ärenden som skulle föredras för styrgruppen.

Projektet består av två arbetspaket, och de uppdrag som hänför sig till dem har i tillämpliga delar genomförts parallellt. Resultaten av utredningarna samt riktlinjerna i arbetspaket 1 samlades i en bedömningspromemoria om utveckling av digital identitet som publicerades den 18 mars 2021 (https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=938337e8-306d-4737-bc4b-02bd2911f308). Finansministeriet begärde utlåtanden om bedömningspromemorian via tjänsten utlåtande.fi under tiden 18 mars 2021–30 april 2021. Det kom sammanlagt 117 utlåtanden. Utlåtandena samt ett sammandrag av dem finns på de ovannämnda projektsidorna. Vid sidan av bedömningspromemorian om utveckling av digital identitet har Traficom och Konkurrens- och konsumentverket gjort en egen utredning om marknaden för digital identifiering(https://www.traficom.fi/sites/default/files/media/publication/S%C3%A4hk%C3%B6isen_tunnistamisen_markkinat_-_S%C3%A4hk%C3%B6inen%20tunnistaminen%20turvallisen%20asioinnin%20mahdollistajana%2017%2003%202021p.pdf)

Åtgärderna enligt arbetspaket 2 inleddes sommaren 2021. För projektet tillsattes den 23 juni 2021 en lagstiftningsgrupp, som bestod av medlemmar från finansministeriet, inrikesministeriet, undervisnings- och kulturministeriet, kommunikationsministeriet, arbets- och näringsministeriet samt social- och hälsovårdsministeriet samt experter från Transport- och kommunikationsverket, Myndigheten för digitalisering och befolkningsdata samt polisstyrelsen. För projektet tillsattes också en underarbetsgrupp för konsekvensbedömningen, som bestod av medlemmar från finansministeriet, inrikesministeriet, kommunikationsministeriet, Transport- och kommunikationsverket, Myndigheten för digitalisering och befolkningsdata, polisstyrelsen samt Konsument- och konkurrensverket. Grupperna deltog i beredningen av regeringens proposition, men av orsaker som har att göra med tidtabellen färdigställdes regeringens proposition som tjänsteuppdrag vid finansministeriet.

Finansministeriet begärde utlåtanden om utkastat till regeringens proposition med förslag till lagstiftning om digital identitet via tjänsten Utlåtande.fi under tiden 21 februari–8 april 2022. Inom utsatt tid kom det 651 remissvar på begäran om utlåtande. Av dessa kom 127 utlåtanden från organisationer. Tio som svarade meddelade att de inte har något att yttra i saken. Efter remisstidens utgång tillfrågades dessutom aktörer inom förtroendenätet om de vill yttra sig. De

som besvarade förfrågan bekräftade att de inte avger separat utlåtande utan förenar sig med intresseorganisationernas (Finanssiala ry eller FiCom) utlåtanden. Responsen från medborgarna omfattade sammanlagt 524 utlåtanden inom utsatt tid. Utlåtandena och ett sammandrag av dem finns i statsrådets projektportal (projekt-ID VM092:00/2021).

Lagförslagets innehåll har behandlats på möten för ministerarbetsgruppen för utveckling av digitaliseringen, dataekonomin och den offentliga förvaltningen 1.6.2022 samt 23.6.2022.

## 2 Nuläge och bedömning av nuläget

### 2.1 Allmänt om omvärlden

Den lagstiftning och de funktionella lösningar som propositionen gäller blir en del av en omvärld där identiteten visas och de uppgifter som gäller en person behandlas på mycket olika sätt. Medborgare och andra som uträttar ärenden i det finländska samhället behöver visa upp personuppgifter som gäller dem själva samt styrka sin identitet i många olika slags situationer, såväl med traditionella handlingar som styrker identiteten i situationer där de uträttar ärenden fysiskt som elektroniskt i olika e-tjänster. Behovet av att identifiera en person kan basera sig på ett praktiskt behov eller tillvägagångssätt, men det kan också förutsättas i lagstiftningen eller med stöd av ett avtal. Exempelvis i konsumentskyddslagen (38/1978) åläggs skyldighet att noggrant kontrollera identiteten i fråga om konsumentkreditavtal och det preciseras ytterligare hur identiteten ska kontrolleras i samband med e-tjänster.

I nuläget granskas metoderna för att styrka identitet och visa upp uppgifter oftast med avseende på e-tjänster eller traditionellt uträttande av ärenden på plats. Som ett typiskt exempel på det förstnämnda kan betraktas stark autentisering med bankkoder och som ett typiskt exempel på det senare uppvisande av pass som identitetsbevis. Situationerna där man uträttar ärenden har dock blivit mer mångskiftande, och till exempel i samband med uträttande av ärenden på plats kan också e-tjänster nyttjas. Å andra sidan kan utvecklingen i fråga om e-tjänster gå mot bestyrkta handlingar som innehas av personen – i princip på samma sätt som när personen själv innehar och fritt kan visa upp ett pass som myndigheten beviljat. Utvecklingen av digital identitet förutsätter att omvärlden granskas som en helhet och förslagen i propositionen gäller regleringen av såväl e-tjänster och elektronisk identifiering som traditionella dokument som styrker identiteten. Nuläget i fråga om bägge granskas nedan.

### 2.2 Handlingar som styrker identiteten: pass och identitetskort

*Allmänt om handlingar som styrker identiteten*

Finsk lagstiftningen reglerar inte på allmän nivå vilka handlingar som kan användas för att styrka identiteten. Nationellt används inte begreppet officiellt identitetsbevis och i lagstiftningen ställs det inga krav på vilka slags handlingar som kan fungera som identitetsbevis eller vilka handlingar som ska godkännas. Lagstiftningen och praxisen för att styrka identiteten berör dels reglering av vissa handlingar som myndigheterna utfärdat, i praktiken pass och identitetskort, dels reglering av identifiering som sker ansikte mot ansikte hos vissa myndigheter, i vissa branscher eller i samband med vissa kundkontakter. Sätten att kontrollera identiteten ansikte mot ansikte har dessutom i praktiken kunnat utformas på mångahanda sätt.

Pass och identitetskort är handlingar som styrker identiteten och som utfärdas av polisen. Med vissa undantag som gäller identitetskort är de också resedokument. För närvarande innehas ett pass eller identitetskort av cirka 4,1 miljoner finländare, av vilka cirka 580 000 är minderåriga.

Varje år utfärdas sammanlagt cirka 1,1 miljoner pass och identitetskort, och det finns sammanlagt cirka 4,8 miljoner giltiga pass och identitetskort.

I passlagen (671/2006) och lagen om identitetskort (663/2016) föreskrivs det om till exempel utfärdande, överlämnande och indragning av dessa handlingar. Centralt i dem är bestämmelserna om försättningarna för utfärdande av en handling, och om identifiering av personen när pass eller identitetskort utfärdas. I passlagen föreskrivs det inte uttryckligen om passets ställning som en handling som styrker identiteten, men enligt 1 § i lagen om identitetskort innehåller lagen bestämmelser om identitetskort som utfärdas för finska medborgare och utlänningar som vistas i Finland för styrkande av identiteten. Lagarna ålägger inte aktörer separat att godkänna handlingarna som identitetsbevis eller för att identifiera en person.

I passlagen och lagen om identitetskort föreskrivs det att vid ansökan om pass eller identitetskort ska sökanden i princip visa upp en giltig handling som styrker identiteten. Närmare bestämmelser om handlingar som styrker identiteten och som utfärdas av polisen finns i statsrådets förordning om pass och identitetskort (1167/2016).

*Identitetskort och utfärdande av identitetskort*

Lagen om identitetskort innehåller bestämmelser om identitetskort som utfärdas för finska medborgare och utlänningar som vistas i Finland för styrkande av identiteten. Enligt 1.2 § i lagen gäller det som i lagen om identitetskort föreskrivs om identitetskort också identitetskort som utfärdas för utlänningar som vistas i Finland (identitetskort för utlänningar), sådana identitetskort som utan vårdnadshavarnas samtycke utfärdas för en minderårig (identitetskort för minderårig) samt temporära identitetskort.

Enligt 2 § kan ett identitetskort som utfärdats för en finsk medborgare i enlighet med bestämmelser som utfärdats med stöd av 2 § 1 mom. i passlagen användas som resedokument i stället för pass. Enligt 2 mom. gäller det som föreskrivs i 1 mom. inte ett identitetskort för minderårig, ett temporärt identitetskort som avses i 15 § eller ett identitetskort som avses i 17 § 3 mom.

Ansökan om identitetskort ska göras hos polisen. Ansökan kan anhängiggöras på elektronisk väg. Sökanden ska personligen infinna sig hos myndigheten för komplettering av ansökan, om inte något annat följer av 10 §. Enligt 10 § i lagen om identitetskort behöver den som ansöker om identitetskort på elektronisk väg inte personligen infinna sig hos myndigheten, om 1) ett identitetskort eller pass för finsk medborgare har utfärdats för sökanden under de sex år som föregår ansökan om identitetskort och sökanden vid den ansökan personligen har besökt myndigheten, 2) sökanden har varit äldre än 12 år när en handling som avses i 1 punkten har utfärdats, och 3) sökanden under de sex år som föregår ansökan om identitetskort har lämnat ett namnteckningsprov för identitetskort eller pass, och sökandens efternamn eller förnamn inte har ändrats efter detta.

För en minderårig sökande kan ett identitetskort utfärdas, om vårdnadshavarna ger sitt samtycke till det. Om någon av vårdnadshavarna inte på grund av resa, sjukdom eller annat motsvarande skäl kan ge sitt samtycke och om dröjsmål med avgörandet skulle medföra oskälig olägenhet, kan det med stöd av lagens 16 § utfärdas ett identitetskort utan detta samtycke. För en minderårig sökande kan ett identitetskort för minderårig utfärdas utan vårdnadshavarnas samtycke. Det är fråga om en särskild typ av identitetskort för minderårig där vårdnadshavarnas samtycke inte behövs för ansökan. I lagen om identitetskort föreskrivs ingen undre åldersgräns för utfärdande av identitetskort för minderårig.

Till ansökan ska fogas sökandens ansiktsbild, på vilken sökanden utan svårighet kan kännas igen. Enligt 1 § i inrikesministeriets förordning om passfotografier och fotografier på identitetskort (1168/2016) ska till passansökan och ansökan om identitetskort fogas ett högst sex månader gammalt svartvitt fotografi eller färgfotografi av sökandens ansikte.

*Identitetskortets chips och dess informationssäkerhet*

Europaparlamentets och rådets förordning (EU) 2019/1157 om säkrare identitetskort för unionsmedborgare och uppehållshandlingar som utfärdas till unionsmedborgare och deras familjemedlemmar när de utövar rätten till fri rörlighet, nedan EU:s ID-förordning, trädde i kraft i början av augusti 2019. Enligt artikel 3.5 i EU:s ID-förordning ska identitetskort innefatta ett mycket säkert lagringsmedium som innehåller en ansiktsbild av innehavaren och två fingeravtryck i interoperabla digitala format. Vid insamlingen av biometriska kännetecken ska medlemsstaterna tillämpa de tekniska specifikationer som fastställs i kommissionens genomförandebeslut C(2018)7767.

Enligt 5 § i lagen om identitetskort har identitetskortet en teknisk del i vilken det lagras uppgifter om medborgarcertifikat, de uppgifter för identifiering av kortinnehavaren som behövs vid elektronisk kommunikation och andra nödvändiga uppgifter. I den tekniska delen kan också de uppgifter som avses i 4 § 1 mom. lagras. Ett identitetskort för minderårig och ett temporärt identitetskort har inte någon sådan teknisk del som avses i paragrafen. Hänvisningen till lagens 4 § 1 mom. innebär att i identitetskortets tekniska del, dvs. chipset, kan finnas kortinnehavarens efternamn, förnamn, kön, födelsetid och personbeteckning, dag för utfärdande av identitetskortet och sista giltighetsdag, den myndighet som utfärdat identitetskortet, kortets nummer och i fråga om finska medborgare uppgift om nationalitet. I identitetskortets chips kan dessutom finnas kortinnehavarens fotografi och namnteckning.

På det sätt som framgår ovan föreskrivs det i EU:s ID-förordning att nationella identitetskort som EU:s medlemsländer utfärdar ska uppfylla minimikraven på säkerhet samt vissa specifikationer enligt EU:s ID-förordning. Fingeravtryck är ett biometriskt kännetecken som är en permanent, oföränderlig och oåterkallelig del av individen. Biometriska kännetecken ställer särskilda krav på informationssäkerheten så att det kan säkerställas att integritetsskyddet tillgodoses. Av denna orsak bör det föreskrivas om informationssäkerheten för identitetskortets chips i lagen om identitetskort.

Enligt led 40 i EU:s ID-förordning bör de registrerade ha tillgång till de personuppgifter som behandlas på deras identitetskort och uppehållshandlingar och ha rätt att få dem rättade genom att en ny handling utfärdas om uppgifterna är felaktiga eller ofullständiga. I 8 § i lagen om identitetskort finns bestämmelser om rätt för kortinnehavaren att kontrollera personuppgifterna i identitetskortets tekniska del och vid behov begära att uppgifter rättas eller stryks.

*Pass och utfärdande av pass*

Enligt 3 § i passlagen utfärdas för styrkande av rätten att resa för finska medborgare på ansökan pass, om inte något annat följer av lag. I 5 § i passlagen föreskrivs om passets innehåll och enligt 1 mom. antecknas i ett pass sökandens efternamn och förnamn, kön, födelsetid och personbeteckning, nationalitet, födelsehemkommun, den dag passet utfärdats och sista giltighetsdag, den myndighet som utfärdat passet och passets nummer. I passet finns dessutom passinnehavarens ansiktsbild och namnteckning. I ett pass med begränsat giltighetsområde antecknas de länder som passet berättigar innehavaren att resa till eller de länder som passet inte berättigar inneha-

varen att resa till. I stället för födelsehemkommunen antecknas ”utlandet”, om sökandens födelsehemkommun inte tillförlitligt kan utredas eller om antecknandet av födelsehemkommunen i passet sannolikt skulle äventyra passinnehavarens säkerhet. Ett pass är giltigt i fem år från den dag då passet utfärdades.

I 5 a § i passlagen föreskrivs det om passets tekniska del och kontroll av uppgifterna. Enligt 1 mom. innehåller ett pass en teknisk del enligt rådets förordning (EG) nr 2252/2004 om standarder för säkerhetsdetaljer och biometriska kännetecken i pass och resehandlingar som utfärdas av medlemsstaterna (EU:s passförordning). Enligt 2 mom. lagras i den tekniska delen passinnehavarens ansiktsbild och de fingeravtryck som avses i 6 a § inklusive nödvändiga tilläggsuppgifter i enlighet med vad som bestäms i EU:s passförordning. I den tekniska delen kan också de uppgifter lagras som avses i 5 § 1 mom. I EU:s passförordning finns bestämmelser om passinnehavarens rätt att kontrollera de uppgifter om honom eller henne som finns lagrade i passets tekniska del. Enligt 3 mom. finns bestämmelser om passets säkerhetsdetaljer och biometriska kännetecken i EU:s passförordning. På pärmen till ett pass med ett biometriskt kännetecken finns en symbol som anger detta.

Polisstyrelsen ska i enlighet med EU:s passförordning och de bestämmelser som utfärdats för tillämpning av den se till att uppgifterna i passets tekniska del skyddas effektivt mot intrång, olovlig avläsning, modifiering, användning och övrig olovlig behandling. Certifikat som hänför sig till säkerställandet av äktheten och integriteten hos uppgifterna i den tekniska delen eller som behövs för avläsning av fingeravtryck utfärdas av Myndigheten för digitalisering och befolkningsdata. Utrikesministeriet svarar för skyddet av uppgifterna i den tekniska delen i diplomatpass och tjänstepass och i pass som utfärdats av en i 10 § avsedd beskickning utomlands.

Ansökan om pass ska göras hos polisen. Ansökan kan anhängiggöras på elektronisk väg. Sökanden ska dock personligen infinna sig hos myndigheten för komplettering av ansökan. Enligt 6 § 4 mom. i passlagen ska till ansökan fogas sökandens ansiktsbild, på vilken sökanden utan svårighet kan kännas igen. Sökanden ska som identifieringshandling uppvisa en giltig handling där sökandens identitet framgår. Om sökanden inte kan uppvisa en identifieringshandling, utförs identifieringen av den myndighet som utfärdar passet. Elektronisk kommunikation förutsätter ett sådant identifieringsverktyg som avses i lagen om stark autentisering och elektroniska signaturer. Enligt 5 mom. utfärdas genom förordning av statsrådet närmare bestämmelser om de identitetshandlingar som polisen utfärdar. Genom förordning av inrikesministeriet får närmare bestämmelser utfärdas om antalet ansiktsbilder som ska fogas till ansökan och om kraven på ansiktsbilderna. För en minderårig utfärdas pass, om den minderåriges vårdnadshavare ger samtycke till det.

Om sökanden ansöker om nytt pass på elektronisk väg inom sex år från utfärdandet av ett tidigare pass eller identitetskort och det för ett tidigare pass eller ett tidigare sådant identitetskort som avses i 2 § 1 mom. i lagen om identitetskort har tagits fingeravtryck och lämnats namnteckningsprov, behöver sökanden enligt 6 b § inte vara personligen närvarande när han eller hon ansöker om pass. Då tas inga fingeravtryck för det nya passet. När sökanden ansöker om nytt pass på elektronisk väg ska han eller hon dock personligen infinna sig hos myndigheten, om det behövs för att sökanden ska kunna identifieras, lämna nya fingeravtryck, lämna ett nytt namnteckningsprov eller av någon annan särskild orsak.

### 2.3 Stark autentisering

Vid stark autentisering är det fråga om att verifiera identiteten elektroniskt. I lagen om stark autentisering och betrodda elektroniska tjänster (617/2009, nedan *autentiseringslagen*) föreskrivs det om kraven på stark autentisering och om tillhandahållande av identifieringstjänster

till tjänsteleverantörer, till allmänheten och till andra leverantörer av identifieringstjänster. Lagens syfte är att med hjälp av bestämmelserna försöka främja utvecklingen av stark autentisering på marknadsvillkor. Lagens centrala mål är att främja säkerheten hos e-tjänster och vid anlitandet av tjänster genom att utöka användningen av stark autentisering. Med hjälp av stark autentisering kan konsumenterna tryggt styrka sin identitet i olika elektroniska tjänster och leverantörer av e-tjänster kan identifiera sina kunder. Transport- och kommunikationsverket övervakar efterlevnaden av autentiseringslagen.

Autentiseringslagen innehåller en definition av stark autentisering samt närmare krav på denna. Dessa krav överensstämmer med Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (nedan *eIDAS-förordningen*). I fråga om elektronisk identifiering gäller eIDAS-förordningen de system för elektronisk identifiering som medlemsländerna anmält. Nationella identifieringsmetoder kan anmälas till EU-kommissionen i enlighet med eIDAS-förordningen. Det ska vara möjligt att använda en anmäld identifieringsmetod för att uträtta ärenden inom den offentliga förvaltningen i andra medlemsländer. I förordningen föreskrivs det om vilka slags system för elektronisk identifiering som medlemsstaterna kan anmäla till kommissionen, hur anmälan görs och vilka krav som ställs på de identifieringssystem och identifieringsmetoder som anmäls. I förordningen och de genomförandeakter som antagits med stöd av den anges tre tillitsnivåer för identifieringstjänster: låg, väsentlig och hög. I Finland ställs det åtminstone samma krav på tillförlitlighet och informationssäkerhet som vad eIDAS-förordningen och genomförandeakterna kräver av gränsöverskridande system för elektronisk identifiering på tillitsnivån väsentlig.

Enligt autentiseringslagen avses med stark autentisering identifiering av en person, av en juridisk person eller av en fysisk person som företräder en juridisk person och verifiering av identifikatorns autenticitet och riktighet genom tillämpning av en elektronisk metod som motsvarar tillitsnivån väsentlig eller hög enligt eIDAS-förordningen. Det är alltså fråga om styrka identiteten elektroniskt med hjälp av ett identifieringsverktyg för stark autentisering. Enligt 2 § i autentiseringslagen avses med identifieringsverktyg ett sådant medel för elektronisk identifiering som avses i artikel 3.2 i eIDAS-förordningen. I eIDAS-förordningen används begreppet medel för elektronisk identifiering i samma betydelse som identifieringsverktyg.

Lagens definition är teknikneutral och beskriver vilka komponenter som helst som i fysisk, digital eller kunskapsmässig form tillsammans bildar ett identifieringsverktyg. Ett identifieringsverktyg för stark autentisering kan alltså tekniskt basera sig på olika metoder. Med verktyg kan avses till exempel ett certifikat som finns på ett SIM-kort eller ett annat kort och den PIN-kod eller användaridentifikation i kombination med ett utbytbart lösenord som behövs för att använda det, eller fingeravtryck i kombination med en PIN-kod. Identifieringsverktyg för stark autentisering som för närvarande används i Finland är bankernas bankkoder och teleföretagens mobilcertifikat samt Myndigheten för digitalisering och befolkningsdatas medborgarcertifikat som finns på de identitetskort som polisen utfärdar och de organisationscertifikat som finns på de organisationskort som Myndigheten för digitalisering och befolkningsdata beviljar.

### 2.4 Förtroendenät och marknad för stark autentisering

I autentiseringslagen föreskrivs det om förtroendenätet för leverantörer av identifieringstjänster. Leverantörer av tjänster för stark autentisering ska innan de inleder sin verksamhet göra en skriftlig anmälan till Transport- och kommunikationsverket. De leverantörer av identifieringstjänster som gjort anmälan bildar direkt med stöd lagen ett förtroendenät för elektronisk identifiering. I autentiseringslagen föreskrivs det om de skyldigheter som hänför sig till identifierings-

tjänsteleverantörernas verksamhet i förtroendenätet, såsom leverantörernas skyldigheter att tillhandahålla tjänster och samarbeta sinsemellan, maximipriserna för identifieringstjänster samt skyldighet att bedöma att ett identifieringsverktyg överensstämmer med kraven. Genom bestämmelserna om förtroendenätet har det skapats en marknad för elektronisk identifiering genom att ställa vissa krav på verksamheten hos leverantörer av identifieringstjänster och föreskriva om tillsyn över dem.

I förtroendenätet finns två slags aktörer: leverantörer av identifieringsverktyg och leverantörer av tjänster för identifieringsförmedling. I autentiseringslagen föreskrivs det om dessa aktörers skyldigheter och om deras verksamhet i förtroendenätet. Leverantörer av identifieringsverktyg och leverantörer av tjänster för identifieringsförmedling är bägge leverantörer av identifieringstjänster. Leverantör av identifieringstjänster är således ett överbegrepp till dessa två begrepp. Med leverantörer av identifieringsverktyg avses aktörer som tillhandahåller identifieringsverktyg till användarna, dvs. fysiska personer och juridiska personer. I Finland är leverantörer av identifieringsverktyg banker, teleföretag och Myndigheten för digitalisering och befolkningsdata. Med leverantörer av tjänster för identifieringsförmedling avses de aktörer som förmedlar identifieringstransaktioner till e-tjänster. Leverantörer av tjänster för identifieringsförmedling ingår avtal med leverantörer av identifieringsverktyg om att de får förmedla identifieringstransaktioner som görs med identifieringsverktyg till e-tjänster. Samma tjänsteleverantör kan vara leverantör av både verktyg och förmedlingstjänst.

I Transport- och kommunikationsverkets register finns för närvarande 16 leverantörer av tjänster för stark autentisering. Av dessa tillhandahåller 14 aktörer ett eget identifieringsverktyg för stark autentisering. Det finns åtta identifieringstjänster som förmedlar identifiering av även andra användare än användarna av det egna identifieringsverktyget för stark autentisering. Av dem som tillhandahåller tjänster för identifieringsförmedling tillhandahåller två endast förmedlingstjänster, dvs. de tillhandahåller inte ett eget verktyg för stark autentisering. Av dem som tillhandahåller tjänster för identifieringsförmedling förmedlar sex alla identifieringsverktyg som används i Finland till e-tjänster med undantag av Myndigheten för digitalisering och befolkningsdatas person- och organisationscertifikat. Myndigheten för digitalisering och befolkningsdata är förmedlingstjänst för det egna identifieringsverktyget.

När man granskar marknaden för identifieringstjänster för stark autentisering som helhet kan man konstatera att i och med att leverantörer av tjänster för identifieringsförmedling har kommit ut på marknaden har marknadskonstellationerna förändrats kännbart och förmedlingstjänsternas marknadsandel av försäljningen för e-tjänster är redan avsevärd. En enskild förmedlingstjänsts marknadsandel påverkas i hög grad av huruvida förmedlingstjänsten på grundval av konkurrensutsättning levererar identifiering till den offentliga sektorn. Ansvaret för anskaffningen av stark autentisering för hela den offentliga förvaltningens del och förmedlingen av den till organisationerna via förmedlingstjänsten Suomi.fi-identifikation har centraliserats till Myndigheten för digitalisering och befolkningsdata.

E-tjänster, såsom webbutiker och elektroniska tjänster inom den offentliga förvaltningen, skaffar stark autentisering för sina tjänster centralt från förtroendenätet. Tidigare har utmaningen varit att leverantörer av elektroniska tjänster inte har kunnat skaffa identifiering av kunder som använder olika identifieringsverktyg på ett samlat sätt och faktiskt konkurrensutsätta elektroniska identifieringstjänster och de har sålunda inte kunnat aktivt kontrollera de kostnader som användningen av identifieringstjänster orsakar. Genom bestämmelserna om förtroendenätet skapades bättre möjligheter för leverantörer av elektroniska tjänster att påverka och kontrollera kostnaderna för identifiering. Ett syfte med bestämmelserna om förtroendenätet är också att

skapa förutsätter för nya identifieringsverktyg att komma ut på marknaden och för nya affärsmöjligheter i samband med identifiering. Samtidigt är avsikten också att garantera att användningen av de nuvarande identifieringsverktygen kan fortsätta ostörd.

Autentiseringslagen känner för närvarande inga situationer där en leverantör av ett identifieringsverktyg för stark autentisering skulle tillhandahålla verktyget utan att höra till leverantörsnätet eller där stark autentisering skulle tillhandahållas utanför förtroendenätet. Inom ramen för den nuvarande lagstiftningen är det möjligt att tillhandahålla identifieringstjänster utan att göra anmälan till Transport- och kommunikationsverket, men då har leverantören av identifieringstjänster inte ställning som leverantör av tjänster för stark autentisering. Leverantören har då inte heller verifierade bevis på att leverantören i sin verksamhet uppfyller samma krav som leverantörerna av identifieringstjänster i förtroendenätet och leverantören omfattas inte av Transport- och kommunikationsverkets tillsyn.

För närvarande är Myndigheten för digitalisering och befolkningsdata den viktigaste enskilda köparen av identifieringstjänster, som centralt förmedlar identifieringstjänster till den offentliga förvaltningen via Suomi.fi-identifikation. Om man inte beaktar de identifieringstransaktioner där det är fråga om identifiering i identifieringsverktygsleverantörens egna tjänster, som inte omfattas av lagstiftningen om stark autentisering och dess tillämpningsområde, så riktas uppskattningsvis cirka 60–75 procent av identifieringstransaktionerna till den offentliga förvaltningens tjänster via Suomi.fi-identifikation. Myndigheten för digitalisering och befolkningsdata är en viktig kund för leverantörerna av identifieringstjänster. Aktörer inom den offentliga förvaltningen är ofta genom lagstiftning förpliktade att använda stark autentisering i sina e-tjänster, där personuppgifter eller annars sekretessbelagd information behandlas.

Resten, uppskattningsvis cirka 25–40 procent av identifieringstransaktionerna riktas till e-tjänster som tillhandahålls av aktörer i den privata sektorn och den tredje sektorn. Många aktörer i den privata sektorn berörs av skyldighet till stark autentisering av sina kunder, och därför har de infört stark autentisering i sina e-tjänster. Det viktigaste användningsområdet för stark autentisering i den privata sektorn hänför sig till uträttande av ärenden och betalning i nätbanken. Andra som använder stark autentisering av sina kunder i den privata sektorn är bland annat apotek, läkarstationer och andra företag som tillhandahåller hälso- och sjukvårdstjänster, försäkringsbolag, teleföretag, elföretag, postserviceföretag och företag som tillhandahåller resetjänster. Användningen av stark autentisering i den privata sektorns och den tredje sektorns e-tjänster är dock fortfarande i utvecklingsfasen och i största delen av tjänsterna används inte stark autentisering. Tillväxtpotentialen för identifieringstjänsterna för stark autentisering i den privata sektorns och tredje sektorns e-tjänster är således stor.

Antalet identifieringstransaktioner som gjorts via Suomi.fi-identifikation med ett identifieringsverktyg för stark autentisering i den offentliga förvaltningens tjänster har ökat snabbt. År 2017 gjordes cirka 55 miljoner identifieringar via Suomi.fi-identifikation, medan antalet identifieringar 2018 var cirka 82 miljoner och 2019 107 miljoner. Den snabba utvecklingen förklaras av att under 2017–2019 har den offentliga förvaltningens tjänster i snabbt takt digitaliserats och för användning av tjänsterna har det krävts stark autentisering av kunden. Den snabba tillväxten har dock planat ut och medan den årliga ökningen av antalet identifieringstransaktioner 2018 var cirka 50 procent jämfört med föregående år, var tillväxten 2019 bara 31 procent. Något motsvarande lika heltäckande material om användningen av identifieringsverktyg i privata e-tjänster finns inte tillgängligt på grund av att informationen är splittrad och omfattas av företagshemlighet.

Det kan förväntas att antalet identifieringstransaktioner i den offentliga förvaltningens tjänster kommer att plana ut ytterligare, och 2021 och 2022 kommer den årliga tillväxten enligt uppskattningar som gjordes hösten 2021 att vara cirka 20 procent. Därefter antas tillväxten plana ut ytterligare. År 2020 orsakade coronan ett större språng än förväntat, en ökning på cirka 36 procent jämfört med föregående år, men antalet transaktioner 2020 antas ange ny nivå för transaktionerna under kommande år. De största aktörerna i den offentliga sektorn har i huvudsak digitaliserat sina tjänster, så några betydande språng är inte längre att vänta, men användarnas övergång till e-tjänster ger tillväxt några år till. Därefter förväntas antalet identifieringstransaktioner plana ut till en årlig tillväxttakt på cirka 10 procent.

### 2.5 Myndigheten för digitalisering och befolkningsdatas certifikattjänster

Bestämmelser om Myndigheten för digitalisering och befolkningsdatas certifikattjänster finns i lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata (661/2009, nedan *BDS-lagen*), närmare bestämt i lagens 6 kap. I lagens 61 § föreskrivs det om tjänster som tillhandahålls vid certifierad elektronisk kommunikation och enligt dess 1 mom. ska Myndigheten för digitalisering och befolkningsdata producera, tillhandahålla och administrera medborgarcertifikat som är avsedda att användas vid certifierad elektronisk kommunikation samt certifikatregistertjänster och spärrlisttjänster som direkt hänför sig till användningen av medborgarcertifikat. Enligt 61 § 2 mom. i BDS-lagen får Myndigheten för digitalisering och befolkningsdata dessutom producera följande tjänster som används vid certifierad elektronisk kommunikation: 1) tillhandahållande och administrering av andra certifikat än medborgarcertifikat, 2) verifiering av parterna vid certifierad elektronisk kommunikation och administrering av kommunikationen, 3) elektronisk signering och kryptering av elektroniska handlingar och meddelanden, 4) bevarande och verifiering av äktheten, konfidentialiteten och integriteten i fråga om elektroniska handlingar och meddelanden, 5) verifiering av aktörernas ställning eller roll vid certifierad elektronisk kommunikation, 6) tillhandahållande och administrering av certifikatregistertjänster och spärrlisttjänster som hänför sig till användningen av andra certifikat än medborgarcertifikat, 7) tillhandahållande och administrering av certifierade tidsstämplingstjänster, 8) tillhandahållande av andra motsvarande funktioner eller tjänster som gäller certifierad elektronisk kommunikation.

Med medborgarcertifikat avses ett certifikat som utfärdats av Myndigheten för digitalisering och befolkningsdata för en fysisk person och som ingår i ett i lagen om identitetskort avsett identitetskort eller i en annan myndighetshandling eller ett tekniskt underlag och som används för verifiering av personen, för elektroniska underskrifter och för kryptering av handlingar och meddelanden. Med medborgarcertifikat avses också ett av Myndigheten för digitalisering och befolkningsdata utfärdat certifikat som ingår i en annan myndighetshandling eller ett tekniskt underlag och som används i ovannämnda syfte och som uppfyller kraven i EU:s förordning om elektronisk identifiering. Medborgarcertifikat ska innehålla en elektronisk kommunikationskod som identifierar innehavaren av certifikatet eller någon annan identifieringsuppgift som identifierar personen och som inte innehåller information om personen. Även andra nödvändiga tekniska uppgifter som behövs vid användningen av ett certifikat kan ingå i medborgarcertifikat och andra certifikat som Myndigheten för digitalisering och befolkningsdata utfärdar för fysiska personer. Beslut om dessa uppgifter fattas av Myndigheten för digitalisering och befolkningsdata. På ansökan om medborgarcertifikat som ingår i ett identitetskort tillämpas lagen om identitetskort.

När uppgifter om en person första gången registreras i befolkningsdatasystemet ska han eller hon tilldelas en sådan individuell teknisk identifieringskod som behövs när en elektronisk kommunikationskod ska skapas. De tekniska identifieringskoderna skapas automatiskt i befolkningsdatasystemet. Enligt 63 § 2 mom. ska Myndigheten för digitalisering och befolkningsdata

ändra en teknisk identifieringskod till en individuell elektronisk kommunikationskod när 1) ett medborgarcertifikat eller ett annat certifikat som Myndigheten för digitalisering och befolkningsdata utfärdar för fysiska personer första gången utfärdas för en person, eller 2) en person vars uppgifter registrerats i befolkningsdatasystemet inte har en elektronisk kommunikationskod och Myndigheten för digitalisering och befolkningsdata av en i 43 § 2 mom. 2 punkten avsedd certifikatutfärdare får en begäran om att ändra personens tekniska identifieringskod till en elektronisk kommunikationskod.

Medborgarcertifikat och andra certifikat för fysiska personer som Myndigheten för digitalisering och befolkningsdata utfärdar och som används allmänt vid elektronisk kommunikation samt uppgifterna i dem får registreras i ett offentligt register som förs av Myndigheten för digitalisering och befolkningsdata och som var och en har rätt att få uppgifter ur i enlighet med bestämmelserna om myndigheternas offentliga handlingar i lagen om offentlighet i myndigheternas verksamhet (621/1999, nedan *offentlighetslagen*).

### 2.6 Elektronisk identifiering i den offentliga förvaltningens tjänster

Bestämmelser om myndigheternas skyldighet att tillhandahålla sina tjänster digitalt finns i lagen om tillhandahållande av digitala tjänster (306/2019). Enligt lagens förarbeten är lagen om tillhandahållande av digitala tjänster en speciallag som kompletterar förvaltningslagen och andra allmänna förvaltningslagar, där de särskilda krav som ställs på digitala tjänster definieras och lika möjligheter för var och en att sköta sina ärenden oberoende av tjänstens art tryggas och behoven hos grupper med särskilda behov i samhället tillgodoses när det gäller tillgången till tjänster.

Enligt 2 kap. 5 § i lagen om tillhandahållande av digitala tjänster ska myndigheterna ge alla en möjlighet att med hjälp av digitala tjänster eller andra elektroniska dataöverföringsmetoder sända elektroniska meddelanden och handlingar som hänför sig till deras behov att uträtta ärenden. I praktiken betyder bestämmelsen att myndigheterna är skyldiga att ordna sina tjänster så att elektronisk kommunikation är möjlig i alla ärenden som hänför sig till myndighetens ansvarsområde och befogenheter. Eftersom det i lagen om tillhandahållande av digitala tjänster föreskrivs om skyldighet för myndigheterna att ge förvaltningens kunder möjlighet att sända elektroniska meddelanden till myndigheterna, är möjligheten att uträtta ärenden inte begränsad till anhängiggörandet av ärenden. Man måste kunna uträtta ärenden hos myndigheterna med hjälp av digitala tjänster och andra elektroniska dataöverföringsmetoder av vilken orsak som helst som har att göra med förvaltningens kunders behov av att uträtta ärenden inom förvaltningen.

Med stöd av det som föreskrivs i lagen om tillhandahållande av digitala tjänster måste alla anhängiggöranden och interimistiska åtgärder under behandlingen av ett ärende kunna skötas även elektroniskt, om det inte föreskrivs något annat i lagen, eftersom i lagen nämns också elektroniska handlingar som måste kunna sändas till myndigheterna med hjälp av elektroniska dataöverföringsmetoder som de använder. Bestämmelsen i lagens 2 kap. baserar sig således inte bara på sändande av meddelanden mellan myndigheter och förvaltningens kunder utan den innebär att det för myndigheterna föreskrivs en heltäckande skyldighet att ordna möjlighet att uträtta ärenden elektroniskt och tillhandahålla digitala tjänster inom myndighetens ansvarsområde. Lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003) stödjer för sin del genom sina procedurbestämmelser ordnandet av digitala tjänster och uträttandet av ärenden elektroniskt hos myndigheterna.

Enligt 6 § i lagen om tillhandahållande av digitala tjänster föreskrivs det att ett krav på stark autentisering endast kan införas då det finns ett motiverat behov av stark autentisering på grund

av behovet att säkerställa en användares åtkomsträttigheter i anslutning till en tjänst eller dess datainnehåll eller på grund av rättsverkningarna av en åtgärd som utförs i tjänsten. Om det är möjligt att få se och använda sekretessbelagt datainnehåll i en digital tjänst, ska tjänsteanvändaren identifieras med hjälp av stark autentisering. Med stöd av paragrafen är det dock möjligt att av vägande och motiverade skäl använda någon annan motsvarande informationssäker identifieringstjänst.

I regeringens proposition till riksdagen med förslag till lag om tillhandahållande av digitala tjänster och lag om ändring av lagen om elektronisk kommunikation i myndigheternas verksamhet (RP 60/2018) preciseras de situationer där stark autentisering bör krävas. Enligt förarbetena ska myndigheterna med stöd av lagen om tillhandahållande av digitala tjänster från fall till fall bedöma behovet av identifiering i sina tjänster. En myndighet ska kunna kräva stark autentisering till exempel när en användare i en tjänst kan se uppgifter om sig själv eller om en person som han eller hon företräder med stöd av ett bemyndigande. Stark autentisering ska dock användas särskilt i tjänster där användaren kommer åt att se eller hantera uppgifter om sitt hälsotillstånd, andra uppgifter inom särskilda kategorier av personuppgifter, uppgifter om en klientrelation i socialvården, uppgifter om elevvård samt företags- och yrkeshemligheter. (RP 60/2018 rd)

I annan lagstiftning finns det relativt få bestämmelser om när det förutsätts uttryckligen stark autentisering för att uträtta ärenden elektroniskt. Exempelvis i 18 § i lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003) förutsätts i samband med bevislig delvisning en identifieringsteknik som är datatekniskt tillförlitlig och bevislig. Speciallagstiftningen innehåller emellertid en del bestämmelser om styrkande av identiteten vid elektronisk kommunikation som gäller ett visst ansvarsområde eller en viss tjänst. Då kan det i lagen förutsättas antingen identifieringsverktyg för stark autentisering enligt autentiseringslagen eller något annat informationssäkert identifieringssätt. Speciallagarna kan också allmänt förutsätta att identiteten kan bevisas på ett tillförlitligt sätt. Särskilt vid elektronisk kommunikation i samband med hälso- och sjukvård kan det på lagnivå uttryckligen förutsättas stark autentisering enligt autentiseringslagen.

Syftet med lagen om förvaltningens gemensamma stödtjänster för e-tjänster (571/2016, nedan *lagen om stödtjänster*) är att förbättra tillgången och kvaliteten på offentliga tjänster, att förbättra tjänsternas informationssäkerhet och interoperabilitet samt styrningen av tjänsterna och att främja effektiviteten och produktiviteten inom den offentliga förvaltningens verksamhet. Lagen innehåller bestämmelser om den offentliga förvaltningens gemensamma stödtjänster för e-tjänster. Med stödtjänst avses en sådan gemensam stödtjänst för e-tjänster som användarorganisationen (t.ex. en myndighet) använder som stöd för sina elektroniska tjänster eller för någon annan uppgift som den har eller tjänst som den tillhandahåller. I lagen föreskrivs det om stödtjänsternas funktionaliteter, om ansvar och uppgifter för dem som tillhandahåller tjänster samt om behandlingen av personuppgifter och andra uppgifter för produktionen av stödtjänster. I lagen föreskrivs det också om skyldighet och rätt att använda gemensamma stödtjänster. Produktionen av stödtjänster är med vissa undantag koncentrerad till Myndigheten för digitalisering och befolkningsdata.

Organisationer inom den offentliga förvaltningen är enligt lagen om stödtjänster förpliktade att för stark autentisering i första hand använda en sådan tjänst för identifiering av fysiska personer som avses i 3 § 4 punkten i lagen, och som identifierar en fysisk person som använder den offentliga förvaltningens e-tjänster med hjälp av en tjänst som tillhandahålls av en sådan leverantör av identifieringstjänster som avses i autentiseringslagen, administrerar identifieringstransaktionen och till användarorganisationen lämnar ut identifieringsuppgifter om en person ur

befolkningsdatasystemet (Suomi.fi-identifikation). Organisationer inom den offentliga förvaltningen ska i princip använda Suomi.fi-identifikation i e-tjänster där stark autentisering behövs.

### 2.7 Kommissionens förslag till ändring av eIDAS-förordningen

Kommissionen överlämnade i juni 2021 ett förslag till förordning om ändring av Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller inrättandet av en ram för europeisk digital identitet (COM (2021) 281 final). Det är alltså fråga om ett förslag till ändring av eIDAS-förordningen som det redogörs mer ingående för i avsnitt 2.3 (senare *eIDAS-ändringsförslaget)*. Genom förslaget skapas en enhetlig rättslig ram för en applikation för en europeisk e-identitetsplånbok. Genom förslaget vill man särskilt säkerställa att alla i EU har tillgång till pålitliga och säkra digitala id-lösningar. Målet är dessutom att tjänsteleverantörer inom den offentliga och den privata sektorn kan lita på de digitala id-lösningar som utvecklas när användarna uträttar ärenden och identifierar sig i deras tjänster.

Genom eIDAS-ändringsförslaget skapas en enhetlig rättslig ram för en applikation för en europeisk e-identitetsplånbok. Detta är den viktigaste reformen enligt ändringsförslaget. En av plånboksapplikationens viktigaste funktioner är att möjliggöra elektronisk identifiering för applikationsanvändaren. Dessutom kan den som använder plånboksapplikationen styrka personuppgifter och intyg som gäller honom eller henne samt skapa elektroniska underskrifter. Enligt förslaget ska alla medlemsländer vara skyldiga att tillhandahålla åtminstone en applikation för en elektronisk plånbok enligt förordningen. Plånboksapplikationen kan produceras av den offentliga eller den privata sektorn. Det ska vara avgiftsfritt och frivilligt för medborgarna att använda plånboksapplikationen. Enligt förslaget ska plånboksapplikationen kunna användas i så stor utsträckning som möjligt i samhällets tjänster i såväl den offentliga som den privata sektorn.

eIDAS-ändringsförslaget innehåller också gemensamma krav på sådana betrodda tjänster som gör det möjligt att tillhandahålla personuppgifter och intyg (enligt förordningen elektroniska attesteringar av attribut). Organisationer och enheter ska kunna tillhandahålla personuppgifter och intyg som de utfärdat (såsom examensbevis och intyg) elektroniskt som en betrodd tjänst i användarens plånboksapplikation. Förordningen definierar kraven på den tjänst som tillhandahålls, dvs. elektroniska attesteringar av attribut samt leverantören. Genom att tillhandahålla sina tjänster i enlighet med förordningens krav kan en leverantör visa att den tjänst som leverantören tillhandahåller är tillförlitlig. För att öka tillförlitligheten har en leverantör av betrodda tjänster möjlighet att ansöka om myndighetsgodkännande för sin tjänst.

En U-skrivelse som innehåller Finlands ståndpunkt har utarbetats om kommissionens förslag för riksdagen (U 41/2021 rd, https://www.eduskunta.fi/SV/vaski/Kirjelma/Documents/U_41+2021.pdf). Kommissionens förslag har börjat behandlas i rådets arbetsgrupp för telekommunikation.

När behandlingen av eIDAS-ändringsförslaget i sinom tid slutförs blir det aktuellt att bedöma nationellt huruvida man vill fortsätta att förenhetliga den nationella lagstiftningen med eIDAS-förordningen. För närvarande har man velat förenhetliga de nationella kraven på stark autentisering med eIDAS-förordningens krav på det sätt som beskrivs mer ingående i avsnitt 2.3. I vilket fall som helst håller världen för digital identitet och e-tjänster även nationellt på att utvecklas i en riktning där en person själv kontrollerar delningen av uppgifter som gäller honom eller henne till tredje parter med hjälp av nya lösningar i anslutning till hantering av identiteten. Utifrån det lagstiftningsförslag som gäller eIDAS-förordningen håller man i EU på att utveckla plånboksapplikationen för europeisk digital identitet till en sådan lösning. På det sätt som beskrivits ovan är det möjligt att eIDAS-förordnignen i framtiden kommer att förplikta medlemsstaterna att tillhandahålla plånboksapplikationer enligt förordningen.

Den målsatta tidtabellen för behandlingen av eIDAS-ändringsförslaget är ambitiös och i detta skede är det fortfarande osäkert enligt vilken tidtabell förordningen kan träda i kraft. Det är emellertid viktigt att redan nu utveckla nya lösningar för digital identitet och göra dem tillgängliga. Det nationella utvecklingsarbetets framskridande bör inte heller vara helt och hållet bundet till EU-beredningen. Trots detta är det emellertid mycket viktigt att på nationell nivå också fästa uppmärksamhet vid utvecklingsarbetet på EU-nivå för att undvika överlappande utvecklingsarbete och kostnader. Utvecklingsarbetet på nationell nivå bör i vilket fall som helst redan i detta skede vara så enhetligt som möjligt med den kommande eIDAS-regleringen och skapa förutsättningar för att i framtiden skapa även plånboksapplikationer som uppfyller eIDAS-förordningens krav.

## 3 Målsättning

Propositionens mål är att främja målet i statsminister Marins regeringsprogram att Finland är känt som ett föregångarland där de möjligheter som digitaliseringen och den tekniska utvecklingen medför utvecklas och tillvaratas över förvaltnings- och sektorsgränserna. Målet är att höja teknik- och digitaliseringsberedskapen hos den offentliga sektorn och utveckla samarbetet mellan den offentliga sektorn och den privata sektorn. Propositionens mål är dessutom i enlighet med regeringsprogrammet att finska medborgare och alla som bor i Finland ska ges möjlighet till elektronisk identifiering samt att främja utvecklingen av fungerande identifieringslösningar. Målet främjas genom att lagstiftningen möjliggör att Myndigheten för digitalisering och befolkningsdata producerar de behövliga tjänsterna för digital identitet samt att Polisen tillhandahåller de digitala identitetskort som i stor utsträckning används i samhällets tjänster.

Genom propositionen främjas också en persons möjligheter att själv hantera sina egna uppgifter i offentliga tjänster (s.k. självägd identitet, Self-sovereign identity), vilket också är inskrivet i regeringsprogrammet. Målet är att i den första fasen göra det möjligt för en person att själv visa vissa uppgifter om sin identitet, samt att skapa grundläggande lösningar och praxis för att visa självägda myndighetsuppgifter, så att utvecklingen kan föras vidare i framtiden.

Ett viktigt mål för propositionen är dessutom att göra det möjligt för utlänningar att identifiera sig i e-tjänster på ett likvärdigt sätt. Genom att utöka Myndigheten för digitalisering och befolkningsdatas uppgifter med produktion av ett e-tjänstverktyg för utlänningar och genom att skapa lagstiftningsmässiga förutsättningar för nyttjande av e-tjänstverktyget är strävan att förbättra utlänningars möjligheter att uträtta ärenden i finländska e-tjänster. Dessutom är propositionens mål att främja möjligheten att uträtta ärenden elektroniskt även för personer som inte kan eller vill använda smarttelefon. Propositionens mål är dessutom att säkerställa att den offentliga förvaltningens kostnader för stark autentisering är förutsägbara.

## 4 Förslagen och deras konsekvenser

### 4.1 De viktigaste förslagen

*Allmänt*

I propositionen föreslås ny lagstiftning om sådana nya tjänster för uträttandet av ärenden digitalt som myndigheterna producerar, samt en funktionell förändring i anslutning till produktionen och användningen av dem. I propositionen föreslås att det ska produceras e-legitimation, e-tjänstverktyg för utlänningar och identifieringsverktyg för fysiska personer. De utgör nya lösningar för att styrka identiteten och visa personuppgifter samt för elektronisk identifiering som är avsedda för fysiska personer. Syftet med dem är att säkerställa att personer som anlitar det

finländska samhällets tjänster har omfattande möjlighet att visa upp en av myndigheterna bestyrkt identitet samt bestyrkta uppgifter i anslutning till identiteten i olika situationer.

Vad gäller e-legitimationen och e-tjänstverktyget för utlänningar handlar det om en utveckling av möjligheten för personer att själva välja vilka personuppgifter som visas upp. Att tillhandahålla en persons egna uppgifter i en digital miljö så att personen själv kan hantera dem kallas allmänt självägd identitet. Med självägd identitet (eng. Self-Sovereign Identity, SSI) avses en modell för behandling av personuppgifter där personen själv kan hantera visandet av personuppgifter som härrör från honom eller henne själv eller en betrodd tredje part i en e-tjänst där personuppgifter behövs. Med principen om självägd identitet avses alltså att personerna hanterar sina personuppgifter själva, dvs. bestämmer hur de ska användas. I detta skede begränsas dock de självägda personuppgifterna till de uppgifter som kan härledas från de identitetshandlingar som ligger till grund för e-legitimationen eller e-tjänstverktyget för utlänningar.

*Tjänster för digital identitet och bevis för kärnidentitet*

I propositionen föreslås det att det stiftas en ny lag om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata. Enligt den föreslagna lagstiftningen ska det i fortsättningen vara Myndigheten för digitalisering och befolkningsdatas uppgift att producera ett informationssystem för digital identitet, som består av en applikation för digital identitet och ett därtill anslutet bakomliggande system. I praktiken är det är fråga om att Myndigheten för digitalisering och befolkningsdata ska producera en applikation som laddas ned i en persons mobila terminal och med vars hjälp det är möjligt att använda e-legitimationen eller e-tjänstverktyget för utlänningar. Den applikation som Myndigheten för digitalisering och befolkningsdata producerar ska fungera som teknisk plattform för e-legitimationen och e-tjänstverktyget för utlänningar. Lagen ska innehålla väsentliga informationssäkerhetskrav och kräva att informationssystemet regelbundet genomgår bedömning av ett bedömningsorgan för informationssäkerhet. I lagen ska det dessutom föreskrivas att informationssystemet ska uppfylla samma krav som för närvarande förutsätts av verktyg för stark autentisering.

I propositionen föreslås det dessutom att Myndigheten för digitalisering och befolkningsdata ska producera bevis för kärnidentitet. Beviset för kärnidentitet är en central del av den föreslagna lagstiftningshelheten, eftersom ett gällande bevis för kärnidentitet ska vara en förutsättning för att använda e-legitimationen och e-tjänstverktyget för utlänningar. Beviset för kärnidentitet ska vara ett tekniskt tillförlitligt sätt att elektroniskt visa att den som förfogar över beviset har en identitet som är registrerad i befolkningsdatasystemet. Med andra ord är det fråga om bestyrkta och tekniskt kontrollerbara uppgifter om att en person har en i Finland registrerad identitet som fortfarande är i kraft. I praktiken är beviset på kärnidentitet i den första fasen ett certifikat. Myndigheten för digitalisering och befolkningsdata upprättar, beviljar och registrerar ett bevis för kärnidentitet när en person tar i bruk e-legitimationen eller e-tjänstverktyget för utlänningar.

*E-legitimation*

I propositionen föreslås det att det stiftas en ny lag där det föreskrivs om e-legitimation. En e-legitimation gör det möjligt för innehavaren att styrka identiteten samt att visa vissa bestyrkta uppgifter som gäller honom eller henne. Det är fråga om de bestyrkta uppgifter som kan härledas ur en sådan identitetshandling som ligger till grund för e-legitimation, dvs. i praktiken uppgifter i personens gällande pass eller identitetskort. E-legitimationen ska dock inte fungera som resedokument. I propositionen föreslås det att e-legitimationen ska grunda sig på principen om självägd identitet. Härmed avses att en person själv kan bestämma för vem han eller hon vill visa

de uppgifter om honom eller henne som finns i e-legitimationen och vilka uppgifter han eller hon vill visa. Myndigheten ska inte ha någon möjlighet att bestämma om visandet av uppgifter och myndigheten ska inte ha tillträde till uppgifterna i e-legitimationen.

Enligt den lagstiftning som föreslås i propositionen ska en person direkt med stöd av ett giltigt identitetskort eller pass ha rätt att få en e-legitimation. Ett temporärt identitetskort eller ett sådant identitetskort för minderårig som har utfärdats för en person under 15 år, ett tillfälligt pass eller ett nödpass ska däremot inte ge rätt till en e-legitimation. I propositionen föreslås det att i lagen om identitetskort och passlagen intas uttryckliga bestämmelser om vilka identitetshandlingar som ger rätt till en e-legitimation. En e-legitimation är således inte en ny typ av ärende och den utfärdas inte separat, utan rätten att ta i bruk en e-legitimation uppstår direkt med stöd av ett giltigt identitetskort eller pass. Även om en person har rätt till en e-legitimation ska det vara helt frivilligt att i praktiken ta den i bruk. Det ska vara avgiftsfritt att ta i bruk e-legitimationen.

Enligt den lagstiftning som föreslås i propositionen ska e-legitimationen kunna användas för att styrka identiteten då man uträttar ärenden på plats hos en tjänsteleverantör på samma sätt som man nu använder identitetskort och pass. Dessutom ska e-legitimationen kunna användas för att styrka identiteten i e-tjänster på samma sätt som de nuvarande identifieringsverktygen för stark autentisering. För att möjliggöra detta föreslås i propositionen ändringar i autentiseringslagen, där definitionen av stark autentisering ändras så att den också omfattar elektronisk identifiering med hjälp av e-legitimation. Sålunda ska elektronisk identifiering med hjälp av e-legitimation likställas med elektronisk identifiering med hjälp av de nuvarande identifieringsverktygen för stark autentisering.

I propositionen föreslås dessutom att det i fortsättningen föreskrivs i autentiseringslagen om en ny roll som leverantör av tjänster för digital identitet och tjänsteleverantörensskyldighet att tillhandahålla e-legitimation för förmedling i förtroendenätet. I praktiken är Myndigheten för digitalisering och befolkningsdata den leverantör av tjänster för digital identitet som avses i autentiseringslagen. Bestämmelserna gör det möjligt att använda e-legitimation i den privata sektorns e-tjänster via förtroendenätet samt att nyttja dem när leverantörerna av de nuvarande identifieringsverktygen gör den så kallade inledande identifieringen av den som ansöker om ett elektroniskt identifieringsverktyg. Enligt den föreslagna lagstiftningen blir leverantören av tjänster för digital identitet ändå inte part i förtroendenätet och autentiseringslagen ska tillämpas på leverantören av tjänster för digital identitet endast till de delar som det föreskrivs uttryckligen om det.

*E-tjänstverktyg för utlänningar*

I propositionen föreslås det bestämmelser om ett nytt e-tjänstverktyg för utlänningar. E-tjänstverktyget ska göra det möjligt att styrka innehavarens identitet samt att visa vissa andra bestyrkta uppgifter. Det är fråga om uppgifter som kan härledas ur den utländska identitetshandling som ligger till grund för e-tjänstverktyget samt om en finsk personteckning som registrerats för utlänningen. I propositionen föreslås det på samma sätt som i fråga om e-legitimationen att också e-tjänstverktyget för utlänningar ska fungera enligt principen om självägd identitet, dvs personen kan själv kontrollera vilka personuppgifter som visas upp. E-tjänstverktyget ska dock kunna användas endast i e-tjänster, eftersom det inte är möjligt att i det införa en sådan ansiktsbild av innehavaren som är en förutsättning för tillförlitligt uträttande av ärenden ansikte mot ansikte. E-tjänstverktyget främjar dock utlänningars möjlighet att uträtta ärenden elektroniskt och förhindrar att parallella identiteter uppkommer i myndigheternas register.

Enligt förslagen i propositionen ska Myndigheten för digitalisering och befolkningsdata utfärda e-tjänstverktyg för utlänningar. För att ett e-tjänstverktyg ska utfärdas förutsätts att personen registreras i befolkningsdatasystemet så att en utländsk medborgare beviljas en personbeteckning i samband med förfarandet. Här har förslagen i denna proposition kopplingar till förslagen i propositionen som gäller en reform av personbeteckningen, för i och med dem ska det bli möjligt att bevilja personbeteckning till en större grupp personer än tidigare. Dessutom ska personbeteckning kunna beviljas i ett förfarande för distansregistrering utan att en utländsk medborgare kommer till Finland. Också e-tjänstverketyget för utlänningar ska kunna tas i bruk i samband med förfarandet för distansregistrering. E-tjänstverktyget för utlänningar ska vara avgiftsbelagt så att ibruktagandet innehåller en myndighetsavgift. Därefter ska det dock vara avgiftsfritt att använda e-tjänstverktyget

Enligt förslagen i propositionen ska det kunna finnas två typer av e-tjänstverktyg för utlänningar beroende på hur innehavaren av e-tjänstverktyget har identifierats när e-tjänstverktyget utfärdades. Förfarandet för distansregistrering når inte upp till samma tillitsgrad som identifiering av en person ansikte mot ansikte, och av denna orsak ska ett e-tjänstverktyg som utfärdats enbart med stöd av distansregistrering duga i e-tjänster endast när stark autentisering inte förutsätts. Med andra ord motsvarar tillförlitligheten hos ett e-tjänstverktyg som utfärdats enbart med stöd av distansregistrering inte ett identifieringsverktyg för stark autentisering. Enligt förslagen ska e-tjänsterna själv kunna bestämma i vilka tjänster identifiering kan godkännas med e-tjänstverktyg med lägre tillförlitlighet än stark autentisering.

E-tjänstverktyget för utlänningar ska dock kunna nå upp till samma tillitsnivå som stark autentisering när personen i något skede har identifierats ansikte mot ansikte. Utlänningen kan till exempel komma till Finland senare, varvid han eller hon kan besöka Myndigheten för digitalisering och befolkningsdata, där han eller hon kan identifieras. Efter identifiering ansikte mot ansikte kan e-tjänstverktyget för utlänningar användas i e-tjänster också när stark autentisering förutsätts. För att möjliggöra detta föreslås i propositionen motsvarande ändringar i autentiseringslagen som i fråga om e-legitimation. Ändringarna stärker i dessa situationer statusen för e-tjänstverktyget för utlänningar vid stark autentisering och gör det möjligt att förmedla e-tjänstverktyget i förtroendenätet.

*Identifieringsverktyg för fysiska personer*

I propositionen föreslås dessutom bestämmelser om identifieringsverktyg för fysiska personer. Identifieringsverktyg för fysiska personer ska kunna beviljas personer under motsvarande förutsättningar som identifieringsverktyg för stark autentisering beviljas för närvarande. Identifieringsverktyget för fysiska personer ska också vad funktionen och tillförlitligheten beträffar motsvara de nuvarande identifieringsverktygen för stark autentisering. Det ska vara avgiftsbelagt att ta i bruk identifieringsverktyget för fysiska personer, men därefter ska dess användning vara avgiftsfri.

Identifieringsverktyget för fysiska personer är avsett för sådana personer som inte har möjlighet att eller inte vill använda det digitala identitetsbeviset därför att det fungerar med hjälp av en mobilapplikation i en smarttelefon. Identifieringsverktyget för fysiska personer ska kunna användas endast i enlighet med lagen om stödtjänster och det ska enbart möjliggöra elektronisk identifiering i myndigheternas e-tjänster. Sålunda gör identifieringsverktyget det möjligt för var och en att använda den offentliga sektorns e-tjänster. Identifieringsverktyget ska inte tillhandahållas som identifieringsverktyg i förtroendenätet och det ska således inte vara möjligt att identifiera sig med det i den privata sektorns e-tjänster.

## 4.2 Huvudsakliga konsekvenser

### 4.2.1 Ekonomiska konsekvenser

#### 4.2.1.1 Konsekvenser för hushållen

Förslagen bedöms i någon mån ha konsekvenser för hushållens ekonomiska ställning, men de kan betraktas som måttliga på individnivå. Får att få en e-legitimation eller ett identifieringsverktyg för fysiska personer förutsätts det att man har ett giltigt pass eller identitetskort, vilka är avgiftsbelagda handlingar som utfärdas av myndigheterna. När det gäller e-legitimation är det fråga om en tilläggstjänst till dessa handlingar. För närvarande har cirka 4,1 miljoner finländare ett giltigt pass eller identitetskort, och av dem är cirka 580 000 minderåriga. Varje år utfärdas sammanlagt 1,1 miljoner pass och identitetskort, och det finns sammanlagt cirka 4,8 miljoner giltiga pass och identitetskort. Förslaget har således konsekvenser för en mycket stor grupp finländare. Som bakgrund till siffrorna bör man beakta att i och med de ändringar av autentiseringslagen som trädde ikraft vid ingången av 2019 har det inte längre varit möjligt att få de bankkoder som behövs till exempel för att använda nätbanken utan pass eller identitetskort.

Det föreslås att kostnaderna för e-legitimation och produktionen av dem delvis läggs till kostnaderna för pass och identitetskort i enlighet med lagen om grunderna för avgifter till staten. Kostnaderna för e-legitimation ökar de fasta kostnaderna för produktionen av pass och identitetskort med cirka 3 euro per utfärdad handling (uppskattningsvis 1,1 miljoner beviljade handlingar per år). Förslaget inverkar således eventuellt på priset på pass och identitetskort. Priset på pass och identitetskort varierar årligen på grund av antalet utfärdade handlingar, så förslagens slutliga konsekvenser för medborgarna är också beroende av andra faktorer. Priset på pass är 44–50 euro och priset på identitetskort 54–60 euro 2022. Priset på bägge handlingarna är förmånligare vid elektronisk ansökan. Förslaget medför ett måttligt tryck på att höja priset på pass eller identitetskort. Utöver myndighetskostnaderna för pass och identitetskort bör också priset på fotografiet beaktas (cirka 0–20 euro). Ur denna synvinkel är förslagets ekonomiska konsekvenser för hushållen tämligen måttliga.

I samband med utkomststöd kan man på vissa villkor få pass eller identitetskort med betalningsförbindelse. För låginkomsttagare som inte är berättigade till utkomststöd kan avgifterna för pass eller identitetskort ändå vara en betydande kostnad.

Användningen av e-legitimation förutsätter att man har en smarttelefon. Enligt Statistikcentralens undersökning Befolkningens användning av informations- och kommunikationsteknik från 2021 använde 88 procent av finländarna en smarttelefon (Finlands officiella statistik (FOS): Befolkningens användning av informations- och kommunikationsteknik (e-publikation), ISSN=2341-8699. 2021. Helsinki. Statistikcentralen. Åtkomstsätt: http://www.stat.fi/til/sutivi/2021/sutivi_2021_2021-11-30_tie_001_fi.html). I åldersklassen 16—54-åringar använder över 96 procent av medborgarna en smarttelefon. Dessutom finns det en surfplatta i 53 procent av hushållen. I Transport- och kommunikationsverket Traficoms konsumentundersökning om användningen av kommunikationstjänster 2021 (https://www.traficom.fi/fi/julkaisut/viestintapalvelujen-kuluttajatutkimus-2021) uppskattar man att 89,7 procent av finländarna har en smarttelefon. Man kan alltså anta att de flesta hushållen har sådan utrustning som förutsätts för e-legitimation, och förslaget innebär därmed inga betydandetilläggskostnader för hushållen.

Förslagets tillitsnivå- och andra informationssäkerhetskrav ställer krav på slutanvändarens mobila enhets informationssäkerhetsegenskaper. Detta innebär att e-legitimationen inte kan användas på en del av de mobila enheter som är i användning. I praktiken har kraven att göra med

skyddet av data i den mobila enheten. Skydd på applikationsnivå är inte tillräckligt med tanke på de planerade lösningarna utan det behövs också skydd på enhetsnivå. Av de Android-enheter som används i Finland uppfyller 80–90 procent för närvarande minimikraven på skydd på enhetsnivå. När det gäller de iOS-telefoner som används i Finland bedöms motsvarande egenskap finnas hos 100 procent av enheterna i början av 2023. Kravet på skydd på enhetsnivå preciseras i och med implementeringen och bedömningarna av informationssäkerheten och detta kan påverka andelen enheter som stöds. På motsvarande sätt förändras andelen enheter som stöds i takt med att enheterna förnyas. Det är emellertid klart att antalet enheter som stöds har betydelse för vilka ekonomiska konsekvenser förslaget har för hushållen.

Enligt förslaget ska identifieringsverktyget för fysiska personer vara en alternativ lösning till den elektroniska identifiering som krävs för att använda den offentliga sektorns e-tjänster, om en person inte vill eller kan använda e-legitimationen som förutsätter en mobil terminal. Det föreslås att produktionen av verktyget för identifiering av fysiska personer delvis finansieras med budgetmedel så att kundpriset subventionernas genom att Myndigheten för digitalisering och befolkningsdata beviljas ett förslagsanslag för de fortlöpande kostnaderna. Då skulle kundpriset för identifieringsverktyget för fysiska personer bli runt eller något under det beräknade självkostnadsvärdet. Man har under beredningen uppskattat att avgiften för kunderna kommer att ligga på mellan 10 och 20 euro. Detta skulle motsvara prisnivån på andra motsvarande tjänster som produceras av den privata sektorn. En avgift skulle ge kunden rätt till högst två enheter under en tidsperiod om 10 år. Det pris som kunden ska betala fastställs närmare genom en förordning som utfärdas separat i enlighet med lagen om grunderna för avgifter till staten.

Förslagen bedöms i någon mån ha konsekvenser också för utlänningar som behöver uträtta ärenden i finländska digitala tjänster. Konsekvenserna kan betraktas som måttliga på personnivå. E-tjänstverktyget för utlänningar kräver att man har ett giltigt pass eller identitetskort i något land. Priset på e-tjänstverktyget för utlänningar uppskattas bli cirka 7 euro baserat på 64 000 användare per år. Det uppskattade antalet användare baserar sig på antalet användare av den identifieringstjänst för utlänningar som Myndigheten för digitalisering och befolkningsdata tillhandahåller för närvarande samt på undervisnings- och kulturministeriets uppskattning av antalet som ansöker om studieplats i Finland. E-tjänstverktygets pris kan variera från år till år beroende på det faktiska antalet användare.

#### 4.2.1.2 Konsekvenser för företagen som tjänsteleverantörer

På detaljmarkanden för tjänster för stark autentisering finns både leverantörer av identifieringsverktyg och leverantörer av tjänster för identifieringsförmedling, som tillhandahåller identifieringstjänster till konsumenter och e-tjänster. Samma företag kan ha bägge rollerna. I Transport- och kommunikationsverkets register finns för närvarande totalt 16 leverantörer av tjänster för stark autentisering. Av dessa tillhandahåller 14 aktörer ett eget identifieringsverktyg för stark autentisering medan det finns åtta identifieringstjänster som förmedlar också andra användares identifiering än det egna identifieringsverktyget för stark autentisering. Av leverantörerna av tjänster för identifieringsförmedling tillhandahåller två enbart förmedlingstjänster, dvs. de har inget eget identifieringsverktyg för stark autentisering som de kan tillhandahålla för e-tjänster. År 2021 har en ny förmedlingstjänsts anmälan om inledande av verksamhet anhängiggjorts. Av leverantörerna av tjänster för identifieringsförmedling av stark autentisering förmedlar sex alla identifieringsverktyg som används i Finland utom Myndigheten för digitalisering och befolkningsdatas person- och organisationscertifikat till e-tjänster.

Leverantörerna av identifieringsverktyg bedöms orsakas både negativa och positiva konsekvenser av förslagen som gäller *e-legitimation*. Å ena sidan, om e-legitimation börjar användas i stor

utsträckning inom e-tjänster och tjänster för identifieringsförmedling, kan detta leda till en situation där affärsmöjligheterna för aktörer som tillhandahåller endast identifieringsverktyg försämras. Detta kan leda till minskat investeringsintresse bland aktörer som tillhandahåller identifieringsverktyg och eventuellt också till att aktörer lämnar detaljmarknaden för tjänster för stark autentisering. Dessutom kan intresset bland nya leverantörer av identifieringsverktyg för att släppa ut nya identifieringsverktyg på marknaden minska eller så kan man försöka erbjuda identifieringsverktyg med lägre säkerhetsnivå. Sannolikheten för dessa förändringar påverkas av i hur stor utsträckning e-legitimation tas i bruk och i hur stor utsträckning det blir möjligt att använda dem i tjänster för identifieringsförmedling och e-tjänster. Om e-legitimation inte börjar användas i stor utsträckning blir också konsekvenserna för nuvarande och nya aktörer på detaljmarknaden för tjänster för stark autentisering små.

Å andra sidan gör förslaget det möjligt för nuvarande leverantörer av identifieringsverktyg för stark autentisering att nyttja e-legitimation som en del av processen för beviljande av identifieringsverktyg för stark autentisering. Inledande digital identifiering av en person och lagring av denna information är något förmånligare än inledande identifiering med hjälp av ett fysiskt dokument. Särskilt om en kundrådgivare nu ska granska och eventuellt kopiera ett fysiskt dokument samt lagra kopian orsakar användningen av fysiska dokument kostnader som försvinner i och med användningen av e-legitimation. Omfattande användning av e-legitimation som avgiftsfritt verktyg för inledande identifiering kan i någon mån minska kostnaderna för beviljande av identifieringsverktyg för stark autentisering.

E-legitimation kan sannolikt tas i bruk som ett nytt identifieringssätt i e-tjänster med mycket små ändringar, om de nuvarande tjänsterna för digitaliseringsförmedling fungerar som förmedlare. Då får e-legitimationen snabbt tämligen omfattande användningsmöjligheter via förtroendenätets förmedlingstjänster. Ibruktagande av förmedlingstjänsterna förutsätter nya integreringsmetoder eftersom gränssnittsimplementeringarna för e-legitimationen avviker från de nuvarande gränssnittsimplementeringarna i förtroendenätet. Detta kan orsaka smärre kostnader för förmedlingstjänsterna.

Förslagen som gäller e-legitimation och särskilt det bevis för kärnidentitet som Myndigheten för digitalisering och befolkningsdata producerar kan på längre sikt öka affärsmöjligheterna för de nuvarande tjänsterna för identifieringsförmedling. I framtiden kan olika e-identitetsplånböcker och det bevis för kärnidentitet som eventuellt lagras i dem samt övriga bestyrkta personuppgifter skapa ett helt nytt affärsområde, som är betydligt mer omfattande än den nuvarande affärsverksamheten för elektronisk identifiering. Förslaget om e-legitimation kan dock på kort sikt eventuellt minska affärsmöjligheterna för aktörer som tillhandahåller enbart identifieringstjänster.

Förslaget bedöms inte i princip påverka möjligheterna att tillhandahålla elektronisk identifiering, men förslaget kan ha konsekvenser för den allmänna prisnivån på elektronisk identifiering och således på affärsverksamhetens allmänna lönsamhet. För närvarande betalar tjänster för identifieringsförmedling ett så kallat partipris till leverantörer av identifieringsförmedling, som kan vara högst 3 cent per transaktion. E-tjänster betalar ett avtalat pris till tjänster för identifieringsförmedling, vilket kan omfatta ett fast pris och ett transaktionsbaserat pris för identifieringstransaktioner (3 cent ökat med förmedlingstjänstens andel). Dessutom betalar konsumenterna i regel en månadsersättning för rätten att använda identifieringstjänsten. För de flesta konsumenter är identifieringstjänsterna grundläggande banktjänster, och vid sidan av dem får de också tillgång till tjänster för elektronisk identifiering. Mobiloperatörernas mobilcertifikat baserar sig också i regel på månadsfakturering av konsumenten. Det väsentliga är att i fråga om digital identitet är identitetshandlingen en avgiftsbelagd produkt för medborgaren, men att använda den är i princip avgiftsfritt för e-tjänster och andra förlitande parter. Detta förändrar i

någon mån inriktningen av kostnaderna jämfört med den nuvarande modellen. Detta gäller i synnerhet tjänsterna för identifieringsförmedling, för vilka det ska vara avgiftsfritt att nyttja e-legitimation och förmedlingstjänsten ska själv kunna bestämma vilken ersättning som tas ut av e-tjänsten.

Det är svårt att uppskatta e-legitimationens inverkan på lönsamheten för affärsverksamheten för elektronisk identifiering som helhet, särskilt eftersom e-legitimationens användningsgrad bland medborgarna eller de tjänster där e-legitimation kan användas inte är kända. Det faktiska antalet användare kommer att påverkas särskilt av hur lättanvänd den förslagna lösningen är samt möjligheterna att använda den i olika tjänster.

Den digitala identiteten har sannolikt konsekvenser för utvecklingen av identifieringssätten, men trenden påverkas också väsentligt av utvecklingen på EU-nivå. Exempelvis ändringsförslaget som gäller eIDAS-förordningen samt det projekt för utvecklande av en digital plånbok för vissa affärsbanker som är verksamma i EU som inleddes hösten 2021 kommer också att bestämma hur elektronisk identifiering utvecklas i Finland.

I förslagets beredningsfas har man bedömt att för alla nuvarande tjänsteleverantörer kommer det inte att vara särskilt lönsam affärsverksamhet att sälja tjänster för elektronisk identifiering utanför den egna affärsverksamheten. De flesta tillhandahåller sina kunder denna möjlighet, eftersom de vill betjäna sina kunder genom att ge dem möjlighet att använda en bekant metod för elektronisk identifiering i även andra tjänster än de egna banktjänsterna. Förslaget kan ha konsekvenser för olika aktörers vilja att tillhandahålla sina identifieringsverktyg för mera omfattande användning via förtroendenätet för elektronisk identifiering. Detta kan också ha mer omfattande konsekvenser för olika aktörers vilja att investera i utvecklandet av elektroniska identifieringsverktyg och detta kan slutligen leda till en situation där aktörer lämnar förtroendenätet.

För den offentliga sektorns del fungerar förmedlingstjänsten Suomi.fi-identifikation, som underhålls av Myndigheten för digitalisering och befolkningsdata, även i fortsättningen som förmedlingstjänst för elektronisk identifiering. Förslaget har inga konsekvenser för möjligheterna för de nuvarande aktörerna inom elektronisk identifiering att tillhandahålla tjänster också till den offentliga sektorn. När det gäller projektet för digital identitet är målet att hålla den offentliga sektorns kostnader för elektronisk identifiering under kontroll och detta kan ha konsekvenser för den totala summa som den offentliga sektorn i fortsättningen betalar för elektronisk identifiering som den privata sektorn producerar.

De föreslagna bestämmelserna tar inte ställning till den offentliga förvaltningens framtida roll som köpare av elektronisk identifiering. Ett mål för finansministeriets projekt Digital identitet är emellertid att skapa förutsättningar för att hålla kostnadsnivån för den offentliga sektorns elektroniska identifiering under kontroll. Under projektet har man ansett att det även i fortsättningen bör vara möjligt att identifiera sig i den offentliga sektorns e-tjänster med alla identifieringstjänster med vilka det avtalats om saken. Kostnaderna för elektronisk identifiering inom den offentliga sektorn kommer i hög grad att påverkas av i vilken utsträckning e-legitimationen tas i bruk. Om användningen förblir låg kan kostnaderna för den offentliga förvaltningen av användningen av andra identifieringsverktyg öka när volymen av stark autentisering ökar. Om medborgarna tar i bruk e-legitimationen i stor utsträckning kan kostnaderna på motsvarande sätt sjunka. Detta kan ha konsekvenser för affärsverksamheten för elektronisk identifiering via förtroendenätet och dess lönsamhet samt för möjligheterna att tillhandahålla elektronisk identifiering i den privata sektorns tjänster på marknadsvillkor. Detta kan i sin tur påverka möjligheterna för användarna av elektronisk identifiering att använda e-tjänster.

*E-tjänstverktyget för utlänningar* bedöms inte ha några betydande ekonomiska konsekvenser för de nuvarande aktörerna för elektronisk identifiering. E-tjänstverktyget för utlänningar kan användas av utlänningar i första hand i den offentliga sektorns digitala tjänster, men e-tjänstverktyget för utlänningar kan också nyttjas av aktörer inom den privata sektorn på samma sätt som digitala identitetshandlingar. Utlänningars möjligheter att få ett identifieringsverktyg för stark autentisering enligt de nuvarande bestämmelserna har under beredningen av propositionen identifierats som en betydande utmaning när det gäller utlänningars möjligheter att uträtta ärenden hos finska myndigheter. Strävan har varit att beakta detta genom att göra det möjligt att höja säkerhetsnivån hos e-tjänstverktyget genom ett besök ansikte mot ansikte, varvid information om identifieringen ansikte mot ansikte kan inkluderas i datainnehållet i e-tjänstverktyget för utlänningar. Å andra sidan kommer omfattningen av användningen av e-tjänstverktyget för utlänningar också att vara beroende av i hur stor omfattning privata och den offentliga förvaltningens e-tjänster godkänner e-tjänstverktyg som tagits i bruk genom distansregistrering.

*Identifieringsverktyget för fysiska personer* kan i princip ha ekonomiska konsekvenser för affärsverksamheten hos de nuvarande aktörerna för elektronisk identifiering genom att deras intäkter från den offentliga sektorn för identifieringstjänster minskar. Identifieringsverktyget för fysiska personer är en alternativ lösning till den elektroniska identifiering som krävs för användning av den offentliga sektorns digitala tjänster, om en person inte vill eller kan använda digitala identitetshandlingar som finns i en mobil terminal. Identifieringsverktyget för fysiska personer bedöms ändå inte börja användas i någon betydande omfattning, så de ekonomiska konsekvenserna för enskilda ekonomiska aktörer är tämligen små.

#### 4.2.1.3 Konsekvenser för företagen som användare av tjänster

*E-legitimationen* ska kunna användas av e-tjänster antingen via de nuvarande förmedlingstjänsterna för identifiering eller genom att direkt använda gränssnitt som produceras av Myndigheten för digitalisering och befolkningsdata. I förslaget till lag om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata föreslås skyldighet för Myndigheten för digitalisering och befolkningsdata att tillhandahålla ett läsargränssnitt för att den kärnidentitet som ingår i e-legitimationen ska kunna kontrolleras då man uträttar ärenden på plats eller i e-tjänster.

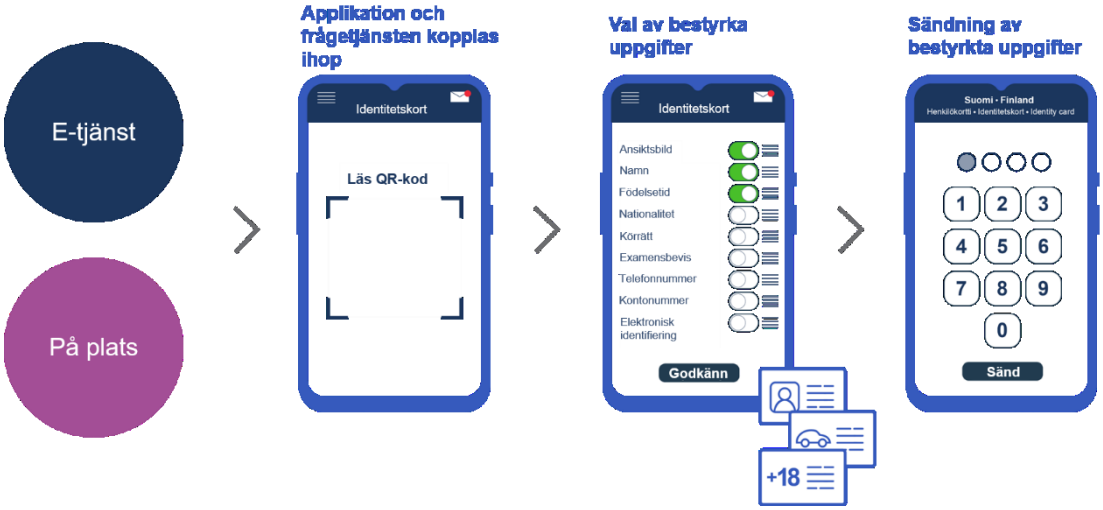
E-legitimationen ska fungera som identifieringsverktyg så att innehavaren av verktyget själv väljer de bestyrkta uppgifter som han eller hon vill visa den förlitande parten. Denna handlingsmodell avviker från den nuvarande handlingsmodellen för förtroendenätet för stark autentisering, där e-tjänsten bestämmer vilka uppgifter den behöver och skaffar dem från identifieringstjänsten som tillhandahåller elektronisk identifiering.

Till den del som e-tjänster vill ta i bruk även de föreslagna e-tjänstlösningarna blir de eventuellt tvungna att företa vissa ändringar i sina egna e-tjänster för att kunna utnyttja den nya handlingsmodellen. På så vis kan förslaget ge upphov till indirekta kostnader. Myndigheten för digitalisering och befolkningsdata beslutar om gränssnittstjänsternas närmare innehåll, så i fortsättningen behöver det bedömas noggrannare hur stor förändring det sist och slutligen är fråga om med avseende på den tekniska implementeringen. För att e-legitimationen och e-tjänstverktyget för utlänningar ska kunna användas direkt i e-tjänster eller vid uträttandet av ärenden på plats förutsätts att e-tjänsterna också genomför integrationer som baserar sig på nya tekniska protokoll. Eftersom dessa protokoll är tämligen nya, är det viktigt att e-tjänsterna tillräckligt noggrant informeras om hur integrationen kan genomföras med hänsyn till informationssäkerhet och dataskydd.

Det är ändå inte obligatoriskt att ta i bruk lösningarna och ur e-tjänsternas synvinkel är kostnaderna således baserat på tjänstens eget val. Dessutom bör man beakta att i princip alla nuvarande tjänster i den privata sektorn som använder stark autentisering använder förtroendenätets nuvarande förmedlingstjänster. Utifrån förslaget är det inte motiverat att anta att företagen kommer att bygga upp egna gränssnittsförbindelser till Myndigheten för digitalisering och befolkningsdatas tjänster i någon stor skala. Istället är det troligt att många företag som också för närvarande använder elektronisk identifiering tillhandahålls e-legitimationen som en ny identifieringstjänst utöver de existerande på ett sätt som inte orsakar dem några förändringar.

Med avseende på de företag som nyttjar tjänsterna kan en konsekvens som är större än de tekniska ändringskostnaderna vara den föreslagna ändring av handlingsmodellen som gäller e-tjänster och uträttande av ärenden på plats när användaren själv väljer vilka bestyrkta personuppgifter han eller hon vill visa e-tjänsten. För användarna är förändringen betydande. Detta kan öka antalet olika kundförfrågningar till exempel i företag som tillhandahåller e-tjänster.

I samband med en kundkontakt begär e-tjänsten styrkta personuppgifter, som den som använder e-legitimation ska visa upp. Användargränssnittet för e-legitimation ska visa användaren för vilken e-tjänst uppgifter håller på att visas och även i övrigt stödja användaren när denne fattar beslut om att visa uppgifter. Användaren ska dessutom frigöra de krypteringsnycklar som används för att skydda dataöverföringen från nyckelförvaringen genom att i den sista fasen ge den verifieringsfaktor (t.ex. PIN-kod) som frigör nycklarna för överföring av de styrkta personuppgifterna. I figuren nedan beskrivs hur det kan gå till när man visar beviset i samband med en kundkontakt:




*Figur 1Uppvisande av bestyrkta uppgifter i samband med en kundkontakt*

När det gäller e-tjänster kan åtgärder också förutsättas för behövliga specifikationer i fall där användaren inte vill förmedla alla sådana uppgifter till e-tjänsten som den begär. Det är möjligt att alla eller en del av de ändringar som eventuellt krävs kan genomföras av de nuvarande tjänsterna för identifieringsförmedling, varvid man inte nödvändigtvis behöver göra några ändringar i e-tjänsterna. Även kostnaderna för handlingsmodellen är valbara, eftersom det inte blir obligatoriskt att tai i bruk e-legitimeringslösningarna.

När man ska bedöma förslagets konsekvenser för användning och nyttjande av elektronisk identifiering är det väsentliga i hur stor omfattning elektroniska tjänster är villiga eller kan nyttja tjänsten för e-legitimation som elektronisk identifieringsmetod samt medborgarnas villighet att använda e-legitimation som verktyg för elektronisk identifiering.

I den marknadsutredning om elektronisk identifiering[1] som Transport- och kommunikationsverket publicerade i mars 2021 konstateras att det står klart att största delen av användarna skulle använda identifieringsverktyget för stark autentisering för identifiering bara leverantörerna av e-tjänster möjliggör det i sina tjänster, och att ur medborgarnas synvinkel finns det en klar efterfrågan på stark autentisering i e-tjänster och de nuvarande användningsmöjligheterna motsvarar inte detta behov (Sähköisen_tunnistamisen_markkinat_-_Sähköinen tunnistaminen turvallisen asioinnin mahdollistajana (traficom.fi), sidan 40). Konsumenterna skulle alltså vilja nyttja identifieringsverktyg för stark autentisering i flera tjänster.

Förslagen kan ha sådana konsekvenser att flera e-tjänster än för närvarande tillhandahåller användarna möjlighet till stark autentisering, särskilt om kostnaderna för stark autentisering sjunker och blir förutsägbara för de organisationer som producerar e-tjänster. Den nuvarande interna debiteringsmodellen för förtroendenätet för stark autentisering baserar sig på bestämmelserna om ett transaktionsspecifikt maximipris, vilka i teorin inte hindrar att det ingås avtal om fasta priser för e-tjänster, men som i praktiken har gjort det sällsynt.

Förslaget kan ha positiva ekonomiska konsekvenser för de aktörer som kan utnyttja möjligheterna med e-legitimering i sin egen affärsverksamhet som alternativ till mera traditionellt uträttande av ärenden på plats och uppvisande av identitetshandlingar. Exempelvis sådana processer för att inleda en kundrelation som för närvarande kräver att kunden är fysiskt närvarande och visar upp ett officiellt identitetskort ska kunna genomföras helt och hållet digitalt. Detta kan möjliggöra nya handlingsmodeller och tillvägagångssätt för att inleda kundrelationer och allmänt tillhandahålla digitala tjänster.

Ibruktagandet av e-legitimation i anslutning till uträttande av ärenden på plats förutsätter sannolikt vissa ändringar i tjänsteleverantörernas rutiner. Enligt förslaget kan e-legitimation då man uträttar ärenden på plats kontrolleras med hjälp av en mobilapplikation som produceras av Myndigheten för digitalisering och befolkningsdata. För att använda mobilapplikationen förutsätts att tjänstemannen på servicestället har tillgång till en mobil enhet. Alternativt förutsätter användningen av kontrollgränssnittet tekniska ändringar i myndighetens tjänstemannasystem för uträttande av ärenden på plats. För att genomföra funktionen för kontroll av e-legitimation vid uträttandet av ärenden på plats förutsätts investeringar av de organisationer som tänker nyttja denna möjlighet, men tills vidare finns det inga uppskattningar av nivån på behövliga investeringar.

Propositionens förslag till bestämmelser innehåller ingen skyldighet att godkänna e-legitimation vid kontroll av identiteten. Enligt förslaget är en e-legitimation en officiell av polisen utfärdad identitetshandling. Om det blir vanligt att använda e-legitimation, kan man emellertid anta att det åtminstone via kundefterfrågan uppstår ett tryck på tjänsteleverantörerna att godkänna e-legitimation som identifieringshandling.

*Förslaget om e-tjänstverktyg för utlänningar* kan ha ekonomiska och verksamhetsmässiga konsekvenser för de aktörer som tillhandahåller tjänster till sådana utlänningar som för närvarande

[1] Sähköisen_tunnistamisen_markkinat_-_Sähköinen tunnistaminen turvallisen asioinnin mahdollistajana (traficom.fi), sidan 40.

inte har någon möjlighet att få elektroniska identifieringsverktyg. E-tjänstverktyget för utlänningar gör det möjligt att tillhandahålla tjänster även till utlänningar, men detta förutsätter sannolikt ändringar i e-tjänsterna och deras bakomliggande system. För aktörerna är det ändamålsenligt att bedöma från fall till fall om ändringarna är lönsamma i förhållande till nyttan av dem.

*Identifieringsverktyget för fysiska personer* ska i enlighet med förslaget inte kunna nyttjas i den privata sektorns e-tjänster, utan det ska fungera som ett verktyg för elektronisk identifiering för de användare som inte har möjlighet att använda e-legitimation som bygger på en mobilapplikation eller andra verktyg för elektronisk identifiering. Sålunda har identifieringsverktyget för fysiska personer inte direkta konsekvenser för den privata sektorns e-tjänster.

#### 4.2.1.4 Konsekvenser för konkurrensen

*Konkurrensrättsliga utgångspunkter*

Tjänster i anslutning till digital identitet har kopplingar till frågor som gäller EU:s bestämmelser om statsstöd (artikel 107 i fördraget om Europeiska unionens funktionssätt) och den nationella lagstiftningen om konkurrensneutralitet (kap. 4 a i konkurrenslagen). Enligt artikel 107.1 i FEUF är stöd som ges av en medlemsstat eller med hjälp av statliga medel, av vilket slag det än är, som snedvrider eller hotar att snedvrida konkurrensen genom att gynna vissa företag eller viss produktion, oförenligt med den inre marknaden i den utsträckning det påverkar handeln mellan medlemsstaterna.

I samband med beredningen av propositionen har dessa frågor bedömts i förhållande till beviset för kärnidentitet, digitala identitetshandlingar, e-tjänstverktyget för utlänningar samt identifieringsverktyget för fysiska personer. Under beredningen har man granskat situationer där ett offentligt samfund tillhandahåller identifieringsverktyg, förmedlingstjänster eller e-tjänster.

Konkurrens- och statsstödsbestämmelserna gäller enheter som bedriver ekonomisk verksamhet, oberoende av juridisk form eller finansieringssätt. Den första frågan som måste bedömas när det gäller tillämpningen av dessa bestämmelser är således om det är fråga om ekonomisk verksamhet. Då kan man granska till exempel om det finns en marknad för tjänsterna eller vill och kan andra aktörer producera tjänster på marknaden. Bestämmelserna om förbjudet statsstöd eller konkurrensneutralitet blir inte tillämpliga när det är fråga om en myndighet som utövar offentlig makt eller agerar i egenskap av myndighet. Om ett offentligt samfund bedriver ekonomisk verksamhet som kan separeras från utövningen av offentlig makt, måste möjligheten till statsstöd bedömas med avseende på denna verksamhet. Om den ekonomiska verksamheten däremot inte kan separeras från utövningen av offentlig makt, hänför sig all verksamhet som samfundet bedriver till utövningen av offentlig makt.

Ur konkurrens- och statsstödsrättslig synvinkel anses en enhet utöva offentlig makt när verksamheten i fråga hör till statens kärnuppgifter eller hänför sig till dem på grund av sin karaktär, sitt syfte eller de tillämpliga reglerna. Allmänt taget är verksamhet som utgör en naturliga del av myndigheternas privilegier och som staten svarar för inte ekonomisk verksamhet, om inte medlemsstaten har beslutat att ta i bruk marknadsmekanismer.

För att klargöra distinktionen mellan ekonomisk och icke-ekonomisk verksamhet har domstolen konsekvent slagit fast att all verksamhet som går ut på att erbjuda varor och tjänster på en marknad utgör ekonomisk verksamhet. Frågan huruvida det finns en marknad för vissa tjänster kan bero på hur dessa tjänster organiseras i den berörda medlemsstaten och kan således variera mellan de olika medlemsstaterna. På grund av politiska val eller den ekonomiska utvecklingen kan

klassificeringen av en viss verksamhet dessutom komma att ändras över tiden. Det som inte är en ekonomisk verksamhet i dag kan bli det i framtiden, och tvärtom.[2]

Om ett offentligt organ bedriver en ekonomisk verksamhet som kan särskiljas från myndighetsutövningen, agerar det organet i egenskap av ett företag med avseende på den verksamheten. Om denna ekonomiska verksamhet däremot inte kan särskiljas från myndighetsutövningen, förblir alla de verksamheter som det offentliga organet utövar knutna till myndighetsutövningen och faller därför utanför begreppet företag.[3]

Förutom lagstiftningen om statligt stöd bör det beaktas att om en medlemsstat har beslutat att ta i bruk marknadsmekanismer och om verksamheten ska anses vara av ekonomisk karaktär ska också 4 a kap. i konkurrenslagen om konkurrensneutralitet tillämpas.

Syftet med konkurrensneutralitetsbestämmelserna i 4 a kap. i konkurrenslagen är att ge den nationella myndigheten befogenheter i ärenden med anknytning till konkurrensneutralitet, som ofta har lett till klagomål till kommissionen, och på så vis skapa förutsättningar för att lösa dylika konkurrensproblem på nationell nivå. Enligt konkurrenslagens 30 b § tillämpas lagens 4 a kap. inte om förfarandet eller verksamhetsstrukturen direkt följer av lagstiftningen eller om tillämpning skulle hindra skötseln av en betydelsefull uppgift som gäller medborgarnas välfärd eller säkerhet eller något annat sådant allmänt intresse. Om tillhandahållandet av digitala identitetshandlingar till någon del anses som ekonomisk verksamhet och annars stå i strid med konkurrensneutralitetsbestämmelserna, ska saken utifrån de föreslagna bestämmelserna bedömas i enlighet med 30 b § i konkurrenslagen som ett förfarande eller en struktur som direkt följer av lagstiftningen. Enligt konkurrensneutralitetsbestämmelserna ska ekonomisk verksamhet på marknaden prissättas marknadsmässigt. Med stöd av konkurrenslagen kan Konkurrens- och konsumentverket också ingripa i till exempel ekonomisk verksamhet som en myndighet bedriver på samma marknad som privat näringsverksamhet eller i ogrundade konkurrensfördelar som myndigheten åtnjuter i denna verksamhet.

*Digitala identitetshandlingar, e-tjänstverktyg för utlänningar, bevis för kärnidentitet samt identifieringsverktyg för fysiska personer*

Som inledande fråga bör behandlas till vilken del tillhandahållandet av e-legitimation, utfärdandet av bevis för kärnidentitet och tillhandahållandet av e-tjänstverktyg för utlänningar och identifieringsverktyg för fysiska personer kan betraktas som utövande av offentlig makt och till vilken del det eventuellt är fråga om ekonomisk verksamhet.

*E-legitimationen* har en fast koppling till pass och identitetskort. Utfärdandet av officiella identitetshandlingar och som grundar sig på en identitet som är registrerad i befolkningsdatasystemet (pass och identitetskort) måste anses utgöra utövning av offentlig mark oberoende av om passet eller identitetskortet är ett fysiskt föremål eller digitalt. När en myndighet kombinerar en fysisk person med dennes kärnidentitet som grundar sig på befolkningsdatasystemet och kopplingen utformas till ett digitalt bevis som kan nyttjas för att bevisa sin identitet då man uträttar ärenden och beviset överlämnas i en applikation så att personen själv kontrollerar den, motsvarar detta med tanke på personens rättsliga situation att ett pass eller ett identitetskort utfärdas. En e-legi-

[2] Kommissionens tillkännagivande om begreppet statligt stöd som avses i artikel 107.1 i fördraget om Europeiska unionens funktionssätt (2016/C 262), punkt 12-13.
[3] Komissionens tillkännagivande 2016/C 262), punkt 18.

timation är enligt den föreslagna regleringen en identitetshandling på samma sätt som identitetskort och pass. Den ska kunna användas och godkännas i syfte att stärka identiteten på samma sätt som identitetskort och pass.

*E-tjänstverktyget för utlänningar* är ett verktyg för att visa uppgifter om identiteten och andra bestyrkta uppgifter i e-tjänster och det tillhandahålls för användning med hjälp av applikationen för digital identitet. E-tjänstverktyget för utlänningar kan således verifieras på samma sätt som digitala identitetshandlingar med hjälp av applikationen för digital identitet och bidrar till att möjliggöra att utlänningar kan uträtta ärenden hos finska myndigheter.

Sambandet mellan e-tjänstverktyget för utlänningar och utövning av offentlig makt är ändå inte likadant som i fråga om e-legitimation, eftersom utfärdande och användning av det inte har någon fast koppling till pass och identitetskort. E-tjänstverktyget för utlänningar är inte heller en med pass eller personkort jämförbar officiell identitetshandling. Det kan ändå anses ha en fast koppling till registrering av befolkningen, som sker i egenskap av myndighet.

Syftet med e-tjänstverktyget är att göra det möjligt att visa personuppgifter som baserar sig på en utländsk identitetshandling i anslutning till e-tjänster, förhindra att parallella identiteter uppkommer i samband med uträttandet av ärenden i e-tjänster och i myndighetsregister, samt att förbättra tillförlitligheten hos de uppgifter som visas. Utfärdande av e-verktyget ska förutsätta att personen registreras i befolkningsdatasystemet så att en utländsk medborgare beviljas personbeteckning i samband med förfarandet. I det finländska samhället kan en dylik individuell identitet beviljas endast genom ett registreringsförfarande som erbjuds av myndigheterna. Att bevilja identiteter som en del av registreringen av befolkningen är en verksamhet som hör till myndigheternas, i detta fall Myndigheten för digitalisering och befolkningsdata, privilegier.

Förutom att det ska vara möjligt att uträtta ärenden hos myndigheterna med e-tjänstverktyget för utlänningar gör lagstiftningen det möjligt att använda verktyget i privata e-tjänster. Ingen annan aktör än en myndighet kan emellertid producera ett e-tjänstverktyg som på ovan beskrivet sätt kan användas för identifiering av en person och som baserar sig på registrering av befolkningen. Till följd av verksamhetens fasta koppling till registrering av befolkningen är det fråga om verksamhet som är en naturlig del av myndigheternas privilegier – i princip inte ekonomisk verksamhet.

*Beviset för kärnidentitet* ska fungera som ett tekniskt tillförlitligt sätt att visa att för den person som innehar beviset finns en i befolkningsdatasystemet registrerad identitet som innehåller kärnidentiteten. Beviset för kärnidentitet ingår i e-legitimationen och e-tjänstverktyget för utlänningar. Eftersom det hör till myndighetens uppgifter att upprätthålla befolkningsdatasystemet och registrera befolkningen, måste utfärdandet av bevis för kärnidentitet betraktas som en oskiljaktig del av myndighetsuppgifterna.

*Identifieringsverket för fysiska personer* handlar om ett fysiskt verktyg som kan användas utan mobil terminal eller chipkort, och vars enda användningsändamål är att göra det möjligt för en person att sköta ärenden på elektronisk väg hos finska myndigheter. När det gäller identifieringsverktyget för fysiska personer kan man bedöma dess inverkan på marknaden för den utrustning som behövs för att tillhandahålla verktyget samt på marknaden för e-tjänster. Myndigheten för digitalisering och befolkningsdata skaffar utrustningen jämte gränssnittslösningar genom sedvanligt offentlig upphandlingsförfarande, dvs. på marknadsvillkor. Identifieringsverktyget för fysiska personer ska inte tillhandahållas via den marknadsmekanism för elektronisk identifiering som anges i autentiseringslagen, och det stannar således utanför marknaden för e-tjänster. Det väsentliga är att användningen av verktyget är begränsad till enbart den offentliga sektorns e-tjänster, beträffande vilka myndigheterna är skyldiga att tillhandahålla sina tjänster

även på elektronisk väg. När det gäller identifieringsverktyget för fysiska personer är det dock möjligt att verksamheten måste bedömas som att den är ekonomisk, så till den delen bedöms konsekvenserna för konkurrensen mer ingående längre fram.

*Bedömning av konsekvenserna för konkurrensen i fråga om e-tjänster, uträttande av ärenden på plats och därtill hörande gränssnitt*

Applikationen för digital identitet kan innehålla antingen en e-legitimation eller ett e-tjänstverktyg för utlänningar. Med applikationen för digital identitet och identifieringsverktyget för fysiska personer kan ärenden uträttas på elektronisk väg. För stark autentisering i e-tjänster har det skapats en konkurrensutsatt marknad i Finland genom autentiseringslagen. Trots marknadens existens går det ändå inte att entydigt och oundvikligen dra slutsatsen att tillhandahållandet av identifieringsverktyg för fysiska personer eller applikationen för digital identitet ska betraktas som ekonomisk verksamhet. Kommissionens beslut SA.25745 gällde Tysklands webbplats för konkursauktioner och där konstaterade kommissionen att myndigheternas verksamhet inte automatiskt ska anses vara av ekonomisk karaktär trots att de går ut på en marknad där privata aktörer redan är verksamma. Enligt kommissionens åsikt avstår myndigheterna inte från att bedriva verksamhet som motsvarar utövning av offentlig makt, trots att privata aktörer har varit snabbare med att tillhandahålla sådana tjänster. Kommissionens andra beslut SA.34646 gällde ett klagomål över en webbtjänst som Nederländerna inrättat och via vilken offentlig upphandling kunde genomföras. I lagen hade myndigheten ålagts en skyldighet som fullgjordes genom den tjänst som myndighetens producerade. Uppfyllandet av en sådan förpliktelse ansågs inte vara av ekonomisk karaktär, utan som utövning av offentlig makt.

Utifrån dessa avgöranden kan man anse att tillhandahållande av identifieringstjänster i den offentliga sektorns e-tjänster kan, trots att det finns motsvarande privat verksamhet på marknaden, stanna utanför begreppet ekonomisk verksamhet. Myndigheterna har i princip i lagen om tillhandahållande av digitala tjänster ålagts skyldighet att producera sina tjänster även elektroniskt och skyldighet att möjliggöra tillträde till e-tjänster för alla kan tolkas ingå i denna helhet. Av en eller annan orsak har inte alla kunder hos den offentliga förvaltningen möjlighet att få identifieringsverktyg producerade på marknadsvillkor, så myndigheterna borde i sista hand med hjälp av identifieringsverktyget för fysiska personer ge alla möjlighet att få ett identifieringsverktyg till myndigheternas e-tjänster.

*Identifieringsverktyget för fysiska personer* har i princip motsvarande egenskaper som de identifieringsverktyg som finns tillgängliga i det nuvarande förtroendenätet, och det har inte samma fasta koppling till utfärdandet av officiella handlingar som styrker identiteten eller myndigheternas uppgifter för att registrera befolkning som digitala identitetshandlingar. Det är således i princip fråga om ekonomisk verksamhet, om verktyget tillhandahålls på marknaden för att används i e-tjänster.

Enligt förslaget ska identifieringsverktyget för fysiska personer dock kunna användas endast i myndigheternas e-tjänster. Det ska inte användas i förtroendenätet eller annars i den privata sektorns e-tjänster, och det konkurrerar således inte direkt med andra identifieringsverktyg som finns på marknaden. Eftersom identifieringsverktyget för fysiska personer är avsett för personer som inte kan använda ett applikationsbaserat identifieringsverktyg är målgruppen mycket begränsad.

För konsumenterna innebär det identifieringsverktyg för fysiska personer som staten tillhandahåller att det utöver de identifieringsverktyg för stark autentisering som finns tillgängliga via

förtroendenätet finns ett nytt fysiskt och tillgängligt identifieringsverktyg som dock kan användas endast för att uträtta ärenden hos myndigheterna. Konsumenterna får sålunda mera att välja mellan, eftersom staten samtidigt fortfarande tillåter att ärenden uträttas med de verktyg för stark autentisering som finns i förtroendenätet. För närvarande är det i första hand bankerna som tillhandahåller sådana alternativa identifieringsverktyg och de kan användas i alla e-tjänster, såväl offentliga som privata. Man kan således anta att i de situationer där konsumenten har möjlighet att använda bankens verktyg i offentliga e-tjänster är efterfrågan på det identifieringsverktyg för fysiska personer som staten tillhandahåller liten. För staten är det emellertid viktigt att säkerställa att personer har möjlighet att uträtta ärenden hos myndigheterna utan att det förutsätts att de ska ha en kundrelation till en bank eller någon annan privat aktör också när de inte vill eller kan använda ett applikationsbaserat identifieringsverktyg. Till denna del är det fråga om att uppfylla likställighetsprincipen. De konsumenter som behöver ett dylikt alternativt identifieringsverktyg för att uträtta ärenden på elektronisk väg hos myndigheterna, erbjuds således ett nytt alternativ. Det kan betraktas som osannolikt att det identifieringsverktyg för fysiska personer som staten producerar skulle ha någon betydande inverkan på den nuvarande verksamheten på förtroendenätsmarknaden.

*Applikationen för digital identitet* gör det möjligt att använda både e-legitimation och e-tjänstverktyg för utlänningar. Med applikationen för digital identitet är det möjligt att uträtta ärenden på elektronisk väg, och i den mån det är fråga om e-legitimationen, som utfärdas som en tilläggstjänst till pass eller identitetskort, ska det också vara möjligt att använda den i anslutning till uträttande av ärenden på plats. Användningen av e-legitimation när ärenden uträttas på plats hos myndigheter förutsätter att mobilapplikationens användargränssnitt möjliggör detta och att identiteten kan säkerställas informationssäkert med hjälp av ett avläsargränssnitt.

Det torde vara möjligt att anse att skapandet av ett sådant digitalt gränssnitt till applikationen för digital identitet som gör det möjligt att verifiera identiteten är en oskiljaktig del av utfärdandet av identitetsbeviset, eftersom identitetsbeviset i praktiken förlorar sin betydelse som det inte kan avläsas eller på något annat sätt verifieras i samband med uträttande av ärenden på plats.

Avläsargränssnittet och produktionen av den kontrollapplikation som innehåller avläsargränssnittet måste bedömas separat från applikationen för digital identitet. De närmare specifikationerna av avläsargränssnittet och kontrollapplikationen fastställs av Myndigheten för digitalisering och befolkningsdata av orsaker som har att göra med kraven på informationssäkerhet. Enligt lagförslaget åläggs Myndigheten för digitalisering och befolkningsdata också att producera en sådan kontrollapplikation med vars hjälp identitetsbeviset kan avläsas. Kontrollapplikationen ska vara fritt tillgänglig för alla som vill ha den utan ersättning.

Även andra än Myndigheten för digitalisering och befolkningsdata ska kunna utveckla sådana kontrollapplikationer som uppfyller de tekniska krav som Myndigheten för digitalisering och befolkningsdata fastställt. Produktionen av kontrollapplikationen kan således eventuellt betraktas som ekonomisk verksamhet. Eftersom kontrollapplikationen ska produceras i form av offentlig upphandling, kan produktionen i vilket fall som helst anses ske på marknadsvillkor.

För närvarande verkar det åtminstone inte på marknaden i Finland finnas lämpliga kontrollapplikationer för digitala identitetskort eller digitala pass. Förslaget bedöms således inte ha några negativa konsekvenser för den existerande marknaden för kontrollapplikationer. Det kan betraktas som möjligt eller rentav sannolikt att det i framtiden kommer ut på marknaden andra kontrollapplikationer än sådana som Myndigheten för digitalisering och befolkningsdata producerar. Å andra sidan bör det konstateras i detta sammanhang att själva kontrollapplikationens kommersiella betydelse sannolikt är liten, och det kan antas att lämpliga kontrollapplikationer snarare uppstår som kringprodukter till andra tjänster.

Lösningen som möjliggör användning av e-legitimation i e-tjänster kan jämföras med lösningen för användning av e-legitimation för att uträtta ärenden på plats. Produktionen av ett gränssnitt för e-tjänster kan på samma sätt som i fråga om gränssnittet för kontroll av identitet då ärende uträttas på plats betraktas som en oskiljaktig del av myndighetens verksamhet och möjligheten att använda e-legitimation.

När en e-legitimation produceras för en person, och de bestyrkta uppgifterna i den kan visas även digitalt i e-tjänster, registrerar myndigheten kärnuppgifterna om personens identitet, verifierar identiteten ansikte mot ansikte och utfärdar ett bevis för kärnidentitet för personen, med vars hjälp denna identitet som kopplats till den fysiska personen kan verifieras. Samtliga dessa är lagstadgade myndighetsuppgifter. På samma sätt som i anslutning till uträttande av ärende på plats är det möjligt att använda en e-legitimation så att det går att verifiera de bestyrkta uppgifter som personen själv visar upp i samband med uträttandet av ärenden endast om identitetshandlingen innehåller ett gränssnitt som behövs för att avläsa den elektroniskt. Att specificera det gränssnitt som behövs kan därför ses som ett naturligt och nödvändigt kontinuum på beviljandet av bevis för kärnidentitet och e-legitimation så att det fortfarande är fråga om utövning av offentlig makt.

Eftersom e-legitimation kan användas i e-tjänster kan de påverka verksamheten på identifieringsmarknaden för e-tjänster. Det är då fråga om indirekta konsekvenser för den marknad som regleras i autentiseringslagen. Om människor börjar använda e-legitimation i stor utsträckning, kan användningen av befintliga elektroniska identifieringsverktyg minska, vilket påverkar affärsverksamheten för leverantörer av förmedlingstjänster och leverantörer av identifieringsverktyg. Verksamheten i fråga om de föreslagna bestämmelser motsvarar dock till denna del bestämmelserna om medborgarcertifikat, som tillhandahålls för elektroniska tjänster via förtroendenätet, och beträffande vilka det har ansetts klart att det handlar om utövning av offentlig makt (RP 36/2009 rd, s.87). Även Statens revisionsverk har i sin rapport om utvecklandet och användningen av identifieringstjänster i den offentliga förvaltningen (161/2008) ansett att Befolkningsregistercentralens medborgarcertifikatverksamhet handlar om myndighetsverksamhet, medan annan utgivning av kvalificerande certifikat eller andra certifikat inte är det. Ovan bedömdes det också i fråga om e-tjänstverktyg för utlänningar att utfärdande av verktyget kan betraktas som sådan verksamhet som hör till myndighetens privilegier. På samma sätt som vid e-legitimation kan möjliggörandet av verktygets användning i e-tjänster betraktas som en oskiljaktig del av myndighetens verksamhet.

På samma sätt som i fråga om medborgarcertifikat görs det genom propositionen möjligt att ta i bruk e-legitimation också i anslutning till privata e-tjänster. Det ska också vara möjligt att ta i bruk e-tjänstverktyget för utlänningar i anslutning till privata e-tjänster. Också i det fallet att möjligheten att använda e-legitimation även i anslutning till privata e-tjänster skulle betraktas som ekonomisk verksamhet, skulle tillhandahållandet av den inte nödvändigtvis vara problematisk med avseende på statsstöds- och konkurrenslagstiftningen. I detta fall bör man lägga märke till att enligt förslaget ska gränssnittet för e-legitimation vara öppet och avgiftsfritt, varvid e-tjänsterna kan kopplas direkt till det eller via gränssnitt som leverantörerna av förmedlingstjänster har byggt upp. När det gäller konsekvenserna för konkurrensen är det sålunda möjligt att förslaget ger upphov till ny affärsverksamhet för leverantörerna av förmedlingstjänster.

Det går inte att till alla delar entydigt jämföra användningen av applikationen för digital identitet med den nuvarande identifieringsmarknaden för e-tjänster, eftersom applikationen för digital identitet i flera avseende avviker från de lösningar som finns på den nuvarande marknaden för identifieringsverktyg. För det första grundar sig applikationen för digital identitet på principen om självägd identitet. Detta betyder i praktiken att de uppgifter som förmedlas från applikat-

ionen i samband med identifieringen inte motsvarar den datahelhet som förmedlas för närvarande med stöd av autentiseringslagens bestämmelser. För det andra är det inte möjligt för leverantören av identifieringsverktyget (dvs. applikationen för digital identitet) att debitera ett pris per identifieringstransaktion, eftersom leverantören av identifieringsverktyget inte får information om när en person använder applikationen för digital identitet för att uträtta ärenden. Informationen förmedlas endast från applikationen till e-tjänsten.

I den mån som användningen av avläsargränssnittet förutsätter investeringar i enheter, såsom smarttelefoner eller separata avläsare av e-legitimation, finns sådana att få på marknaden, och tillhandahållandet av dem regleras inte genom lag. Offentliga e-tjänster skaffar behövlig utrustning på marknaden genom konkurrensutsättning. Likaså finns de teleförbindelser som behövs att få på den fria marknaden. Förslaget har inte heller någon inverkan på möjligheten att tillhandahålla identifieringstjänster utanför den marknad som regleras av autentiseringslagen.

*Sammanfattning av karaktären av tillhandahållandet av tjänster*

På de grunder som beskrivs ovan kan det anses att polisen och Myndigheten för digitalisering och befolkningsdata fungerar i egenskap av myndigheter när de producerar e-legitimation och tjänster som gör det möjligt att använda dem. En e-legitimation omfattas i egenskap av en identitetshandling med fast koppling till identitetskort och pass, av utövningen av offentlig makt, och verksamheten kan således inte betraktas som ekonomisk. Att utfärda handlingar som styrker identiteten och möjliggöra deras användning i samhället är naturligtvis verksamhet som hör till myndigheternas, i detta fall polisens, privilegier.

Myndigheten för digitalisering och befolkningsdatas verksamhet för att producera tjänsterna för digital identitet, som består av informationssystemet för digital identitet, beviset för kärnidentitet, e-tjänstverktyget för utlänningar, tjänsten för hantering av digital identitet, avläsargränssnittet och kontrollapplikationen samt applikationen för digital identitet, kan betraktas som utövning av offentlig makt eller som uppgifter som är en oskiljaktig del av verksamhet som hör till myndighetens privilegier. På motsvarande sätt har tillhandahållandet av Myndigheten för digitalisering och befolkningsdatas tjänst som gäller medborgarcertifikat betraktats som utövning av offentlig makt och medborgarcertifikatet har inte betraktats som ekonomisk verksamhet, utan som utövning av offentlig makt vid tillhandahållandet av identifieringsverktyg (RP 36/2009 rd, s.87 samt GrUU 2/2002). Produktionen av medborgarcertifikat är i lagen om identitetskort bunden till identitetskortet.

4.2.1.5 Konsekvenser för identifieringsmarknadens utveckling

Propositionen har bedömts ha konsekvenser för parterna på den nuvarande identifieringsmarknaden, men i samband med beredningen har det också konstaterats att omvärlden är föremål för mer omfattande förändring och utveckling. Man kan till exempel anta att skillnaden mellan uträttandet av ärenden via e-tjänster och uträttande av ärenden på plats krymper eller försvinner i framtiden. En persons möjlighet att själv bestämma vilka uppgifter han eller hon lämnar om sig själv i kombination med principen om uppgiftsminimering leder dessutom till att den självägda identitetens betydelse ökar. På längre sikt kan man således anta att i stället för en marknad som bygger på den nuvarande autentiseringslagen kommer det eventuellt att utvecklas en ny marknad för identifiering och bestyrkta uppgifter. Förändringens fart och riktning påverkas i hög grad av EU:s eIDAS-ändringsförslag, som skapar en gemensam lagstiftning för plånboksapplikationen för europeisk digital identitet. eIDAS-ändringsförslagets innehåll beskrivs mer ingående i avsnitt 2.6 i propositionen.

Applikationen för digital identitet enligt propositionen utgör inte i sig en digital plånbok. Först efter att eIDAS-ändringsförslaget har godkänts är det möjligt att vidta åtgärder för att genomföra förordningen. Enligt dagens utkast till förordning förefaller medlemsstaterna åläggas skyldighet att producera minst en plånboksapplikation som uppfyller kraven i förordningen. Eftersom det saknas en reglerad marknad kan aktörerna för närvarande fritt utveckla egna plånboksapplikationer och motsvarande lösningar, men det finns ännu inga lagstiftningsmässiga ramar för deras godkännande och tillförlitlighet.

Propositionen innehåller inte något förslag om utfärdande av bevis för kärnidentitet till privata tjänsteleverantörer för att fogas till eventuella privata plånböcker som håller på att utvecklas. Å andra sidan har aktörerna redan nu möjlighet att producera digitala identitetsplånböcker som innehåller en identitet som hanteras av aktören i fråga och som kan stödja sig på uppgifter som Myndigheten för digitalisering och befolkningsdata producerar och som finns registrerade i BDS-informationstjänsterna. För närvarande pågår också utvecklingsarbete i olika branscher i syfte att utveckla identitetsplånbokslösningar. Nya identifieringslösningar utvecklas till exempel inom Finlands autentiseringsandelslag. Enligt propositionen ska det vara möjligt att ta i bruk e-legitimationen och e-tjänstverktyget för utlänningar i privata e-tjänster, om dessa beslutar så, antingen genom direkt koppling till ett gränssnitt som staten tillhandahåller eller genom en lösning som tillhandahålls av en förmedlingstjänst, men verktyget kommer inte att vara en del av autentiseringsmarknaden, liksom inte heller eventuella nya slags verktyg som tas fram av privata aktörer.

Under beredningen av propositionen har man i så stor utsträckning som möjligt, och för att undvika att det uppstår överlappande utvecklingsarbete och extra kostnader, försökt beakta även den utveckling av marknaden som beskrivs ovan och som inbegriper tillhandahållandet av plånboksapplikationer som grundar sig på principen om självägd identitet. Å andra sidan har en utgångspunkt för det nationella utvecklingsarbetet varit att skapa förutsättningar för att tillhandahålla plånboksapplikationer i framtiden så att man efter att eIDAS-ändringsförslaget godkänts i tid hinner fullgöra de skyldigheter som åläggs medlemsstaterna. I princip har strävan varit att statens åtgärder inte ska försvåra privata aktörers självständiga utvecklingsarbete och att inte skapa reglering, tekniska lösningar eller organisatoriska strukturer som kan stå i konflikt med eIDAS-ändringsförslaget. Enligt eIDAS-ändringsförslaget ska såväl offentliga myndigheter som privata aktörer kunna tillhandahålla plånboksapplikationer.

När man bedömer propositionens konsekvenser för marknadsutvecklingen kan det anses som möjligt att marknadsparternas investeringar i den nuvarande identifieringsmarknaden minskar. Detta påverkas dock inte bara av de föreslagna lösningarna utan också av den allmänna utvecklingen av lösningar och marknaden för e-tjänster, till exempel utvecklingen av plånboksapplikationer på EU-nivå. Eftersom staten även i fortsättningen möjliggör e-tjänster med de nuvarande elektroniska identifieringsverktygen kommer en eventuell marknadsövergång att ske mycket behärskat.

Den föreslagna lösningen kan ses som ett steg mot verksamhetsmodeller som bygger på identitetsplånböcker och den bidrar till att de ändringar som eIDAS-ändringsförslaget förutsätter och de skyldigheter som det ålägger kan verkställas i Finland snabbt efter att förordningen godkänts. Detta kan bedömas främja även privata identifieringsverktygstjänster och förmedlingstjänsters rättida tillträde till marknaden, i den mån de kommer att vara beroende av grundläggande lösningar som staten tillhandahåller, såsom bevis för kärnidentitet.

#### 4.2.1.6 Konsekvenser för den inre marknaden

Förslagen har vissa konsekvenser för verksamheten på den inre marknaden. Ur den inre marknadens synvinkel är den nationella digitala identitetslösningen samt e-tjänstverktyget för utlänningar faktorer som syftar till att möjliggöra gränsöverskridande elektronisk identifiering i framtiden. Trots att det i den första fasen är fråga om nationella lösningar, lägger de grunden för framtida lösningar när man förbereder sig för eIDAS-ändringsförslaget och de nya lösningar i anslutning till hantering av identiteten och av bestyrkta uppgifter som utvecklas utifrån det och som är avsedda för gränsöverskridande användning.

Många gällande EU-rättsakter utgår ifrån att e-tjänster borde vara tillgängliga även för andra än finländare, och å andra sidan borde andra medlemsstaters e-tjänster vara tillgängliga för finländska användare. Sådana EU-rättsakter är bland annat förordningen om en gemensam digital ingång ((EU) 2018/1724), direktivet om tjänster på den inre marknaden (2006/123/EG) samt direktivet om användningen av digitala verktyg och förfaranden inom bolagsrätt (2019/1151). De föreslagna lösningarna är en del av den utveckling genom vilken man i Finland eftersträvar sådana fungerande gränsöverskridande lösningar för uträttandet av ärenden som eIDAS-ändringsförslaget förutsätter. Målet är att en eller flera lösningar enligt förslaget ska anmälas enligt förfarandet i eIDAS-förordningen, vilket gör det möjligt för finska medborgare och finska näringsidkare att identifiera sig i myndigheternas tjänster i andra medlemsstater i den mån de är tillgängliga för användare över gränserna. För närvarande har finländare inte tillgång till något identifieringsverktyg som skulle möjliggöra gränsöverskridande elektronisk identifiering.

För att finländare som är bosatta utomlands och utlänningar ska kunna använda e-tjänster, måste det vara möjligt att identifiera dem. En smidig inresefas är väsentlig för att locka internationella experter. Det är dock utmanande att söka arbete eller studieplats från utlandet, eftersom vissa myndighetstjänster förutsätter stark autentisering. Den nationella digitala identitetslösningen samt e-tjänstverktyget för utlänningar kan erbjuda lösningar även på denna utmaning och därmed främja arbetstagarnas rörlighet.

Förslagen kan anses ha konsekvenser som förbättrar medborgarnas och näringsidkarnas fria rörlighet på den inre marknaden, om lösningarna för elektronisk identifiering enligt förslaget möjliggör bättre användning av myndigheternas e-tjänster i hela EU. Detta stödjer också utvecklingen av företagens konkurrenskraft och tillväxtmöjligheter på den inre marknaden, om företagens tillträde till marknaden i andra medlemsländer underlättas. Förbättrade möjligheter till fri rörlighet för medborgare kan ha positiva konsekvenser bland annat för tillgången till kompetens och arbetskraft.

#### 4.2.1.7 Konsekvenser för den offentliga ekonomin

*Allmänt*

Förslaget har konsekvenser för de offentliga finanserna. Kostnaderna för att genomföra de planerade lösningarna uppskattas till sammanlagt cirka 17,5 miljoner euro och de årliga driftskostnaderna till sammanlagt cirka 7 miljoner euro. Avsikten är att en del av de driftskostnader som hänför sig till förslaget ska täckas med kundavgifter i anslutning till verksamheten medan det föreslås att en del av kostnaderna för tjänsterna delvis ska täckas med budgetfinansiering. Förslaget bedöms ha konsekvenser för genomförandemyndigheternas anslagsbehov.

Kostnaderna för att genomföra förslaget täcks av det anslag (28.70.01.) som beviljats finansministeriet i budgeten för 2020.

Driftskostnaderna för beviset för kärnidentitet som hänför sig till lösningarna för digital identitet föreslås täckas helt och hållet med medel ur statsbudgeten. Beviset för kärnidentitet (certifikat) är en nödvändig del av lösningarna för digital identitet, och i framtiden ska det också vara möjligt att nyttja det som grund för en eventuell framtida plånboksapplikation enligt eIDAS-ändringsförslaget. Den EU-lagstiftning som fortfarande är under beredning kommer sannolikt att utgå ifrån att användningen av plånboksapplikationen borde vara avgiftsfri när den som använder plånboksapplikationen är en fysisk person. Myndigheten för digitalisering och befolkningsdatas driftskostnader för beviset för kärnidentitet har uppskattats till 2 miljoner euro per år från och med 2023. De riktas till moment 28.30.03. Omkostnader för Myndigheten för digitalisering och befolkningsdata (reservationsanslag 2 år) inom finansministeriets förvaltningsområde.

Det föreslås att driftskostnaderna för identifieringsverktyget för fysiska personer täcks delvis ur statsbudgeten så att verktyget tillhandahålls som en prestation till sänkt självkostnadsvärde, dvs. kundpriset subventioneras i fråga om de fortlöpande kostnaderna så att kundavgiften för identifieringsverktyget för fysiska personer blir mellan 10 euro och 20 euro. Från och med 2023 orsakar detta kostnader på uppskattningsvis högst 1 miljon euro per år för Myndigheten för digitalisering och befolkningsdata. De riktas till moment 28.30.03. Omkostnader för Myndigheten för digitalisering och befolkningsdata (reservationsanslag 2 år) inom finansministeriets förvaltningsområde.

Förslagets konsekvenser ur genomförandemyndigheternas synvinkel bedöms mer ingående nedan i fråga om respektive aktör. Förslaget bedöms inte ha några direkta konsekvenser för anslagen för de myndigheten som eventuellt har nytta av lösningen, eftersom införandet av den bygger på frivillighet. Dessa övriga myndigheters anslagsbehov bör behandlas separat som en del av planerna för de offentliga finanserna och budgetberedningen. När det gäller e-tjänster ska lösningarna kunna nyttjas via Suomi.fi-identifikation utan separata informationssystemändringar. När lösningen som möjliggör uträttande av ärenden på plats tas i bruk uppkommer kostnader av anskaffningen av de avläsarenheter eller mobila enheter som behövs samt av eventuell integrering av kontrollgränssnittet i kundsystemen. Dessa kostnader som är valbara har uppskattats närmare ur e-tjänsters synvinkel i avsnitt 4.2.1.3.

*Myndigheten för digitalisering och befolkningsdata*

Utvecklingskostnaderna för e-legitimation och de tjänster som hänför sig till dem, för e-tjänstverktyget för utlänningar och för identifieringsverktyget för fysiska personer uppskattas för Myndigheten för digitalisering och befolkningsdatas del till cirka 16 miljoner euro. Utvecklingskostnaderna täcks med det anslag som beviljats finansministeriet i budgetpropositionen för 2020. Under de första åren efter att e-legitimationen tagits i bruk orsakar den fortsatta utvecklingen av lösningen och effektiviserat stöd för ibruktagandet tilläggskostnader på uppskattningsvis 1—2 miljoner euro per år.

Av de årliga driftskostnaderna för digital identitet föreslås att 3—3,5 miljoner euro ska täckas centralt, varav cirka 2 miljoner euro allokeras till att täcka kostnaderna för e-legitimationen och tjänster i anslutning därtill av ett anslag som beviljas under Myndigheten för digitalisering och befolkningsdatas omkostnadsanslagsmoment, och för att täcka kostnaderna för identifieringsverktyget för fysiska personer föreslås ett årligt förslagsanslag på högst en miljon euro. Anslagsbehoven beaktas från och med budgetpropositionen för 2023.

Det föreslås att driftskostnaderna för identifieringsverktyget för fysiska personer delvis ska täckas ur statsbudgeten så att verktyget tillhandahålls som en prestation till sänkt självkostnadspris, dvs. kundpriset subventioneras vad gäller de fortlöpande kostnaderna. Årskostnaderna för

identifieringsverktyget för fysiska personer och tjänster i anslutning därtill beror i någon mån på antalet användare. Kostnaderna för att genomföra tjänsten har uppskattats till cirka 750 000 euro och den fasta kostnaden till cirka 461 000 euro per år. Enligt Myndigheten för digitalisering och befolkningsdatas uppskattning skulle kostnaderna för att producera och tillhandahålla identifieringsverktyget för fysiska personer vara cirka 600 000 euro per år med 30 000 användare. Under beredningen av propositionen har man bedömt att kundavgiften för identifieringsverktyg för fysiska personer borde vara mellan 10 euro och 20 euro, som är ungefär samma nivå som motsvarande verktyg som den privata sektorn tillhandahåller på marknaden. För detta ändamål föreslås att Myndigheten för digitalisering och befolkningsdata beviljas ett årligt förslagsanslag på högst 1 miljon euro, som kan användas för att täcka kostnaderna för tillhandahållande av identifieringsverktyget för fysiska personer.

Årskostnaderna för e-tjänstverktyget för utlänningar och tjänster i anslutning till det har uppskattats till cirka 1,55 miljoner euro, varav det har föreslagits att driftskostnaderna för ibruktagandet och användningen av verktyget, cirka 350 000 euro per år, ska täckas med kundavgifter. Det har uppskattats att cirka 64 000 e-tjänstverktyg för utlänningar kommer att tas i bruk varje år, varvid kundavgiften skulle bli cirka 12–13 euro per verktyg som tas i bruk.

Förslaget kan ha vissa utgiftssänkande effekter på de offentliga finanserna i fråga om de identifieringstransaktioner som köpts av privata aktörer för stark autentisering och som förmedlats via Myndigheten för digitalisering och befolkningsdatas tjänst Suomi.fi-identifikation till den offentliga sektorns organisationers digitala tjänster och för de avgifter som tas ut för dessa transaktioner. Effekten är beroende av i hur stor omfattning e-legitimation eller identifieringsverktyget för fysiska personer används i stället för tjänster från den privata sektorn som identifieringssätt i offentliga tjänster.

E-legitimationen och e-tjänstverktyget för utlänningar samt den europeiska e-identitetsplånbok som eventuellt utvecklas senare bedöms på lång sikt påverka Myndigheten för digitalisering och befolkningsdatas totala inkomster från den privata sektorn för informationstjänster. Konsekvenserna börjar synas uppskattningsvis 2025, när användningen av lösningen antas ha blivit etablerad bland konsumenterna och tjänsteleverantörerna har integrerat funktionen i sina egna system. Tjänsteleverantörerna måste dock upprätthålla parallella BDS-förbindelser för att betjäna de konsumentkunder som inte använder e-identitetsplånbok. Detta ökar kostnaderna för tjänsteleverantörerna. Myndighetens för digitalisering och befolkningsdatas inkomstförluster uppskattas i den första fasen till cirka 50 000 euro per år. Inkomstförlusten kan öka senare när kärnuppgifterna utvidgas så att den under de följande ramperioderna skulle uppgå till 0,5–0,7 miljoner euro.

*Polisen*

Produktionen och ibruktagandet av e-legitimation orsakar fortlöpande kostnader och kostnader av engångsnatur för polisen, vilka täcks delvis med kundavgifter, delvis av det anslag som beviljats finansministeriet och delvis av polisens anslag.

Ur polisens synvinkel förutsätter de föreslagna bestämmelserna inte något separat beslutsfattande eller annat separat förfarande i fråga om utfärdandet av e-legitimation. Det beslut genom vilket pass eller identitetskort utfärdas innehåller också rätt för den sökande att ta i bruk e-legitimationen. Till följd av övergångsbestämmelsen gäller detta också pass och identitetskort som utfärdats före lagens ikraftträdande.

Det svårt att bedöma hur många som kommer att ta kontakt med polisen i anslutning till e-legitimationen, eftersom detta påverkas av både hur många som använder verktyget och hur användbart verktyget är. Antalet tros ändå inte åtminstone under det första året vara sådant att det skulle kräva mera personresurser till polisens rådgivningstjänst. Det är dock skäl att förbereda sig på ett visst behov av tilläggsresurser i framtiden. Antalet kontakter kan dämpas med bra information samt genom att se till att det finns heltäckande information om saken på webben.

Ibruktagandet av det nya identifieringssättet och de nya uppgifterna förutsätter ny utrustning samt utbildning av personalen. De avläsare som ska finnas på tillståndsdiskarna samt det läsprogram som ska installeras i mobila enheter täcks av det anslag som beviljats finansministeriet i budgetpropositionen för 2020. De viktigaste utbildningshelheterna gäller utbildning i användning av den myndighetsportal som ska användas för hantering av e-legitimation och de nya avläsarenheterna. För deras del är det centralt att behövligt utbildningsmaterial och utbildningsmiljöer finns tillgängliga i så god tid som möjligt innan e-legitimationen tas i bruk. Mer omfattande utbildning förutsätts för de arbetstagare inom polisens tillståndsförvaltning som utför nya uppgifter i anslutning till e-legitimationen, dvs. ibruktagande och indragning. Detta berör uppskattningsvis 400 personer.

Det årliga underhållet av e-legitimation ger upphov till kostnader för polisen som i enlighet med avgiftsförordningen täcks med kundavgifterna för pass och identitetskort. Ibruktagandet av e-legitimation förutsätter 24/7-beredskap för underhållets del, för att kunna garantera en säker och pålitlig användning av verktyget. De behövliga personresurserna har uppskattats till två årsverken. Dessutom orsakar beredskapen andra driftskostnader av olika typ. Driftskostnaderna uppskattas till cirka 300 000 euro per år. Den uppskattade kostnaden täcker polisens eget arbete och dessutom kostnaderna för stöd som köps från TUVE Valtori samt kostnader för polisens applikationsleverantör.

När man uppskattar kostnaderna för tilläggsarbetet kan priset på en enskild timme beräknas på följande sätt. Priset på ett årsverke inom resedokumentprocessen är cirka 54 000 euro. Ett kalkylmässigt timpris fås genom att använda relationstalet 1640 timmar, varvid timpriset blir 33 euro. Tilläggsarbetet kommer således utifrån denna uppskattning att uppgå till cirka 1800 timmar, varvid kostnaderna för den ökade arbetsmängden är 59 400 euro. Eftersom beslutsfattandet i anslutning till indragningar inte är verksamhet som finansieras med tillståndsmedel måste denna summa på uppskattningsvis 3300 euro täckas med polisens anslag. I övrigt hänför sig de kostnader som uppkommer till avgiftsbelagda tillstånd och kommer således att överföras till priset på de beviljade tillstånden. Under 2023 kommer det att utfärdas uppskattningsvis 1,1–1,3 miljoner pass och identitetskort, så kostnadseffekten av tilläggsarbetet är cirka 0,04–0,05 euro per utfärdat pass och identitetskort.

*Utrikesförvaltningen*

Ibruktagandet av e-legitimation orsakar utrikesförvaltningen kostnader av engångsnatur för anskaffningen av enheter.

När det gäller anskaffningarna av QR-avläsarenheter har priset för en enskild enhet för utrikesförvaltningens del uppskattats till cirka 300 euro. Enligt utrikesministeriets åsikt borde det finnas åtminstone en QR-kodavläsare vid varje kundserviceställe i Finlands beskickningar och eventuellt borde denna avläsaregenskap också vara nedladdad i de beskickningsanställdas tjänstetelefoner. Dessutom borde en QR-kodavläsare läggas till i de ambulerande bärbara passportföljerna. En preliminär kostnadsuppskattning för anskaffningarna av enheter är cirka 30 000

euro för hundra enheter samt eventuella försändelse- och installationskostnader. De avläsarenheter som kundserviceställena i Finlands beskickningar får samt det avläsarprogram som ska installeras i mobila enheter täcks av det anslag (28.70.01) som beviljats finansministeriet i budgeten för 2020.

För utrikesförvaltningens del består de fasta kostnaderna för e-legitimation av de personalkostnader som orsakas av merarbetet i kundservicen.

E-legitimationen kommer sannolikt att sysselsätta kundservicen i Finlands beskickningar mer än till exempel polisen i Finland därför att inte tillnärmelsevis alla utlänningar har finska bankkoder, mobilcertifikat eller identitetskortets medborgarcertifikat, som gör det möjligt att ta i bruk e-legitimation på elektronisk väg.

Antalet besök vid beskickningarna för att ta i bruk e-legitimation uppskattas till cirka 10 000 under 2023. Besöken kommer att koncentreras särskilt till sådana beskickningar där det finns många utlandsfinländare inom beskickningens verksamhetsområde. I fortsättningen kan antalet besök antas jämnas ut i någon mån, men det är svårt att uppskatta det exakta antalet besök i fortsättningen. Dessutom måste man beakta att antalet kundkontakter kan variera från år till år, och därför är det svårt att i detta skede ge någon genomsnittlig uppskattning av antalet kontakter per år. Man måste också beakta att e-legitimationen är giltiga en viss tid och till exempel om smarttelefonen går sönder eller byts ut måste också e-legitimationen tas i bruk på nytt, vilket förutsätter ett besök i beskickningen, om personen inte har finska bankkoder, mobilcertifikat eller identitetskortets medborgarcertifikat. För att sköta en enskild kundkontakt i beskickningen kan man uppskatta att det krävs cirka 15 minuter, så den årliga arbetsbördan blir 2500 timmar 2023. Kostnadsberäkningen för 2500 arbetstimmar med en genomsnittlig timlön på 84,50 euro är 211250 euro, vilket skulle höja priset för pass och identitetskort som utfärdas av utrikesförvaltningen med 10–20 euro.

Tilläggsutgifterna för den kundservice som hänför sig till ibruktagandet av e-legitimationen hänför sig till utrikesförvaltningens avgiftsbelagda verksamhet och de ska i enlighet med lagen om grunderna för avgifter till staten täckas med avgifter i anslutning till ibruktagandet ave-legitimationen. Bestämmelser om avgifter finns i utrikesministeriets förordning om avgifter för utrikesförvaltningens prestationer (650/2020).

#### 4.2.1.8 Konsekvenser för samhällsekonomin

Propositionen bedöms inte ha några konsekvenser för samhällsekonomin på kort sikt, men på längre sikt kan förslaget ha mindre konsekvenser. Strävan med propositionen är att skapa en grund för en bredare användning av digitala tjänster än nu inom olika samhällssektorer. Genom förslagen om e-legitimation och bevis för kärnidentitet tas de första stegen mot en självägd digital identitet. Den föreslagna handlingsmodellen förändrar den nuvarande verksamhetsidén för marknaden för elektronisk identifiering, men kan samtidigt leda till betydligt större konsekvenser för den digitala tjänsteproduktionen samt för till exempel säkert uträttande av ärenden via olika kanaler.

Ibruktagandet av e-tjänstverktyget för utlänningar kan påverka Finlands attraktionskraft som investeringsobjekt och destinationsland för utländska experter, när det blir lättare för investerare och experter som funderar på att flytta till landet att använda e-tjänster.

### 4.2.2 Konsekvenser för myndigheternas verksamhet

#### 4.2.2.1 Konsekvenser för uppgifter och tillvägagångssätt

Förslagen har konsekvenser för uppgifterna för de myndigheter som för närvarande utfärdar identitetshandlingar. Förslaget om e-legitimation ger polisen samt utrikesförvaltningen nya uppgifter i samband med utfärdandet av e-legitimation.

Förslaget om Myndigheten för digitalisering och befolkningsdatas tjänster i anslutning till digital identitet ökar i någon mån myndighetens uppgifter jämfört med nuläget. Förslagets viktigaste konsekvenser till denna del hänför sig till informationssystemet för digital identitet och administrationen av det samt till produktionen av e-tjänstverktyget för utlänningar. Myndigheten för digitalisering och befolkningsdata ska producera det informationssystem för digital identitet som består av mobilapplikationen och dess bakomliggande system, med vars hjälp bestyrkta uppgifter kan visas i anslutning till e-tjänster och uträttande av ärenden på plats. Myndigheten för digitalisering och befolkningsdata ska också producera, tillhandahålla och administrera bevis för kärnidentitet, samt producera och utfärda e-tjänstverktyg för utlänningar. Till de nya uppgifterna hör också att producera de funktioner som hänför sig till produktionen av lösningarna, såsom en hanteringstjänst, ett avläsargränssnitt samt kontrollapplikationer. Bestämmelser om uppgifterna för Myndigheten för digitalisering och befolkningsdata finns i den nya lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata.

Enligt förslaget ska e-legitimationen vara en officiell av polisen utfärdad identitetshandling. Polisen ska godkänna användningen av e-legitimation också för att hämta ut pass, identitetskort eller andra tillstånd. Polisen har bedömt åtgärderna för att göra det möjligt att utfärda e-legitimationer och använda dem hos polisen samt konsekvenserna av detta. Konsekvenserna hänför sig i första hand till anskaffningen av behövlig utrustning. Till polisstationernas serviceställen för tillståndsförvaltningen bör skaffas avläsarenheter, som kan nyttjas när man bistår vid ibruktagandet av e-legitimation samt för att kontrollera digitala identitetshandlingar som visas upp för att styrka identiteten.

Dessutom har polisen för avsikt att möjliggöra användning i fältverksamheten, så att polisens mobilapparater kan nyttjas för att kontrollera e-legitimation. Möjliggörandet av användning av e-legitimation anses inte ha andra än mindre konsekvenser i form av utbildningsbehov utöver kostnaderna för mobil utrustning.

För utrikesförvaltningens del hänför sig konsekvenserna i första hand till anskaffning av behövlig utrustning, kundservice samt utbildningsbehov hos personalen i Finlands beskickningar. E-legitimationen kommer sannolikt att sysselsätta kundservicen i Finlands beskickningar något mer än till exempel polisen i Finland därför att inte tillnärmelsevis alla utlandsfinländare har finska bankkoder, mobilcertifikat eller identitetskortets medborgarcertifikat, som skulle göra det möjligt att ta i bruk e-legitimation på elektronisk väg. Kontrollen av e-legitimation ska genomföras så att den förkortar den tid som behövs för respektive identifieringstransaktion. Jämfört med traditionella fysiska dokument kan kontrolltransaktionen nästan helt och hållet fokuseras på att säkerställa att personen i fråga är den vars uppgifter förmedlas när den e-legitimationen används. När det gäller traditionella fysiska dokument måste man i en kontrollsituation alltid beakta möjligheten att det uppvisade dokumentet är förfalskat eller att uppgifterna i det är manipulerade på något annat sätt. När det är fråga om en e-legitimation finns det ingen sådan risk, eftersom det inte går att läsa uppgifterna om det inte är fråga om uppgifter som utlämnats i realtid av myndigheterna. När man kontrollerar en e-legitimation i en kontrollapplikation är det också möjligt att få ansiktsbilden betydligt större än i ett fysiskt identifieringsdokument.

Detta påskyndar jämförelsen av ansiktsbilden med den person som identitetshandlingen utvisar och ökar säkerheten vid kundkontakten.

Transport- och kommunikationsverket Traficom fungerar som övervakande myndighet enligt autentiseringslagen och deltar i koordineringen av samarbetet mellan aktörerna i förtroendenätet. Genom regeringens proposition skapas nya uppgifter för förtroendenätet, när leverantörer av tjänster för identifieringsförmedling i fortsättningen kan förmedla även e-legitimation samt e-tjänstverktyg för utlänningar utöver nuvarande identifieringsverktyg. Detta påverkar Traficoms uppgifter.

Enligt förslaget ska Myndigheten för digitalisering och befolkningsdata efter att ha hört Traficom och Polisstyrelsen besluta om de närmare tekniska kraven och informationssäkerhetskraven på informationssystemet för digital identitet. Dessutom begärs utlåtande av Traficom om den bedömning som gjorts av ett bedömningsorgan och som ska göras med två års mellanrum.

Statens center för informations- och kommunikationsteknik Valtori producerar verksamhetsområdesoberoende IKT-tjänster för statsförvaltningen. Det kan ses som Valtoris uppgift att centralt dela den applikation som Myndigheten för digitalisering och befolkningsdata lanserar till de anställdas tjänstetelefoner inom statsförvaltningen.

När man bedömer förändringana i myndigheters verksamhet bör användning av e-legitimation i e-tjänster särskiljas från dess användning för uträttande av ärenden på plats. Ibruktagandet av lösningen förutsätter inga ändringar i myndigheternas e-tjänster, eftersom den ska tillhandahållas så att den kan nyttjas via Suomi.fi-identifikationstjänsten som produceras av Myndigheten för digitalisering och befolkningsdata. Användaren kan dock se förändringarna till exempel i form av begäran att lämna uppgifter som behövs för identifiering till e-tjänsten antingen direkt eller via tjänsten Suomi.fi. Med tanke på användarna borde ändringarna som gäller hur uppgifter efterfrågas genomföras enhetligt.

I anslutning till uträttande av ärenden på plats kan motsvarande förmedlingstjänst inte användas, så ibruktagandet av e-legitimationen förutsätter åtminstone ändringar i myndigheternas rutiner. Enligt förslaget ska e-legitimationen vid uträttande av ärenden på plats kunna kontrolleras med hjälp av en mobilapplikation som producerats av Myndigheten för digitalisering och befolkningsdata. Användning av mobilapplikationen förutsätter att tjänstemannen på servicestället har tillgång till en mobil enhet. Alternativt förutsätter användning av kontrollgränssnittet tekniska ändringar i myndighetens tjänstemannasystem för ärendehantering. Myndigheten för digitalisering och befolkningsdata ska fastställa krav på andra applikationer och lösningar som gör det möjligt att läsa beviset med hjälp av ett gränssnitt.

Myndigheten för digitalisering och befolkningsdata utfärdar e-tjänstverktyg för utlänningar och beviljar identifieringsverktyg för fysiska personer för att styrka identiteten i anslutning till e-tjänster. Avsikten är inte att verktygen ska nyttjas i anslutning tilluträttande av ärenden på plats. Ibruktagandet förutsätter inga ändringar i myndigheternas e-tjänster, eftersom lösningen tillhandahålls via tjänsten Suomi.fi-identifikation, som produceras av Myndigheten för digitalisering och befolkningsdata.

E-tjänstverktyg för utlänningar utfärdas i huvudsak med hjälp av distansregistrering. När utlänningar anländer till Finland kan de emellertid höja tillitsnivån på sitt e-tjänstverktyg genom att identifiera sig ansikte mot ansikte på Myndigheten för digitalisering och befolkningsdatas serviceställen. Detta kan påverka antalet besök på serviceställena, om e-tjänstverktyget för utlänningar tas i omfattande bruk också av personer som uträttar ärenden i Finland. Myndigheten för

digitalisering och befolkningsdata svarar också för åtgärder i anslutning till beviljande av identifieringsverktyg för fysiska personer, vilket kan öka behovet av besök på myndighetens serviceställen.

#### 4.2.2.2 Konsekvenser för organisation och personal

Produktionen av informationssystemet för digital identitet, e-tjänstverktyget för utlänningar samt identifieringsverktyget för fysiska personer har uppskattats föranleda ett tilläggsbehov på 20–25 årsverken vid Myndigheten för digitalisering och befolkningsdata. Olika kundstöduppgifter samt uppgifter i anslutning till utvecklande och underhåll av informationssystemet kräver tjänstearbete. För polisen har tilläggsbehovet för uppgifter i anslutning till underhåll av informationssystemet uppskattats till cirka 2 årsverken.

Distansregistrering av utlänningar och identifiering har beräknats öka behovet av kundrådgivning och kommunikation hos Utbildningsstyrelsen. Tilläggsarbetet i anslutning till rådgivning och kommunikation uppgår i ibruktagandefasen till uppskattningsvis 2 årsverken, i driftsfasen till uppskattningsvis 0,5 årsverken.

För Traficom har förslaget uppskattats orsaka ett tilläggsbehov av 1 årsverke. Tjänstearbete hänför sig inte bara till de lagstadgade uppgifterna enligt förslaget (utlåtande om bedömningskriterierna, utlåtande om auditeringen) utan också till bland annat stöduppgifter i anslutning till beredningen av bedömningskriterierna, information och kontakter till Myndigheten för digitalisering och befolkningsdata och förtroendenätet, utredning av eventuella störningar, om störningarna påverkar förtroendenätet, eventuella uppdateringsbehov i Traficoms föreskrifter, anvisningar och rekommendationer för att säkerställa interoperabilitet samt medborgarinformation om förhållandet mellan de nya verktygen och existerande verktyg för stark autentisering. Dessutom ses Traficom ha åtminstone en biträdande roll när den föreslagna lösningen anmäls som en gränsöverskridande lösning inom EU, samt en biträdande roll vid utarbetandet av Myndigheten för digitalisering och befolkningsdatas föreskrift om avläsarapplikationen.

#### 4.2.2.3 Konsekvenser för myndigheternas informationshantering

Förslaget har konsekvenser för informationshanteringen hos polisen samt Myndigheten för digitalisering och befolkningsdata. I det skede då förslagen bereddes, i februari 2020, framställde Polisstyrelsen samt Myndigheten för digitalisering och befolkningsdata en begäran om utlåtande enligt 9 § i lagen om informationshantering inom den offentliga förvaltningen till finansministeriet. I begäran om utlåtande och i det utlåtande som finansministeriet utarbetade på begäran har man bedömt den planerade förändringens konsekvenser för informationshanteringen. Dessa bedömningar håller i regel fortfarande streck, men när projektet framskridit har det angetts vissa riktlinjer som avviker från de tidigare planerna och som på ett centralt sätt inverkar på informationshanteringen hos polisen samt Myndigheten för digitalisering och befolkningsdata.

Den viktigaste förändringen i förhållande till de konsekvenser av ändringarna som framförts tidigare gäller funktionslogiken för digital identitet. Enligt den ursprungliga planen var det meningen att e-legitimationen skulle fungera så att uppgifterna med användarens bemyndigande alltid skulle utlämnas till den som kontrollerar uppgifterna direkt från det passregister och det identitetskortsregister som Polisstyrelsen för. Det var meningen att den planerade handlingsmodellen skulle ge upphov till en stor mängd logginformation om användningen av verktyget.

Enligt de föreslagna bestämmelserna utlämnas uppgifterna till en applikation som användaren förfogar över. Efter utlämnandet är uppgifterna inte längre myndighetens och de berörs inte av

myndighetens ansvar för informationshanteringen. Uppgifterna utlämnas således inte från myndighetens register direkt till privata aktörer till exempel i en situation där identiteten kontrolleras. I en kontrollsituation ska det i enlighet med förslaget också vara möjligt att försäkra sig om att uppgifterna är aktuella, men det är Myndigheten för digitalisering och befolkningsdata som kontrollerar detta och personuppgifter utlämnas inte direkt från myndigheten till kontrollören.

Med det planerade sättet att genomföra e-legitimation ska uppgifter emellertid fortfarande utlämnas också utanför myndighetssektorn, eftersom uppgifterna i fortsättningen utlämnas till privatpersoner i samband med att de tar i bruk e-legitimationen. Uppgifterna utlämnas alltså till den berörda personen själv så att myndigheten utlämnar verifierade personuppgifter till den enhet som personen innehar. När det gäller e-legitimation är uppgiftskällan polisens passregister eller identitetskortsregister, så att polisen lämnar ut e-legitimationsinnehavarensuppgifter som finns där till Myndigheten för digitalisering och befolkningsdata, som ser till att uppgifterna läggs till i användarens applikation.

Genomförandet av e-legitimation förutsätter för polisens del att ett nytt informationssystem tas i bruk. Det är fråga om en MHEKO-förgrundstjänst som är fast knuten till informationssystemet Identitetskort och pass, dvs. Heko-Passi, och vars uppgift är att förmedla uppgifter i identitetskortsregistret och passregistret till Myndigheten för digitalisering och befolkningsdata. I samband med genomförandet behöver det inte göras några ändringar i polisens elektroniska plattform.

Förslagen medför nya lagstadgade uppgifter för Myndigheten för digitalisering och befolkningsdata samt nya informationssystem och informationsresurser i anslutning till produktionen av dem. Myndigheten för digitalisering och befolkningsdata ska i fortsättningen producera informationssystemet för digital identitet, som gör det möjligt att producera och använda e-legitimationen och e-tjänstverktyget för utlänningar. Myndigheten för digitalisering och befolkningsdata ska dessutom tillhandahålla identifieringsverktyget för fysiska personer. Produktionen av identifieringsverktyget för fysiska personer förutsätter bakomliggande tjänster för hantering av verktyget.

E-legitimationen och e-tjänstverktyget för utlänningar ska enligt förslaget fungera på ett sätt om delvis kan jämföras med de personcertifikat som Myndigheten för digitalisering och befolkningsdata producerar för närvarande, där de personuppgifter som finns i certifikatet överlämnas till personen själv som nyttjar dem. I den föreslagna lösningen är den informationsmängd som behandlas dock avsevärt större och innehåller också information ur polisens register. Dessutom är lösningen annorlunda så till vida att plattformen är en mobilapplikation. Likaså kan den lösning som hänför sig till verifieringen av information jämföras med de certifikattjänster som Myndigheten för digitalisering och befolkningsdata producerar för närvarande.

Funktionsprinciperna enligt förslaget avviker avsevärt från de nuvarande principerna för elektronisk identifiering. För Myndigheten för digitalisering och befolkningsdata i egenskap av den aktör som producerar tjänsterna uppkommer inte motsvarande heltäckande transaktionsinformationsregister över användningen av tjänsten som vad som uppkommer över produktionen av elektroniska identifieringstjänster eller till exempel stödtjänster för e-tjänster. Funktionsprincipen är enligt förslaget densamma som när pass och identitetskort används i anslutning till uträttande av ärenden på plats; användarens ansvar framhävs.

Förslaget innefattar nya register som innehåller personuppgifter för vilka Myndigheten för digitalisering och befolkningsdata är personuppgiftsansvarig, till exempel plattformsregistret

samt registret över e-tjänstverktyg för utlänningar. Myndigheten för digitalisering och befolkningsdata ansvarar i egenskap av personuppgiftsansvarig för att de uppgifter som lagras i registren hanteras korrekt och för att de utlämnas till den berörda personen själv.

Förslaget medför särskilda uppgifter, som förutsätter tillgång till sådan information att tillförlitligheten hos de personer som behandlar denna information måste bedömas. Förslaget medför också särskilda uppgifter som förutsätter tillgång till sådana lokaler att tillförlitligheten hos de personer som arbetar där måste bedömas. Dessa uppgifter är till exempel uppgifter i anslutning till hanteringen av informationssystem samt sådana kundsupportuppgifter som lösningen förutsätter. Förslaget har ändå inte bedömts medföra någon förändring i Myndigheten för digitalisering och befolkningsdatas tillvägagångssätt för att bedöma tillförlitligheten hos de personer som arbetar som tjänstemän eller som experter som värvats i form av köpta tjänster; de nuvarande rutinerna och metoderna har bedömts vara tillräckliga.

Enligt förslaget ska e-legitimationen innehålla en ansiktsbild som lagrats i passregistret eller identitetskortsregistret. Med stöd av 24 § 1 mom. 4 punkten i offentlighetslagen är polisens tolkning att uppgifter i fråga om pass och identitetskort som ska hemlighållas är fingeravtryck, ansiktsbild och passets eller identitetskortets nummer. För att producera lösningen enligt propositionen förutsätts således att sekretessbelagd information, dvs. passets eller identitetskortets bild behandlas. Medan lösningen utvecklas och upprättshållskan sekretessbelagd eller säkerhetsklassificerad information behandlas i anslutning till säkerhetsarrangemangen för informationssystem hos Myndigheten för digitalisering och befolkningsdata eller polisen.

Förslaget innehåller också specialbestämmelser om informationssäkerhet som gäller de centrala kvalitets- och informationssäkerhetskraven på informationssystemet för digital identitet. På informationssystemet samt Myndigheten för digitalisering och befolkningsdatas uppgifter ska lagen om informationshantering inom den offentliga förvaltningen tillämpas, inklusive lagens 4 kap., där det föreskrivs om kraven på basnivå på informationssäkerheten inom den offentliga förvaltningen. Förslaget innehåller särskilda krav, som gäller informationssystemet för digital identitet utöver dessa krav på basnivå och som preciserar kraven på basnivå. Avsikten är inte att bestämmelserna ska avvika från de allmänna bestämmelserna i lagen om informationshantering inom den offentliga förvaltningen.

Enligt förslaget ska det informationssystem för digital identitet som lösningen ger upphov till alltid vara tillgängligt, och det kan således tolkas som en ny kritisk systemhelhet. Informationssystemet för digital identitet nyttjar Polisens Heko-passi-system, och i och med ändringen blir kravet på åtkomst till det också kritiskt. Andra befintliga system som nyttjas (befolkningsdatasystemet, certifikatsystemet) är redan klassificerade som kritiska. Enligt förslaget nyttjas i lösningen inte sekretessbelagd eller säkerhetsklassificerad information i Myndigheten för digitalisering och befolkningsdatas informationsresurser.

Propositionen förorsakar inga ändringar i myndigheternas lokaler och har inga konsekvenser för den fysiska säkerheten i databehandlingsmiljön. Reformen ändrar inte tillträdesrättigheterna eller inloggningssättet till befintliga informationssystem. Tillträdesrättigheterna till nya informationssystem fastställs utifrån behovet med iakttagande av grunderna för minimering av tillträdesrättigheter.

Förslaget föranleder behov av dataloggning i anslutning till tjänsterna för digital identitet samt identifieringsverktyget för fysiska personer. Hos Myndigheten för digitalisering och befolkningsdata samlas heltäckande logginformation i anslutning till tjänsterna för digital identitet till den del som det är fråga om att föra in verifierade personuppgifter i en mobil enhet som personen innehar samt om plattformshantering medan det inte uppkommer någon logginformation om

den egentliga användningen av e-legitimationen eller e-tjänstverktyget för utlänningar. När det gäller identifieringsverktyget för fysiska personer samlas logginformation om såväl hanteringen som användningen av verktyget.

Förslagen orsakar inga ändringar i myndigheternas sätt att omvandla dokument till elektronisk form eller några risker för tillförlitligheten eller integriteten hos dokument som omvandlats till elektronisk form. Förslagen föranleder inget behov av avvikelser i fråga om omvandlingen till elektronisk form och inga ändringar i tillgången till informationsmaterial i maskinläsbar form. Den modell med självägd identitet som beskrivs i förslagen medför ändringar i myndighetens användning av information samt i sätten att förmedla information mellan kunden och den som utnyttjar informationen, och i möjligheterna att uträtta ärenden elektroniskt.

Propositionen orsakar ändringar i myndigheternas rätt att få information. Produktionen av systemet för digital identitet förutsätter i fråga om e-legitimation att Myndigheten för digitalisering och befolkningsdata har rätt att få sådana uppgifter om pass och identitetskort som polisen registrerat, till exempel när en e-legitimation tas i bruk. Detta genomförs med hjälp av tekniska gränssnitt.

Reformen orsakar vissa tekniska ändringar i polisens möjligheter att få information. Polisen måste få tillgång till uppgifter som registrerats i systemet för digital identitet i anslutning till e-legitimation, för att kunna producera registreringsuppgifter i anslutning till dem. Detta genomförs med hjälp av en elektronisk förbindelse.

Registreringen av e-tjänstverktyg för utlänningar och identifieringsverktyg för fysiska personer kan med stöd av lagen om samservice inom den offentliga förvaltningen produceras som samservice tillsammans med andra myndigheter. För att genomföra detta förutsätts att myndigheterna i fråga har möjligheter att få information ur systemet för digital identitet vad gäller e-tjänstverktyget för utlänningar samt ur det system som hänför sig till identifieringsverktyget för fysiska personer. Detta genomförs med hjälp av tekniska gränssnitt. I propositionen bestäms det inte om förvaringstiderna för uppgifter eller handlingar, så Myndigheten för digitalisering och befolkningsdata ska fastställa dem. Som grund kan användas till exempel 24 § i autentiseringslagen. Enligt propositionen grundar sig handlingarnas giltighetstid på giltighetstiden för den identifieringshandling som ligger bakom utfärdandet. Detta har bedömts ha konsekvenser för arkiveringstiderna.

Propositionens e-tjänstverktyg för utlänningar kan användas via Suomi.fi-identifikation. E-tjänstverktyget för utlänningar tillhandahålls med motsvarande gränssnitt som identifieringsverktygen för stark autentisering för närvarande, men gränssnittens datastruktur är annorlunda. Nyttjande av e-tjänstverktyget för utlänningar förutsätter att den ibruktagande organisationen gör ändringar i de tekniska gränssnitten.

När det gäller e-legitimationen och e-tjänstverktyget för utlänningar baserar sig propositionen på att uppgifterna utlämnas till personen själv och därefter kontrolleras av honom eller henne själv. Myndigheten för digitalisering och befolkningsdata deltar inte i de situationer där uppgifterna används och kan inte reda ut ändamålet med uppgifterna. Ändamålet med uppgifter i identifieringsverktyget för fysiska personer enligt propositionen utreds i enlighet med processerna och rutinerna för ibruktagande av Suomi.fi-identifikation.

Lösningen enligt propositionen producerar uppgifter som ska föras in i ett ärenderegister. Enligt propositionen ska Myndigheten för digitalisering och befolkningsdata meddela ett beslut om en sökande inte beviljas e-tjänstverktyg för utlänningar eller identifieringsverktyg för fysiska personer. Likaså ska ett beslut meddelas om Myndigheten för digitalisering och befolkningsdata

återkallar ett verktyg utan innehavarens begäran. Något motsvarande har inte föreslagits i fråga om e-legitimation.

Propositionen orsakar ändringar i ärendehanteringssystemet via ärendenumren samt specifikationen av metadata. Dessutom måste handlingarnas offentlighetsvärde fastställas. I reformen föreslås inga ändringar i de gällande bestämmelserna om offentlighet och sekretess för handlingar. Reformen medför behov av uppdateringar i myndighetens beskrivning av handlingsoffentligheten.

#### 4.2.3 Konsekvenser för miljön

Förslaget kan ha mindre miljökonsekvenser, i första hand genom att de digitala tjänsterna samt antalet terminaler eventuellt ökar. Digitala tjänster kan i princip antas vara något bättre än uträttande av ärenden på plats ur miljösynvinkel, men detta påverkas till exempel av på vilket sätt besöken till servicestället företas. Den ökning av antalet terminaler som beror enbart på förslaget är sannolikt tämligen liten. Det är dock skäl att beakta de miljösynpunkter som hänför sig till tillverkningen av terminaler. Särskilt om en stor grupp medborgare till följd av förslaget för säkerhets skull tar i bruk till exempel identifieringsverktyget för fysiska personer, påverkar detta förslagets konsekvenser för miljön. Förslagets miljökonsekvenser bör dock följas i fortsättningen, för att förståelsen för och mätkompetensen när det gäller miljökonsekvenserna av produktion och användning av digitala tjänster överlag ska utvecklas.

#### 4.2.4 Övriga samhälleliga konsekvenser

##### 4.2.4.1 Konsekvenser för medborgarnas ställning i samhället och för det civila samhällets verksamhet

Strävan med förslagen är att främja lika möjligheter för medborgarna att uträtta ärenden och verka som samhällsmedlemmar i olika kommunikationskanaler och serviceprocesser. Förslagen har konsekvenser för likabehandlingen av medborgare och personer som vistas i Finland. Den förslagna e-legitimationen möjliggör en ny metod och ett nytt sätt för medborgarna att styrka sin identitet med hjälp av en digital tjänst i anslutning till uträttandet av ärenden på plats eller i e-tjänster. Förslaget bedöms främja medborgarnas jämlika ställning i samhället, trots att medborgarnas möjligheter att använda e-legitimation i praktiken kan variera beroende på de krav som hänför sig till användningen av lösningen samt av ekonomiska orsaker eller orsaker som hänför sig till en persons fysiska verksamhetsmöjligheter.

Förslaget som helhet bedöms ha i huvudsak positiva konsekvenser för hushållens ställning när det gäller möjligheterna att använda digitala tjänster. I enlighet med förslaget ska det vara möjligt att få e-legitimation oberoende av kundrelationer, på samma sätt som pass eller identitetskort. Detta ökar medborgarnas lika möjligheter att verka jämbördigt i samhället och ger ytterligare möjligheter att nyttja olika metoder och sätt för digital identifiering och styrkande av identiteten.

Å andra sidan är det inte obligatoriskt för digitala tjänster att godkänna e-legitimation i sina tjänster, så de faktiska konsekvenserna för medborgarna framgår först efter att tjänsten tagits i bruk. I fortsättningen bör möjligheterna att använda digital identitet och övriga därtill hörande omständigheter bedömas regelbundet.

I praktiken kräver den föreslagna e-legitimationen en tillräckligt modern smart enhet som lagringsmedium. Största delen av terminalerna innehåller rikligt med olika hjälptekniker (till exempel ändring av storleken på skärminnehållet, olika kontrastmöjligheter, röststyrning), varför

lagringsmedierna för e-legitimation i huvudsak är tillgängliga. Applikationen för e-legitimation ska uppfylla de tillgänglighetskrav som föreskrivs för mobila applikationer i lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata, så som helhet kommer en stor grupp användare ha möjlighet att använda e-legitimation. Europaparlamentets och rådets direktiv 2019/882 om tillgänglighetskrav för produkter och tjänster kommer att ställa enhetliga tillgänglighetskrav för terminaler som säljs på EU:s inre marknad. De nationella lagförslagen för att genomföra direktivet behandlas som bäst i riksdagen och de förslagna lagarna om tillgänglighet ska enligt förslaget börja tillämpas 2025.

I framtiden är avsikten att i enlighet med eIDAS-förordningen anmäla e-legitimation och identifieringsverktyget för fysiska personer för gränsöverskridande uträttande av ärenden med tillitsnivån väsentlig. Detta förbättrar medborgarnas möjlighet till gränsöverskridande uträttande av ärenden inom EU. Då kan man logga in i digitala tjänster inom den offentliga förvaltningen i andra medlemsstater med e-legitimation och identifieringsverktyget för fysiska personer, om dessa möjliggör identifiering med tillitsnivån väsentlig. Lösningarna möjliggör ännu inte identifiering i e-tjänster som förutsätter tillitsnivån hög.

E-legitimation kan avsevärt underlätta särskilt utlandsfinländares möjligheter att uträtta ärenden i finländska digitala tjänster, särskilt i den offentliga sektorns digitala tjänster, eftersom e-legitimation fås i samband med pass och identitetskort och är sannolikt lättare att tas i bruk och användas för stark autentisering än det nuvarande medborgarcertifikatet på identitetskortet. Å andra sidan är utlandsfinländarnas andel av det totala antalet användare av digitala tjänster relativt liten. För utlandsfinländarnas del har det i olika sammanhang framförts att det är svårt att sköta ärenden i Finland just för att det saknas identifieringsverktyg för stark autentisering. E-legitimation möjliggör ett nytt elektroniskt identifieringssätt åtminstone i den offentliga sektorns digitala tjänster. Om aktörer inom den privata sektorn börjar nyttja e-legitimation, förbättras utlandsfinländares möjligheter att uträtta ärenden i finländska digitala tjänster avsevärt jämfört med nuläget.

E-legitimation kan ha konsekvenser för uträttandet av sådana ärenden på plats, där personen ska styrka sin identitet. E-legitimation kan underlätta till exempel oplanerade bankbesök, om banken godkänner e-legitimation för att styrka identiteten i anslutning till uträttande av ärenden på plats. På längre sikt kan förslaget ha en positiv effekt så att sätten att styrka identiteten i anslutning till uträttandet av ärenden på plats förenhetligas till exempel genom att osäkerheten beträffande när körkort duger som identitetsbevis och när det krävs pass eller identitetskort minskar. Överlag tar e-legitimationen styrkandet av identiteten ett steg i riktning mot hur till exempel olika lösningar för mobil betalning fungerar, där en person inte behöver annat för betalningstransaktionen än en mobil enhet som innehåller en mobil plånbok med de betalkort som finns lagrade i den.

Det föreslagna identifieringsverktyget för fysiska personer är ett alternativt identifieringssätt för de personer som inte kan eller vill använda e-legitimation för att identifiera sig i den offentliga sektorns digitala tjänster. Identifieringsverktyget för fysiska personer kan möjliggöra elektronisk identifiering i den offentliga förvaltningens e-tjänster för personer som inte använder mobila enheter. Det kan hända att identifieringsverktyget för fysiska personer inte kommer att användas mycket i vardagen, men det är betydelsefullt med avseende på likabehandlingen av personer och beredskapen för elektronisk identifiering. Om verktyget på uppskattat sätt används sällan kan det leda till att stödtjänsterna till exempel i form av begäranden om rådgivning eller glömda koder relativt sett ökar.

Propositionen innehåller också förslag om ett e-tjänstverktyg för utlänningar. Förslaget kan avsevärt underlätta utländska personers möjligheter att uträttande ärenden i finländska digitala

tjänster. För närvarande baserar sig uträttandet av ärenden till stor del på antingen myndighetsspecifika lösningar eller, när en utlänning uträttar ärenden för ett företags räkning, på den av Myndigheten för digitalisering och befolkningsdata producerade identifieringstjänsten för utländska medborgare, dvs. identifieringstjänsten Finnish Authenticator.

#### 4.2.4.2 Konsekvenser för barn

Förslaget kan ha små konsekvenser för barn. Förslaget kan förbättra barns möjligheter att uträtta ärenden i vissa digitala tjänster samt också föräldrarnas möjligheter att sköta sina barns ärenden, men konsekvenserna gäller i huvudsak dem som är över 15 år. Vem som helst som har ett finskt pass eller identitetskort kan få e-legitimation. Minderåriga som fyllt 15 ska kunna få e-legitimation också utan föräldrarnas samtycke. De som är under 15 år ska kunna få e-legitimation på samma villkor som pass eller identitetskort, dvs. med vårdnadshavarnas samtycke. Förslaget förändrar inte i praktiken de nuvarande möjligheten för dem som är under 15 år att få verktyg för stark autentisering, men ger ett nytt alternativ vid sidan av det nuvarande medborgarcertifikatet.

För dem som är över 15 år förändras ställningen och de faktiska möjligheterna att uträtta ärenden digitalt något jämfört med nuläget genom förslagen. I dag varierar barns möjligheter och rättigheter att få bankkoder eller mobilcertifikat som fungerar som identifieringsverktyg för stark autentisering enligt beviljare. Vissa aktörer har inga åldersgränser för tillgång till tjänsterna med vårdnadshavarnas samtycke, en del har satt en åldersgräns (t.ex. 12 år) och krav på vårdnadshavarnas samtycke för åtkomst till tjänsterna. I fortsättningen kan den som är över 15 år och som har ett giltigt pass eller identitetskort få en e-legitimation utan vårdnadshavarens samtycke.

Förslagen ger minderåriga som fyllt 15 år något större möjligheter än nu att uträtta ärenden i olika digitala tjänster med hjälp av stark autentisering. För närvarande har barn möjlighet att få olika verktyg för stark autentisering, men åldersgränserna och praxisen för beviljande av dem varierar mellan olika aktörer. Samtidigt bör det dock påpekas att alla digitala tjänster inte nödvändigtvis kan ta emot minderåriga som självständigt uträttar ärenden, om e-tjänstsystemen i princip är uppbyggda endast för myndiga. Detta förutsätter att e-tjänsterna eventuellt har förmåga och behov att identifiera åldern hos de personer som får uträtta ärenden i tjänsten samt att kontrollera åldern som en del av processen.

Minderårigas möjlighet att få e-legitimation och behov av att uträtta ärenden där sådana krävs kan också påverka polisens verksamhet. De föreslagna ändringarna gör det möjligt för minderåriga att självständigt ta i bruk e-legitimation, om de har ett gällande pass eller identitetskort som ger rätt att resa och har fyllt 15 år samt identitetskort som inte ger rätt att rätt att resa och som utfärdats utan vårdnadshavarens samtycke. Eftersom alla som har ett pass eller ett identitetskort som ger rätt att resa oberoende av ålder har rätt att ta i bruk e-legitimation betyder det att sådana minderåriga också har självständig rätt att uträtta ärenden hos polisen för att ta i bruk e-legitimation.

#### 4.2.4.3 Konsekvenser för sysselsättningen och arbetslivet

Förslagen bedöms ha positiva konsekvenser för möjligheterna att använda digitala tjänster med anknytning till sysselsättningen, arbetslivet och arbetsuppgifterna samt för utlänningars sysselsättningsmöjligheter. E-legitimationen gör det möjligt för en person att styrka sin identitet i samband med e-tjänster även i anslutning till arbetsuppgifterna. Detta kan utöka nyttjandet av sådana uppgifter ur myndighetsregistren som styrker identiteten i kontexter där digitala tjänster som riktar sig till företag används.

E-tjänstverktyget för utlänningar kan underlätta utlänningars sysselsättning genom att de får rättvisare möjligheter att sköta uppgifter i anslutning till arbetet också i e-tjänster. E-tjänstverktyget för utlänningar har centrala kopplingar till de lagstiftningsändringar som gäller en reform av personbeteckningen och vilkas syfte är att tillsammans med förslaget om digital identitet ge utlänningar smidigare möjligheter att registrera sin identitet även i det finländska befolkningsdatasystemet och lättare än nu få finsk personbeteckning. E-tjänstverktyget för utlänningar och finsk personbeteckning möjliggör tillsammans personers uträttande av ärenden digitalt samt tillgång till tjänster. I dag förutsätts och nyttjas personbeteckningen i stor utsträckning inom såväl den offentliga som den privata sektorn för att genomföra olika serviceprocesser.

#### 4.2.4.4 Konsekvenser för brottsbekämpningen och säkerheten

Förslaget om e-legitimation kan ha konsekvenser för den allmänna säkerheten hos och förtroendet för den digitala tjänsteverksamheten. Förslaget kan öka till exempel förtroendet för handeln mellan konsumenter och minska bedrägerierna på olika digitala plattformar, om användningen av e-legitimation och stark autentisering utvidgas till handelsplatser mellan konsumenter. E-legitimationen kan eventuellt också öka kontrollen av identiteten vid handel ansikte mot ansikte mellan konsumenter och detta kan bidra till att minska bedrägerierna i sådana affärssituationer.

När det gäller e-tjänstverktyget för utlänningar har säkerhetsaspekterna och riskerna med det beaktats med avseende på ökad brottslighet. Tillsammans med de lagstiftningsändringar som gäller en reform av personbeteckningen innebär de ändringar som nu föreslås grundläggande förändringar i skapandet av registeridentiteter. I samband med beredningen har särskild uppmärksamhet fästs vid säkerheten när ärenden uträttas på distans med e-tjänstverktyget för utlänningar och vid att man i samhället är tillräckligt medveten om den osäkerhet beträffande identitetsuppgifternas tillförlitlighet som hänför sig till förfarandet för distansregistrering. Strävan med dessa åtgärder är att förhindra ökad bedrägeribrottslighet och därmed ökad arbetsbörda för polisen. Särskild uppmärksamhet har fästs vid distansregistreringens säkerhet med avseende på säkerheten hos den ansiktsidentifiering som lösningen utnyttjar för att det ska kunna säkerställas att ansiktsidentifieringen inte missbrukas.

Enligt förslaget ska polisen och Myndigheten för digitalisering och befolkningsdata ha skyldighet att reagera på missbruk av e-legitimationen och e-tjänstverktyget för utlänningar så att användningen av verktyget förhindras till exempel i händelse av identitetsstöld. På motsvarande sätt bör man reagera på situationer där en e-tjänst till exempel samlar in personuppgifter på felaktiga grunder. Fullgörandet av dessa skyldigheter kan påverka polisens och Myndigheten för digitalisering och befolkningsdatas arbetsbörda. Vid sidan av att reagera på missbruk har man under beredningen ansett det viktigt att kunna upptäcka missbruk till exempel i situationer där någon försöker missbruka e-tjänstverktyget för utlänningar genom att registrera ett stort antal digitala identiteter för utlänningar i skadligt syfte. För att förutse missbruk har det konstaterats vara viktigt att polisen och Myndigheten för digitalisering och befolkningsdata upprätthåller en aktuell hotbild och säkerställer att tillräckliga informationssäkerhetskontroller används för att kunna reagera på dessa hot.

Direkt nyttjande av gränsytorna för e-legitimation och e-tjänstverktyg för utlänningar förutsätter inte registrering av e-tjänster, så det är möjligt för brottslingar att försöka skapa e-tjänster som försöker samla in personuppgifter utan grund till exempel genom nätfiske. Avsikten är att begränsa verksamhetsmöjligheterna för e-tjänster som verkar på felaktiga grunder till exempel genom att säkerställa identifiering i e-tjänsterna, informera slutanvändarna tydligt om visandet av uppgifterna och handleda slutanvändarna i säker användning av tjänsterna. Dessutom har

man beaktat situationer där slutanvändarna avsiktligt lämnar ut sin e-legitimation eller e-tjänstverktyg för utlänningar för brottslig användning till exempel för ekonomisk vinning. För dessa situationer kommer e-tjänsterna också ha möjlighet att anmäla missbruk till polisen och Myndigheten för digitalisering och befolkningsdata.

4.2.4.5 Konsekvenser för informationssamhället

*Behandling av personuppgifter och dataskydd*

Inom ramen för lösningen och med dess hjälp behandlas i stor omfattning uppgifter som gäller både finska medborgare och utlänningar som använder finska e-tjänstverktyg. Vid genomförandet utnyttjas befintliga register och skapas också nya register (t.ex. plattformsregistret och transaktionsinformationsregistret). De frågor som gäller personuppgiftsansvariga och grunderna för behandlingen av uppgifter beskrivs mer ingående i specialmotiveringen.

De föreslagna funktionsprinciperna för förvaring och förmedling av personuppgifter i e-legitimationen och e-tjänstverktyget för utlänningar skiljer sig från principerna för hur de nuvarande identifieringsverktygen för stark autentisering fungerar. E-legitimationen och e-tjänstverktyget för utlänningar innehåller bestyrkta personuppgifter, beträffande vilka individen beslutar hur de används. Individen har alltså möjlighet att bestämma vilka personuppgifter som visas tjänsteleverantören. Enligt förslaget är också principen för förmedling av uppgifter ny; det är möjligt att nyttja e-legitimationen och e-tjänstverktyget för utlänningar direkt i e-tjänsten utan att det finns någon identifierings- eller förmedlingstjänst som mellanhand. Till denna del blir den faktiska inverkan sannolikt liten i den inledande fasen, eftersom man kan anta att lösningen i den inledande fasen i första hand nyttjas med hjälp av tjänster för identifieringsförmedling, Suomi.fi-identifikation och andra motsvarande.

Omfattande behandling av personuppgifter i kombination med användningen av nya tekniska lösningar innebär sannolikt en sådan hög risk för personuppgifter som avses i dataskyddsförordningen. Till följd av detta behövs sådan konsekvensbedömning avseende dataskydd som avses i artikel 35 i dataskyddsförordningen i den fasen då de tekniska lösningarna och användningsmodellerna för lösningen preciseras. Också när det gäller befintliga register kommer man att ta i bruk nya användningssätt, vilket förutsätter att konsekvensbedömningen avseende dataskydd uppdateras.

När personer upphör att använda e-legitimation, e-tjänstverktyg för utlänningar eller identifieringsverktyg för fysiska personer finns det en risk för att känsliga uppgifter, såsom kryptografiskt material, blir kvar i dessa personers terminaler, så strävan är att säkerställa tillräckliga mekanismer för säker utplåning av dessa uppgifter.

Med tanke på principen om självägd identitet strävar man efter att säkerställa att den som utfärdar e-legitimation eller e-tjänstverktyg för utlänningar inte kan följa med hur verktygen används för att styrka identiteten i anslutning till e-tjänster eller uträttandet av ärenden på plats. I samband med detta är det centralt att säkerställa att exempelvis användningen av spärrlistor eller insamlingen av logginformation inte medför en möjlighet att följa med användningen av verktygen i elektroniska tjänster . Detta krav måste dock bedömas i förhållande till de behov som följer av iakttagna missbruk.

Till användningen av e-legitimation och e-tjänstverktyg för utlänningar hänför sig användningen av ett plattformsregister som upprättas för dessa. I plattformsregistret insamlas inform-

ation om den mobila terminal där verktyget i fråga har tagits i bruk. När det gäller plattformsregistret säkerställs att i det insamlas endast sådana uppgifter som behövs för att verktygen ska kunna användas tryggt och att uppgifterna i plattformsregistret inte utan grund sammanställs med uppgifter i andra register.

Med tanke på felfria uppgifter och rättelse av uppgifter beskrivs i propositionen de sätt på vilka verifierade personuppgifter i e-legitimation och e-tjänstverktyg för utlänningar kan uppdateras ur de register som ligger till grund för dem. Verifierade personuppgifter i personernas mobila terminaler är kortlivade jämfört med det långvariga beviset för kärnidentitet. Enligt planerna ska uppdateringen ske på användarens uttryckliga begäran, så att lösningen fortfarande främjar principen om självägd identitet. Användningen av e-legitimation ska dock i praktiken förutsätta att uppgifterna uppdateras med jämna mellanrum, så att det kan säkerställas att uppgifterna i verktyget är uppdaterade. E-tjänsterna får också information om tidpunkten då de verifierade personuppgifterna uppdaterats, varvid e-tjänsterna kan själva utifrån en riskbedömning avgöra om de litar på de bestyrkta uppgifterna eller förutsätter att uppgifterna fräschas upp innan de godkänns.

Med tanke på internationella uppgiftsöverföringar är strävan när lösningen genomförs att personuppgifter inte överförs utanför EU/EES-området. Detta säkerställs framför allt med avseende på tredje parters applikationskomponenter.

Ur slutanvändarens synvinkel är det centralt att efter att verktyget utfärdats finns det ingen central aktör i lösningen som bestämmer hur verktyget används, utan användaren beslutar själv om han eller hon vill visa upp sina personuppgifter för en viss förlitande part. När det gäller lösningen har strävan varit att stödja slutanvändaren i detta beslutsfattande, så att han eller hon kan försäkra sig om att den förlitande parten säkert är den som parten påstår sig vara. Ur den förlitande partens synvinkel är strävan också att försäkra sig om att personuppgifterna visas i ett tillförlitligt verktyg och att personen faktiskt har kontroll över de uppvisade personuppgifterna, att det har utfärdats av en pålitlig aktör, och att uppgifterna är aktuella och inte har återkallats. I kommunikationen som gäller digital identitet ligger fokus på att beskriva ansvaren tydligt och dessutom stöds slutanvändarna vid en informationssäker användning av verktyget som beaktar dataskyddet. Kommunikationen stöds eventuellt också genom utbildning och handledning för dem som nyttjar digital identitet.

Förlitande parter kan om de vill nyttja e-legitimation och e-tjänstverktyg för utlänningar i anslutning till sina e-tjänster eller för att möjliggöra uträttande av ärenden på plats göra det direkt, dvs. utan att vara beroende av en central aktör. Detta betyder att kontrollfunktionerna, som hjälper slutanvändaren att fatta ett informerat beslut om delning av uppgifter, inkluderas i själva e-legitimationen och e-tjänstverktyget för utlänningar. Av förlitande parter förutsätts dessutom olika åtgärder eller funktioner: 1) möjlighet att identifiera den förlitande parten så att slutanvändaren kan försäkra sig om till vem han eller hon delar sina uppgifter, 2) en heltäckande beskrivning av dataskyddsrutiner, 3) insamling av endast sådana verifierade uppgifter som behövs i det aktuella fallet, och 4) granskning av spärrlistor och utförande av integritetskontroller. Såväl av tjänster för digital identitet som av e-tjänster förutsätts att dataskydd av standardvärde beaktas och detta kan förutsätta utbildning och handledning även för e-tjänster så att de kan iaktta ändamålsbundenhet enligt dataskydd av standardvärde när de samlar in personuppgifter och nyttjar tjänsterna för digital identitet. Vid sidan av dataskydd av standardvärde förutsätts att tjänster för digital identitet beaktar etiska synpunkter.

En väsentlig del av dataskydd av standardvärde och behandling av personuppgifter enligt den allmänna dataskyddsförordningen är att iaktta principen om uppgiftsminimering. För att iaktta denna princip bättre möjliggör e-legitimationen och e-tjänstverktyget för utlänningar så kallat

selektivt visande där en person själv kan bestämma vilka uppgifter han eller hon delar med e-tjänsten. Det måste också vara möjligt att faktiskt välja, så att e-tjänsterna anger att endast sådana uppgifter är obligatoriska som de faktiskt behöver för att garantera sin verksamhet.

*Informationssäkerhet*

Beroendet av centrala komponenter (t.ex. centraliserade identifieringstjänster) för att visa verifierade personuppgifter minskar vid användning av e-legitimation och e-tjänstverktyg för utlänningar, eftersom personen själv förfogar över användningen av uppgifterna. När verktyget tas i bruk förutsätts hög användbarhet och att de överenskomna servicenivåerna iakttas, så med tanke på servicehelheten säkerställs tillräckliga metoder för kontinuitetshantering, förmåga till återhämtning efter störningar, och metoder för att informera slutanvändare och förlitande parter om tjänstens användbarhet. Det är också väsentligt att säkerställa att de bakomliggande tjänsterna har möjlighet att reglera sin kapacitet dynamiskt, så att man kan svara på förändringar i behovet att använda tjänsterna. Det nationella genomförandet av elektronisk identifiering stödjer sig för närvarande i huvudsak på de metoder för stark autentisering som tillhandahålls av banker och teleoperatörer och om användningen av en enskild identifieringsmetod förhindras hindrar det sålunda inte nationellt allt nyttjande av stark autentisering. När det gäller e-legitimation säkerställs tillräcklig resiliens i krissituationer, så om användningen av e-legitimation förhindras kan tillgången till stark autentisering säkerställas. Detta innebär att e-legitimation inte får bli det enda sättet för stark autentisering i e-tjänster. Med avseende på kontinuitetshanteringen förbereder man sig också på internationella krissituationer, till exempel där tillträdet till tjänster som är viktiga för distributionen av e-legitimation (t.ex. appbutiker) förhindras eller försämras.

Enligt planerna ska lämpliga delar av den helhet som e-legitimationen, e-tjänstverktyget för utlänningar och identifieringsverktyget för fysiska personer bildar skaffas från tredje parter. För leverantörerna av dessa delkomponenter säkerställs att samma mekanismer för behandling av informationssäkerhetsavvikelser iakttas i fråga om karakteristika som skaffats via underleverantörskedjor som i fråga om komponenter som tjänsten själv producerat. Motsvarande gäller också för sådan karakteristika för öppen källkod som nyttjas när tjänsterna genomförs. Det måste säkerställas att uppgifterna inte överförs från mobila enheter eller förlitande parter till externa aktörer via till exempel analys- eller felutredningslösningar. Strävan är att hantera dessa risker genom att upprätta skriftliga avtal med aktörer i underleverantörskedjan om deras skyldigheter och försöka säkerställa att dessa skyldigheter fullgörs.

I och med att man genomför principen om självägd identitet kommer de protokoll och standarder som ingår i integrationslösningarna att vara nya jämfört med de standarder och protokoll som används vid genomförandet av många andra identifierings- och tillitstjänster. I detta sammanhang säkerställs att det i specifikationen av standarderna och protokollen har säkerställts på tillräcklig nivå att det finns tillräckliga informationssäkerhetskontroller som garanterar integritet och tillförlitlighet och att kontroller som eventuellt saknas kompenseras med nationella specifikationer.

När det gäller digital identitet har man i propositionen beaktat riskorientering samt de viktigaste hoten som hänför sig till användningen av tjänsterna och lösningarna ur såväl informationssäkerhetens som dataskyddets synvinkel. Dessutom förpliktar lagstiftningen tjänsteproducenterna att upprätthålla aktuell risk- och hotinformation så att de roller och ansvar som hänför sig till underhållet av dessa uppgifter och behövliga åtgärder är specificerade. Av informationssäkerhetskontrollerna av digital identitet förväntas också flexibilitet så att det kan säkerställas att de är effektiva mot nya informationssäkerhetshot och en föränderlig hotmiljö. När det gäller mobila enheter borde informationssäkerhetskontrollerna också beakta enheternas livscykel, så att

nya informationssäkerhetskontroller kan tas i bruk i den takt som enhetstillverkarna gör dem tillgängliga.

Av de aktörer som producerar lösningarna förutsätts ett formbundet förfarande för hantering av förändringar Ur förändringshanteringens synvinkel är det centralt att identifiera situationer där man är tvungen att göra förändringar som bryter interoperabiliteten bakåt ur slutanvändarnas och de förlitande parternas synvinkel, för att kunna minimera konsekvenserna för användningen av tjänsterna. Ur förändringshanteringens synvinkel är det också centralt att definiera de situationer där användningen av verktygen bör förhindras innan användaren installerar en uppdaterad applikationsversion eller situationer där omfattningen av förändringarna förutsätter sådan ny granskning av överensstämmelsen med kraven som utförs av ett bedömningsorgan.

Den föreslagna lagstiftningshelheten anger klara riktlinjer för kraven på hantering av störningar och informationen om störningar. För slutanvändaren är det väsentligt att få synlighet för hur han eller hon har använt sin e-legitimation och sitt e-tjänstverktyg för utlänningar, samt möjlighet att lagra väsentlig logginformation som hänför sig till användningen på en säker plats. Det är också väsentligt att fastställa gränser för i hur många enheter en e-legitimation eller ett e-tjänstverktyg för utlänningar kan tas i bruk. I samtliga situationer bör slutanvändaren kunna överblicka i vilka enheter e-legitimationen eller e-tjänstverktyget för utlänningar används. Den föreslagna lagstiftningen gör det möjligt att dra in en e-legitimation eller ett e-tjänstverktyg för utlänningar i samband med missbruk, till exempel om ett verktyg obehörigt innehas av en annan person. I lagstiftningen är det också möjligt att förhindra att en e-tjänst som beter sig felaktigt får möjlighet att utnyttja e-legitimation och e-tjänstverktyg för utlänningar, till exempel om e-tjänsten sysslar med nätfiske.

Lagstiftningen förutsätter att när en tjänst tillhandahålls ska det finnas förmåga att upptäcka eventuella missbruk, men detta måste sättas i proportion till att personen själv förfogar över uppgifterna (självägd identitet) samt skyddet för privatlivet. I nödsituationer tillhandahålls en möjlighet att förhindra åtkomst till uppgifterna, så att antingen användaren själv eller tjänsteleverantören kan förhindra åtkomst. Dessa situationer måste vara tydligt beskrivna och dessutom måste slutanvändarna och de förlitande parterna kunna informeras klart om hur de ska agera i samband med eventuellt missbruk.

När det gäller e-legitimation och e-tjänstverktyget för utlänningar utlämnas personuppgifter till användarens förfogande, till hans eller hennes personliga mobila terminal. Leverantörerna av operativsystem för mobila terminaler tillhandhåller i sina senaste versioner förmåga att utnyttja enheternas säkerhetselement, varvid man kan säkerställa att uppgifterna separeras på logisk nivå i den mobila terminalen med hjälp av kryptografiska metoder. Å andra sidan är det väsentligt att säkerställa att terminalen i fråga erbjuder tillräckliga skyddsmekanismer för informationens tillförlitlighet och integritet. Detta kan inverka på i vilka enheter e-legitimation eller e-tjänstverktyg för utlänningar kan användas och i vissa situationer kan användningen förhindras, om användaren till exempel inte kan uppdatera sin mobila terminals operativsystemversion till den nivå som krävs.

När det gäller personliga mobila terminaler har centraliserade tjänsteproducenter mindre möjligheter att kontrollera till exempel om enheten innehåller eventuella skadeprogram. Även i dessa situationer bör man försäkra sig om att skadeprogram inte kan äventyra tillförlitligheten och integriteten hos de personuppgifter som finns lagrade i den mobila terminalen. Detta förutsätter att känsliga uppgifter separeras från andra applikationer på logisk nivå med hjälp av kryptografiska metoder.

Eftersom användarna kan visa sina personuppgifter direkt för förlitande parter, överförs ansvaret för informationssäkerheten till den förlitande parten. Med tanke på integrationernas säkerhet är det då centralt att säkerställa att de förlitande parterna utför tillräckliga kontroller av integritet och spärrlistor. I anslutning till uträttande av ärenden på plats kommer man att nyttja dataöverföring via gränssnitt för kontaktlös läsning. I anslutning till såväl uträttande av ärenden på plats som i e-tjänster är det väsentligt att använda krypterad dataöverföring även på meddelandenivå.

Slutanvändaren måste också kunna upphöra att använda en e-legitimation, ett e-tjänstverktyg för utlänningar eller ett identifieringsverktyg för fysiska personer. När användaren upphör att använda dessa verktyg i en viss enhet så bör man kunna försäkra sig om att det inte längre är möjligt att använda det verktyg som tagits i bruk i enheten i fråga och att uppgifterna utplånas på ett säkert sätt. Det ska göras möjligt att radera uppgifter även genom användarens egna åtgärder på distans, om användaren till exempel förlorar kontrollen över sin mobila terminal.

När det gäller hanteringen av krypteringsnycklar måste man vid skapandet av krypteringsnyckelmaterial som kopplas till beviset för kärnidentitet försäkra sig om att de mekanismer som används för att skapa nycklar är säkra. Dessutom måste man försäkra sig om att nyckelmaterialet är självägt, dvs. att bara den aktuella personen kan förfoga över det och att det inte i någon situation röjs för till exempel tjänstens bakomliggande system. Genom informationssäkerhetskraven blir användning av säkra krypteringsalgoritmer obligatorisk.

För att säkerställa informationssäkerhet är ett centralt delområde den bedömning av överensstämmelse med kraven som ett bedömningsorgan utför med jämna mellanrum. Lagstiftningen ger riktlinjer för de kriterier som ska användas och mot vilka överensstämmelsen med kraven bedöms. När det gäller valet av kriterier är Myndigheten för digitalisering och befolkningsdata skyldig att höra Traficom och Polisstyrelsen. Valet av kriterier bör uppmärksammas så att de täcker den övergripande säkerheten i anslutning till såväl e-tjänster som uträttande av ärenden på plats. Dessutom bör kriterierna på ett övergripande sätt beakta att ledningsmodellen för informationssäkra tjänster för digital identitet överensstämmer med kraven.

Av e-tjänster förutsätts inte separat registrering när de nyttjar e-legitimation och e-tjänstverktyg för utlänningar. För att slutanvändarna ska kunna försäkra sig om att e-tjänster är vad de påstår sig vara bör Myndigheten för digitalisering och befolkningsdata ställa krav på de certifikat som används vid identifieringen i e-tjänster. Uppmärksamhet bör fästas på valet av utfärdare av godkända certifikat så att det går att verifiera att e-tjänsten har koppling till en juridisk person i bakgrunden. I de situationer där det upptäcks att e-tjänster till exempel samlar in personuppgifter på felaktiga grunder (t.ex. med hjälp av nätfiske) ska e-tjänstens insamling av uppgifter dessutom kunna förhindras genom att e-tjänstens certifikat läggs till på en separat spärrlista.

E-tjänstverktyg för utlänningar som tas i bruk genom distansregistrering är förenade med osäkerhetsfaktorer som gäller deras tillitsnivå. Till e-tjänsterna förmedlas information om huruvida ett e-tjänstverktyg för utlänningar grundar sig på distansregistrering eller om verktygets innehavares identitet har verifierats ansikte mot ansikte. E-tjänsterna kan använda denna information för att fatta ett beslut baserat på riskbedömning om huruvida de tillåter att e-tjänstverktyg som tagits i bruk enbart genom distansregistrering används i deras tjänster.

# 5 Alternativa handlingsvägar

## 5.1 Handlingsalternativen och deras konsekvenser

*Utvecklingen av e-tjänster på marknadsvillkor*

Under beredningen av propositionen har man övervägt olika alternativa sätt att främja propositionens mål. För det första har man övervägt ett alternativ där det inte skulle göras några betydande ändringar i den nuvarande lagstiftningen, varvid e-tjänsterna och den starka autentiseringen skulle fortsätta att utvecklas på marknadsvillkor. Lagstiftningen om och tjänsterna för stark autentisering har länge utvecklats på marknadsvillkor i Finland. För att utveckla och sätta fart på marknaden har det dock krävts flera ändringar i autentiseringslagen (RP 83/2017 rd, RP 264/2018 rd och RP 237/2020 rd). Lagen föreskriver bland annat om skyldighet för marknadsaktörer att ingå avtal samt om maximipriset för identifieringstransaktioner. Det är således fråga om reglering som ingriper tämligen mycket i marknadsaktörernas näringsfrihet. Tillgången till elektronisk identifiering utvecklades långsamt före lagändringen 2019, men efter det har tillhandahållandet av tjänster för identifieringsförmedling till elektroniska tjänster kommit igång bra.

Autentiseringslagens bestämmelser om informationssäkerhetskraven på identifiering är teknikneutral och de identifieringsverktyg som tillhandahålls användarna har utvecklats. Det tillhandahålls exempelvis allt flera mobilapplikationer och kodkalkylatorer och på marknaden pågår flera projekt för att tillhandahålla nya identifieringsmetoder hos till exempel mobiloperatörer, Findy-gruppen och Finlands Autentiseringsandelslag. Bland medborgarna finns det emellertid fortfarande vissa kategorier av personer som för närvarande saknar möjlighet att få identifieringsverktyg för stark autentisering. De flesta leverantörerna av identifieringsverktyg tillhandahåller verktyg till exempelvis dem som fyllt 15 år och i finanssektorns bestämmelser ingår skyldighet att tillhandahålla ett identifieringsverktyg som en del av de grundläggande banktjänsterna, men ett hinder för att få ett identifieringsverktyg för stark autentisering kan vara att personen i fråga inte är antecknad i befolkningsdatasystemet, att personen inte har ett pass eller identitetskort som utfärdats av en myndighet i Finland eller en EES-stat, Schweiz eller San Marino och som i identifieringslagen förutsätts vid inledande identifiering och polisen inte kan identifiera personen eller att personen inte har möjlighet att skaffa en mobiltelefonanslutning eller ett bankkonto.

Digitala tjänster används i allt högre grad, och i många sektorer sköts ärendena i huvudsak digitalt. När digitala servicekanaler blir de som används mest i stora delar av samhället, växer sig kravet på att alla ska ha åtkomst till tjänsterna och möjlighet att ta del av det digitala samhället allt starkare. Under beredningen har man inte systematiskt analyserat alternativet att föreskriva någon slags allmän skyldighet för leverantörerna av identifieringstjänster att tillhandahålla tjänster, men man kan anta att åtminstone utan nya bestämmelser garanterar utvecklingen av elektronisk identifiering på marknadsvillkor inte helt och hållet att propositionens mål uppnås när det gäller att tillhandahålla lika förutsättningar och möjligheter för alla att nyttja digital identitet i samhällets tjänster.

Utvecklingen av digitala tjänster förutsätter också att det utvecklas lösningar för digital identitet, så att man kan säkerställa att de motsvarar kraven på tjänster som utnyttjar modern teknik. Den nuvarande handlingsmodellen för stark autentisering baserar sig på verksamhet på marknadsvillkor, där identifieringstjänster i huvudsak tillhandahålls av privata företag och identitetshanteringen delvis kontrolleras av dessa tjänsteleverantörer. I samhället finns dock ett växande behov av nya slags tjänster, som gör det möjligt för personen själv att hantera och använda de uppgifter som gäller honom eller henne och oberoende av om han eller hon är kund hos en viss tjänsteleverantör. Ärendets karaktär kräver inte alltid att vissa identifikationsuppgifter skickas till den elektroniska tjänsten. Det kan också vara tillräckligt att visa och styrka till exempel bara åldern elektroniskt. De personuppgifter som förmedlas vid stark autentisering har förblivit desamma och för elektroniska tjänster har inte tillhandahållits ytterligare personuppgifter eller reducerade personuppgifter, dvs. exempelvis bekräftelse av endast åldersuppgiften, eller andra pseudonymiserade elektroniska bekräftelser, trots att autentiseringslagen möjliggör det. Ett mål

för denna proposition är att bygga upp förutsättningar för mer mångskiftande tjänster samt att säkerställa att det finns grundläggande beredskap i samhället att tillhandahålla även sådana lösningar för att styrka personuppgifter och andra bestyrkta uppgifter som kontrolleras av personen själv. Sådana tjänster och sådan beredskap har inte uppkommit inom ramen för den nuvarande modellen för elektronisk identifiering och man kan bedöma att det förutsätts ändringar också i fråga om den av myndigheterna bestyrkta identiteten för att målen ska nås.

*Behövliga lösningar och ändringar görs i samband med genomförandet av kommissionens lagstiftning om europeisk digital identitet*

För det andra har man under beredningen av propositionen funderat på ett alternativ där man skulle vänta på den nya lagstiftningen om europeisk digital identitet. Nationella lösningar och ändringar skulle alltså göras först i samband med de nationella åtgärderna för att genomföra EU:s lagstiftning. I avsnitt 2.7 i propositionen redogörs det mer ingående för förslaget till lagstiftning om europeisk digital identitet. Avsikten med kommissionens förslag till lagstiftning är att skapa en enhetlig rättslig ram för en applikation för en europeisk e-identitetsplånbok, med vars hjälp det skulle vara möjligt att visa upp bestyrkta uppgifter som hänför sig till plånboksapplikationens innehavare. Plånboksapplikationen ska också i EU bygga på idén om att innehavaren av plånboksapplikationen själv förfogar över sina uppgifter och beslutar hur de ska delas och användas. Under beredningen av denna proposition har man identifierat att det i kommissionens förslag till lagstiftning i många avseenden är fråga om en motsvarande lösning för digital identitet och användning av dem som i förslagen enligt denna proposition. Under beredningen har man identifierat en risk för att förslagen enligt propositionen delvis kan överlappa den EU-lagstiftning som bereds samtidigt.

Kommissionens förslag till lagstiftning innehåller en förpliktelse för medlemsstaterna att tillhandahålla en plånboksapplikation enligt EU:s lagstiftning inom 12 månader efter ikraftträdandet av lagstiftningen. Plånboksapplikationen ska kunna tillhandahållas av medlemsstaten, av en av medlemsstaten auktoriserad aktör eller av en av medlemsstaten erkänd aktör, dvs. också en aktör inom den privata sektorn som uppfyller kraven. Det bör påpekas att det är fråga om kommissionens förslag till lagstiftning om en plånboksapplikation, och innehållet i förslaget kommer sannolikt att ändras. Det råder ingen säkerhet om lagstiftningens slutliga innehåll eller om tidpunkten för ikraftträdandet. Man kan dock anta att EU:s lagstiftning kommer att förutsätta att en plånboksapplikation i någon form utvecklas och börjar tillhandahållas i medlemsstaterna. Plånboksapplikationen handlar om en ny slags tjänst med ett identifieringsverktyg för stark autentisering i anslutning till e-tjänster. Det måste reserveras tillräckligt med tid för att utveckla den. Om arbetet med att utveckla plånboksapplikationen inleds först när innehållet i den slutliga EU-lagstiftningen är känt, finns det sannolikt en risk för att plånboksapplikationen inte hinner börja tillhandahållas i Finland av den offentliga eller den privata sektorn inom den tid som EU-lagstiftningen förutsätter, eller att utvecklingsarbetet på grund av tidtabellen inte leder till en tillräckligt högklassig beredning som beaktar de nationella behoven.

Risken med att det nationella utvecklingsarbetet och beredningen av EU-lagstiftningen pågår samtidigt har bedömts vara att det kan uppstå konflikter. Också förvaltningsutskottet har funnit det viktigt att det nationella projektet för en digital identitet beaktar ändringarna i eIDAS-förordningen så att projekten inte står i konflikt med varandra. För att undvika överlappande kostnader och utvecklingsarbete borde enligt utskottet uppmärksamhet fästas vid att samordna det nationella arbetet med EU-beredningen. (FvUU 34/2021 rd)

Å andra sidan kan man också anta att det finns fördelar med samtidig beredning. Delvis parallellt nationellt utvecklingsarbete ökar kunskaperna och insikterna om vilka slags tekniska eller

funktionella lösningar det skulle vara ändamålsenligt att främja inom det europeiska samarbetet. På så vis kan Finland på ett övervägt sätt försöka påverka EU-lagstiftningens innehåll, så att där beaktas också särskilda nationella behov och sådana lösningar som har konstaterats fungera i det nationella utvecklingsarbetet. Genom att höra intressentgrupper i anslutning till det nationella utvecklingsarbete kan man också kartlägga den privata sektorns aktörers åsikter om vilka tekniska och ekonomiska omständigheter som det kan vara skäl för Finland att påverka i EU:s lagstiftningsarbete.

*Det nuvarande medborgarcertifikatet utvecklas*

I stället för den föreslagna nya lagens digitala identitet skulle medborgarcertifikatet kunna utvecklas ytterligare, så att det nyttjas i större utsträckning i samhället. Med stöd av de gällande bestämmelserna används som identifieringsverktyg nätbankskoder, identitetskortets medborgarcertifikat, organisationskortets identifieringscertifikat och mobilcertifikat. I chipsförsedda identitetskort och organisationskort finns av Myndigheten för digitalisering och befolkningsdata beviljat medborgarcertifikat eller identifieringscertifikat. Certifikatet möjliggör tillförlitlig identifiering av en person i samband med e-tjänster.

Medborgarcertifikat används dock av endast 6 procent av dem som använder identifieringsverktyg, så ett mer omfattande nyttjande av det skulle kräva utvecklingsarbete jämfört med nuläget. Myndigheten för digitalisering och befolkningsdata gjorde hösten 2021 en utredning om de nuvarande utmaningarna med kundstigen för att ansöka om, ta i bruk och använda identitetskort. I utredningens konstaterades som en central sak att användaren måste förstå, veta och kunna mycket om ibruktagandet och nyttjandet av medborgarcertifikat. Man måste förstå de tekniska egenskaperna hos de enheter som behövs för användningen för att man ska veta vilka enheter som kan användas och vilka program och vilken tilläggsutrustning de kräver. För att nyttja medborgarcertifikatet krävs dessutom en separat avläsarenhet, som inte automatiskt följer med i samband med ibruktagningsprocessen. Sammanfattningsvis konstaterade Myndigheten för digitalisering och befolkningsdata utifrån utredningen att de mest utmanande bristerna hänför sig till kortavläsarens och applikationens användbarhet. Eftersom de aktiva användarna är så få, stöder e-tjänsterna sällan identifiering med medborgarcertifikat.

Målet med de föreslagna bestämmelserna är att producera en e-legitimation, som inte är samma sak som identifieringsverktyget för stark autentisering, trots att de också innehåller egenskapen stark autentisering. E-legitimationen har en stark koppling till pass och identitetskort; som identitetshandling är den i praktiken ett alternativ till dessa. De ska ändå inte fungera som resedokument. E-legitimationen utfärdas av Polisen och uppgifterna i dem baserar sig på av Polisen bestyrkta och registrerade uppgifter. Det nuvarande medborgarcertifikatet är ett rent identifieringsverktyg, och dess teknik har inte bedömts vara på en sådan nivå att det skulle vara ändamålsenligt att utveckla certifikatet till en e-legitimation i framtiden. I och med eIDAS-utvecklingen kan det bevis för kärnidentiteten som ingår i e-legitimationen också vara något annat än ett certifikat. Bestämmelserna om det nuvarande medborgarcertifikatet baserar sig på bestämmelserna om certifikattjänster, och man kan anta att de nuvarande certifikatbestämmelserna inte är en tillräcklig grund för att utveckla tjänster för digitala identitet. Man kan också anta att det inte heller i framtiden skulle vara ändamålsenligt att nyttja medborgarcertifikatet i den digitala världen, eftersom det kräver en separat applikation för en avläsarenhet.

*Leverantören av tjänster för digital identitet blir en del av förtroendenätet*

Under beredningen av propositionen har man också bedömt ett alternativ där leverantören av tjänster för digital identitet blir en del av förtroendenätet i stället för att det föreskrivs om en

egen separat roll för leverantören i autentiseringslagen. Det redogörs mer ingående för det nationella förtroendenätet och regleringen i anslutning till det i avsnitten 2.1 och 2.2 i propositionen. Om leverantören av tjänster för digital identitet blir en del av förtroendenätet, tillämpas autentiseringslagens bestämmelser på leverantören och de verktyg som leverantören tillhandahåller. Med leverantören av tjänster för digital identitet avses i praktiken Myndigheten för digitalisering och befolkningsdata. Enligt propositionen ska leverantören producera en applikation för digital identitet med vars hjälp det är möjligt att använda e-legitimationen och e-tjänstverktyget för utlänningar.

Med e-legitimationen och e-tjänstverktyget för utlänningar blir det möjligt att styrka identiteten på elektronisk väg. Ur användarens synvinkel är det fråga om i hög grad likadana funktioner som det är möjligt att utföra med de nuvarande identifieringsverktygen, dvs. elektronisk identifiering i elektroniska tjänster för att kunna använda dem. I enlighet med propositionens målsättning främjar e-legitimationen och e-tjänstverktyget för utlänningar personers möjligheter att hantera sina egna uppgifter i offentliga tjänster. Av denna orsak grundar de sig på helt annorlunda funktionsprinciper än de identifieringsverktyg som för närvarande tillhandahålls i förtroendenätet. Detta betyder i praktiken att när en e-legitimation eller ett e-tjänstverktyg för utlänningar används för att identifiera en person på elektronisk väg så motsvarar de uppgifter som förmedlas inte nödvändigtvis den datahelhet som för närvarande förutsätts i samband med identifiering som förmedlas i förtroendenätet. En annan viktig skillnad är att leverantören av tjänster för digital identitet inte får information om när en person använder applikationen för digital identitet för e-tjänster. Sålunda har leverantören av tjänster för digital identitet ingen möjlighet att debitera ett pris per identifieringstransaktion enligt autentiseringslagen.

Om e-legitimation eller e-tjänstverktyg för utlänningar skulle tillhandahållas som identifieringsverktyg i förtroendenätet, skulle det inte vara möjligt att genomföra dem in enlighet med de funktionsprinciper som beskrivs ovan. Detta skulle dock betyda att propositionen inte längre lika starkt skulle främja en persons möjligheter att hantera sina egna uppgifter som finns i offentliga tjänster.

För en ställning utanför förtroendenätet talar också det faktum att trots att det skulle göras möjligt att styrka identiteten också på elektronisk väg med e-legitimation och e-tjänstverktyg för utlänningar, reduceras de ändå inte till enbart elektroniska identifieringsverktyg, utan det är fråga om en större helhet. När det gäller den föreslagna e-legitimationen är det fråga om en offentlig identitetshandling och för vars produktion polisen och Myndigheten för digitalisering och befolkningsdata svarar i egenskap av myndigheter. Trots att de nuvarande identifieringsverktygen kan användas för tillförlitligt styrkande av identiteten, är det i samband med identifieringsverktyg ändå inte fråga om offentliga identitetshandlingar.

## 5.2 Lagstiftning och andra handlingsmodeller i utlandet

### 5.2.1 Danmark

Danmark har redan i flera års tid betraktats som ett av de mest digitaliserade länderna i Europa och man har en klar strategi för elektronisk identifiering. De stora besluten om utvecklande av nationell elektronisk identifiering har fattats inom ramen för digitaliseringsstrategin. Strategin företräds till exempel av dokumenten Digital Strategy 2016-2020 och The future infrastructure for digital identities in Denmark.

I Danmark används det elektroniska identifieringssystemet NemID, som har utvecklats i samarbete mellan den offentliga sektorn och de danska bankerna. Med hjälp av NemID kan man uträtta ärenden i såväl den offentliga som den privata sektorns tjänster. Under 2021 och 2022

kommer MitID stegvis att ersätta NemID. MitID företräder den nya generationens NemID och är en användarvänlig och framtidsinriktad nyckel till nätbank och digital post. Jämfört med NemID har MitID också många tilläggsegenskaper och funktioner, till exempel följer det de nya underskriftsstandarderna och har smarttelefonbaserade, lösenordsbaserade och fysiska verifieringsfaktorer. Den tidigare infrastrukturen granskades och omvärderades så att man skulle kunna införa begreppet certifierad förmedlingstjänst för elektronisk identifiering, som kan förmedla identifieringstransaktioner mellan slutanvändarna och elektroniska tjänster. Syftet med MitID är bland annat att skapa bättre administrativa lösningar för företag och utvidga användningen av personlig elektronisk identifiering så att användarens personliga MitID kan kombineras med en sammanslutnings kod. I och med MitID ökar också de olika inloggningssätten. Utöver detta gör MitID skillnad mellan elektronisk identifiering och elektronisk signatur, samt gör det möjligt att använda tjänster med olika skyddsnivåer.

MitID bygger på en enda gemensam kärnidentitet, som används av offentliga aktörer och dessutom finansinstitut och andra privata tjänsteleverantörer, som behöver säkra digitala identitetsuppgifter. Ett av huvudmålen är att alla registrerade kärnidentiteter ska kunna användas mellan olika sektorer och tjänsteleverantörer. När det gäller MitID identifierar webbtjänstleverantörerna inte användarna själva, utan identifieringen sköts av certifierade förmedlingstjänster. Som förmedlingstjänster kan fungera aktörer inom den offentliga sektorn och aktörer inom den privata sektorn, särskilt banker. Förmedlingstjänster tillhandahålls på en konkurrensutsatt marknad, men identifiering med MitID är avgiftsfri.

MitID används i huvudsak med hjälp av en applikation som laddas i telefonen eller surfplattan, men andra alternativ är MitID code display, som är en liten enhet som visar ett engångslösenord, MitID audio code reader, som är avsedd för till exempel synskadade, samt MitID chip för personer som behöver MitID-inloggning flera gånger om dagen till exempel på grund av sitt arbete. Det finns dock en version av NemID även för juridiska personer, och en sådan version av MitID kommer att lanseras våren 2022.

MitID utvecklas i samarbete mellan staten och Finance Denmark (den danska bankföreningen). I MitID ersätts NemID:s indelning i två självständiga delar – en ”banklösning” och en ”OCES-lösning” med teknik som baserar sig på arkitekturen för en offentlig nyckel – med en gemensam identitet och nya verifieringsmetoder, där det finns en kärnidentitet, som stödjer verifiering samt behandlingen av digitala personidentiteters livscykel.

Den andra lösningen för elektronisk identifiering som används i Danmark är NemLog-in. NemLog-in är en inloggningslösning som möjliggör åtkomst till myndigheternas självbetjäningslösningar hos såväl kommunerna och regionerna som staten. Med hjälp av NemLog-in behöver man logga in bara en gång för att identifiera sig i alla tjänster som använder lösningen. Man loggar in i NemLogi-in med NemID eller MitID och den fungerar som förmedlare av identifieringstransaktionen. Tjänsteleverantörerna använder en NemLog-in-kod för verifiering.

NemID, MitID och NemLog-in täcker ett mycket brett urval tjänster, alla elektroniska tjänster som tillhandahålls av bank- och försäkringssektorn samt en mängd andra privata tjänster. Med dessas hjälp kan man också använda till exempel tjänsterna på adressen borger.dk. Borger.dk är en officiell samserviceportal, där man i princip har tillgång till alla offentliga tjänster i Danmark.

Trots att det inte är obligatoriskt att använda det nationella verktyget för elektronisk identifiering, använder miljontals danska medborgare elektronisk identifiering och antalet användartransaktioner är över 60 miljoner per månad. För närvarande beviljar Danmark inte något nationellt identitetskort.

### 5.2.2 Estland

Estland är ett av de mest digitaliserade länderna i Europa och ett av de mest avancerade när det gäller att införa lösningar för elektronisk identifiering. I Estland svarar två ministerier för policyn och strategin för elektronisk identifiering: inrikesministeriet samt ekonomi- och kommunikationsministeriet.

År 2020 offentliggjorde Estlands inrikesministerium en ny utvecklingsplan för den inre säkerheten 2020–2030. Enligt planen eftersträvar Estland ett stabilt och hållbart identitetshanteringssystem, där säkerhetsaspekter beaktas. Enligt planen ska Estland dessutom tillhandahålla en användarvänlig och modern applikationsmiljö, vilket också stärker informationssamhällets utveckling. För att uppnå de ovannämnda målen strävar man i Estland efter att säkra en stabil identitetshantering och identifiering av personer, använda moderna tekniska lösningar och utveckla automatiseringen av processer, samt efter att utvidga användningen av elektronisk identifiering. Stegen för att uppnå målen är fortlöpande utveckling av ett sådant identitetskort som är förenat med digital verifiering och högklassiga funktioner för att skapa en elektronisk signatur, säkerställande av förekomsten av minst två separata elektroniska identifieringsverktyg för den offentliga sektorn samt säkerställande av den offentliga och den privata sektorns samarbete och förmåga att hantera risker och farliga situationen.

I Estland används flera olika verktyg för elektronisk identifiering som beviljas av den offentliga och den privata sektorn. Mest populära är följande sju verktyg, av vilka de sex första ägs av staten och är anmälda till Europeiska unionen (samtligas tillitsnivå är ”hög”) och ett en privat metod för elektronisk identifiering som inte är anmäld. Samtliga verktyg beviljas endast fysiska personer. Verktygen är ett fysiskt ID-kort med avancerade elektroniska funktioner, ett digitalt ID, dvs. ett elektroniskt verktyg som kan användas endast i en elektronisk miljö, e-medborgarens digitala ID som beviljas andra än estniska medborgare och som kan användas för identifiering av personer och elektronisk signatur endast i en elektronisk miljö, samt ett mobil-ID som är ett verktyg för identifiering av personer och elektronisk signatur som används i en elektronisk miljö. Mobil-ID är ett frivilligt alternativ till elektronisk identifiering med ID-kort. Dessutom används ett diplomatidentitetskort som kan användas för identifiering i såväl en fysisk som en elektronisk miljö, ett uppehållstillståndskort som beviljas tredje lands medborgare och som användas för identifiering och elektronisk signatur i en elektronisk miljö, samt ett smart-ID som är en icke anmäld identifieringslösning som tillhandahålls av den privata sektorn och som också kan användas för att skapa en godkänd elektronisk signatur. Användaren måste betala en avgift för att skaffa de verktyg som staten tillhandahåller. Smart-ID är avgiftsfritt för användaren, finansieringen fås från de leverantörer av elektroniska tjänster som nyttjar det.

Estland har inga planer på att utveckla nya metoder för elektronisk identifiering under de närmaste åren, men man har planerat uppdateringar av uppehållstillståndskortet och ID-kortet. Dessutom kommer man att producera en lösning som ersätter det tidigare mobil-ID, avsikten är att det nya mobil-ID ska lanseras i början av 2022.

Inom Estlands nationella referensram för digital identitet spelar staten en ledande roll, som den som både reglerar och tillhandahåller digital identitet. Trots att också privata tjänsteleverantörer, som kan fungera som förmedlare av elektronisk identitet, tillhandahåller alternativa identifieringsmetoder, blir den identitet som finns i bakgrunden densamma och privata lösningar nyttjar den identitet som staten skapat.

I Estland är ID-kort obligatoriskt för alla medborgare över 15 år och cirka 99 procent av befolkningen i Estland använder ID-kort. Offentliga tjänster finns tillgängliga elektroniskt via portalen eesti.ee. Också många av den privata sektorns tjänster kan användas med hjälp av elektronisk

identifiering. Informationssystemmyndigheten (RIA) spelar en viktig roll för utformningen och utvecklingen av elektronisk identitet i Estland. Informationssystemmyndigheten svarar för att alla som vill kan använda chipsförsedda ID-kort. I Estland utreds också möjligheten att ta i bruk biometriska kännetecken för att identifiera personer. Estland följer riskerna med och lösningarna för elektronisk identifiering i samarbete med olika stater och nationella partner.

### 5.2.3 Norge

Norges BankID är ett allmänt system för elektronisk identifiering, som används av alla norska banker. BankID bygger på en gemensam infrastruktur, där alla användares privata nycklar för verifiering och underskrift förvaras i en centraliserad tjänst, vilket i praktiken betyder att BankID tillhandahåller en distanssignaturstjänst. BankID-systemet förutsätter i enlighet med EU:s eIDAS-regler att godkända certifikat används för underskrifter, dvs. alla BankID-beviljare ska vara godkända leverantörer av betrodda tjänster. Trots flertalet leverantörer av betrodda tjänster, finns det inga verktyg för att skapa och inga distanstjänster för en godkänd elektronisk signatur på den norska marknaden. Detta betyder att största delen av de elektroniska signaturerna är avancerade elektroniska signaturer som har beviljats genom att använda godkända certifikat.

Det finns också en mobil version av BankID, där en privat nyckel har lagrats på SIM-kort, som Mobilcertifikatet i Finland och mID i Estland och Litauen. Samtliga norska mobiltelefonoperatörer samarbetar med BankID. BankID Mobile använder ett godkänt certifikat för elektronisk signatur, men det användas bara för att underteckna korta utlåtanden i textform. Norska staten har skapat en alternativ lösning till BankID som kallas MinID. Med hjälp av MinID kan medborgarna använda offentliga tjänster som inte kräver den högsta tillitsnivån. Andra identifieringsverktyg som används i Norge är till exempel den privata sektorns Buypass och Commfides.

Inloggningsportalen ID-porten, som i stor utsträckning används hos organisationer inom den privata sektorn, har sedan 2020 tillhandahållit åtkomst till cirka 2000 webbtjänster. ID-porten upprätthålls av den offentliga förvaltningen och möjliggör flera olika inloggningssätt, såsom MinID, BankID mobile, BankID, Buypass och Commfides. Via ID-porten kan man också logga in i den centraliserade elektroniska underskrifts- och arbetsflödesportal som staten skapat.

Norge har också utvecklat ett centraliserat serviceställe som kallas Altinn. Dess uppgift är att samla alla uppgifter som alla europeiska tjänsteleverantörer behöver för att grunda ett företag i Norge. I Altinnin-portalen, som rapporterar till den offentliga sektorn, finns en juridiskt bindande samtyckeslösning, som består av verifiering, samtycke samt en logg som lagrar transaktionskedjan med tidsstämpel.

I Norge tillhandahålls QWAC-tjänster på såväl den lokala som den internationella marknaden. Godkända elektroniska stämplar tillhandahålls, men det finns inga valideringstjänster. Organisationer inom den offentliga sektorn använder en icke-godkänd elektronisk distributionstjänst. Det finns en stark företagsmarknad för godkända tillitstjänster. Arbetstagare beviljas i allmänhet ett särskilt certifikat som de kan använda i samband med anställningen, ofta tillsammans med företagets elektroniska stämpel.

I Norge finns det inte för närvarande något system för elektronisk identifiering som är anmält till Europeiska unionen, trots att det har funnits intresse för anmälan. BankID dominerar klart den norska marknaden när det gäller medborgarnas användning av identifieringstjänster och uppskattningarna av användningsgraden bland medborgarna varierar mellan 90 och 98 procent. BankID Mobiles marknadsandel är cirka 50 procent. Statens MinID-system ligger långt ifrån

detta när det gäller användningens omfattning, eftersom det i statens portal ID-porten förekommer över tio gånger flera BankID-inloggningar än MinID-inloggningar per månad. COVID-19-pandemin har haft en stor inverkan på användningen av elektroniska tjänster i Norge, antalet användare har mångfaldigats jämfört med tiden före pandemin.

Eftersom den norska lagstiftningen mycket sällan förutsätter underskrift, stödjer sig e-tjänster i Norge starkt på verifiering tillsammans med kontrolloggar. Om underskrift krävs är avancerad elektronisk signatur med godkänt certifikat vanligast, eftersom det för närvarande inte tillhandahålls några verktyg för att skapa godkända underskrifter, så det finns ingen godkänd underskriftslösning på den norska marknaden.

### 5.2.4 Nederländerna

Nederländernas Agenda för digital förvaltning (DIGIbeter) betonar den digitala identitetens betydelse och beskriver den som pelaren i den digitala förvaltningen. De åtgärder och prioriteringar som beskrivs i Agendan är bland annat utvidgad användning av säkra digitala identifieringsmetoder, säkerställande av tillgång till ett öppet elektroniskt identifieringssystem, utvecklande av applikationer i anslutning till digital identitet tillsammans med det holländska kommunförbundet och i pilotförsök med tio kommuner samt möjliggörande av webbtjänster för en annan persons eller ett företags räkning. Framstegen rapporteras till parlamentet två gånger per år.

I Nederländerna används för närvarande två system för elektronisk identifiering: DigiD för fysiska personer och eHerkenning för juridiska personer. DigiD består av ett användarnamn och ett lösenord samt av ett valbart tilläggsverifieringssteg med textmeddelande eller alternativt genom DigiD-mobilapplikationen. Den offentliga förvaltningen debiteras för tjänsterna. För närvarande är det inte obligatoriskt att använda DigiD eller eHerkenning, utom i den offentliga förvaltningens digitala tjänster, såsom elektronisk skattedeklaration. Användningen av såväl DigiD som eHerkenning har ökat avsevärt de senaste åren.

I Nederländerna bereds en lag om digital förvaltning, vars syfte är att göra det möjligt för medborgare och företag att logga in i statliga tjänster säkert och tillförlitligt, så medborgarna kan nyttja elektronisk identifiering och en tillförlitligare tillitsnivå än nu. Enligt lagen är öppna standarder obligatoriska. I lagen beskrivs också standarder för dem som tillhandahåller identifieringsverktyg.

I Nederländerna finns för närvarande både offentliga och privata tjänsteleverantörer för elektronisk identifiering. Elektronisk ärendehantering i offentliga tjänster förutsätter användning av DigiD. Enligt lagen om digital förvaltning tillåts elektronisk tillgång till offentliga tjänster emellertid via digitala identitetslösningar som utvecklats av privata företag eller av den offentliga och den privata sektorn tillsammans. I fråga om eHerkenning, som används av juridiska personer, kan användarna välja mellan privata identifieringstjänsteleverantörer som staten erkänt.

I nederländska identitetskort finns NFC-teknik och kortet kan skannas, så att medborgarens DigiD-konto kan användas för känsligare tjänster och känsligare uppgifter. Regeringen har också planer på att höja identifieringsmetodernas tillitsnivå. Både DigiD och eHerkenning har anmälts med eIDAS-tillitsnivåerna väsentlig och hög.

### 5.2.5 Tyskland

Tyska förbundsstatens ekonomi- och energiministeriums Digital strategi 2025 anger tio steg för att Tyskland ska bli Europas mest digitaliserade stat. Strategins femte steg ”Stärkande av informationssäkerheten och utvecklande av kunskapsmässig autonomi” betonar att Tyskland jämnar vägen för internationellt ibruktagande av elektronisk identifiering och anger standarder för säkra och tillförlitliga e-tjänster i hela EU.

I Tyskland har de senaste åren utarbetats lagstiftning om elektronisk identifiering. Lagen om främjande av elektronisk identifiering (Gesetz zur Förderung des elektronischen Identitätsnachweises) som trädde i kraft 2017 främjade användningen av elektronisk identifiering via det nationella eID-kortet. De första eID-korten – nationella identitetskort med eID-tilläggsfunktioner – lanserades redan 2010. Den nya lagstiftningen främjade emellertid aktivering och användning av eID-funktionen. Dessutom kan andra organisationer och företag tillhandahålla lösningar för elektronisk identifiering. Lagstiftningen förenklar processen för att bemyndiga företag och myndigheter att tillhandahålla identifieringstjänster. Den andra lagen om elektronisk identifiering, Onlinezugangsgesetz, trädde i kraft i augusti 2017. Enligt lagen ska förbundsstaten, delstaterna och kommunerna tillhandahålla sina förvaltningstjänster digitalt senast 2022.

Planen för ett digitalt Tyskland innehåller nio punkter och enligt den är ett av Tysklands mål att införa elektronisk identitet på tre sätt: ibruktagande av eID-tilläggsfunktioner i mobiltelefoner – bland annat en online ID-funktion, underlättad användning av elektronisk identifiering bland annat genom att optimera återställning och användning av PIN-kod i företagsnät, samt involvering av industrin i kommersiell användning av elektronisk identifiering.

Förutom det nationella identitetskortet och den eID-tilläggsfunktion som aktiveras i identitetskortet kan medborgare i länder utanför EU som bor i Tyskland få ett elektroniskt uppehållstillstånd (Aufenthaltstitel). Dessa identifieringsverktyg har anmälts som två delar i ett elektroniskt identifieringssystem för gränsöverskridande användning i enlighet med eIDAS-förordningen.

Den tyska lagen om identitetskort (Gesetz über eine Karte für Unionsbürger und Angehörige des Europäischen Wirtschaftsraums mit Funktion zum elektronischen Identitätsnachweis) trädde i kraft den 1 november 2019. Identitetskortet är ett fysiskt kort, som innehåller ett chips och med vilket man kan identifiera sig elektroniskt i olika offentliga och privata tjänster. Personkortets eID-tilläggsfunktion kan används också av medborgare i sådana EU-länder som (ännu) inte har ett anmält system för elektronisk identifiering oberoende av om dessa personer vistas i Tyskland eller inte. Kortet kan utfärdas för minst 16-åriga medborgare i EU eller EES-området och det är i kraft tio år. Kortet är avgiftsbelagt. eID-kortet är avsett för elektronisk identifiering, och det ersätter inte pass eller identitetskort, så eID-kortet kan inte användas som resedokument. Med eID-kortet kan man emellertid också identifiera sig på plats och det kan användas tillsammans med antingen dator eller smarttelefon.

Utöver det offentliga systemet för identitetshantering och identifiering finns det i Tyskland också lösningar för den privata sektorn. Lösningarna fungerar dock på lägre nivå än de statliga verktygen, och de motsvarar till exempel inte kraven på elektronisk identifiering enligt penningtvättsdirektivet (EU) 2015/849.

Andra lösningar för elektronisk identifiering, som delvis bygger på förnyad användning av det tyska eID, är det PostID-system som utvecklats av Deutsche Post och med vars hjälp användarna kan arkivera personuppgifter efter den ursprungliga identifieringen och använda dem på nytt i andra processer, den elektroniska identifieringslösningen Identity Giro, som baserar sig på uppgifter som samlats i banksystemen, sparbankernas och andelsbankernas YES-system, med vars

hjälp användarna kan använda nätbankstjänster, samt Verimi, som är en inloggningslösning där användarna kan lagra sitt identitetskort eller körkort för att identifiera sig och för att kunna registrera sig och använda denna registrering i olika partnerskapstjänster, för närvarande till övervägande del finans- och försäkringsbolags tjänster.

Vid sidan av ibruktagande av eID-kortet är en av Tysklands prioriteringar enligt niopunktsplanen ibruktagande av ett mobilt eID. Flera nya lösningar för elektronisk identifiering är också under utveckling. En sådan är till exempel systemet SmartLogin, som för närvarande är tillgängligt för testning och som tillhandahåller användaren åtkomst till en Smart Wallet, där användaren kan lagra sina personuppgifter och använda dem tillsammans med olika tjänsteleverantörer.

Ett utvecklingsobjekt som är under planering i Tyskland är att utvidga antalet tjänster som är tillgängliga via olika metoder för elektronisk identifiering. Exempelvis YES-systemet ger användarna möjlighet att nyttja sina personuppgifter hos andra tjänsteleverantörer. Dessutom är målet för OPTIMOS-projektet som finansieras av förbundsstatens ekonomi- och energiministerium att ta i bruk en Secure eID-applikation genom en tjänst för elektronisk identifiering som stödjer elektronisk identifiering och verifiering samt överföring av personuppgifter.

En del av Tysklands lösningar för elektronisk identifiering bygger på lösningar som staten ansvarar för och en del på sådana som utvecklats av privata aktörer. Å andra sidan är det nationella eID-kortet helt och hållet en tjänst inom den offentliga sektorn, där staten tillhandahåller identiteten. De andra eID-verktyg som presenteras ovan levereras av privata företag – för deras del fungerar staten som förmedlare av elektronisk identifiering när identitetsleverantörer och tjänsteleverantörer sammanförs.

Enligt statistik från oktober 2018 fanns det i Tyskland över 75 miljoner eID-kort och 12 miljoner elektroniska uppehållstillstånd. eID-kortet möjliggör tillgång till över 60 tjänster, som tillhandahålls av såväl offentliga som privata aktörer. Förbundsstatens tjänster kan nås via en portal, men eftersom flera digitala tjänster administreras på lokal nivå, är sådan användning av elektronisk identifiering som främjar samserviceprincipen helt effektiv först när förbundsstatens och de lokala portalerna har slagits samman. Genom att använda det nationella eID-kortet kan man emellertid uträtta ärenden också i portalerna på lokal nivå. Allmän information om användningen av elektroniska identifieringsverktyg ges via en separat webbplats.

I Tyskland stärks användningen av elektronisk identifiering ytterligare senast 2022, då avsikten är att förbundsstaten, delstaterna och kommunerna ska tillhandahålla alla förvaltningstjänster digitalt i Tyskland via förvaltningsportaler och länka dessa portaler till ett nät, som man har åtkomst till också med eID-kort och andra lättanvända identifieringsmetoder. Ju högre tillitsnivå en administrativ tjänst har, desto högre än kraven på de identifieringsverktyg som ska användas. De ändringar som planeras i eID-kortet i framtiden är i första hand fokuserade på små justeringar i anslutning till det accessprotokoll som används för att läsa chipset. För närvarande är det obligatoriskt att foga fingeravtryck till kortet.

## 6 Remissvar och den fortsatta beredningen

### 6.1 Remissvar

Finansministeriet begärde utlåtanden om utkastat till regeringens proposition med förslag till lagstiftning om digital identitet via tjänsten Utlåtande.fi under tiden 21 februari–8 april 2022. Inom utsatt tid kom det 651 remissvar på begäran om utlåtande. Av dessa kom 127 utlåtanden från organisationer. Tio som svarade meddelade att de inte har något att yttra i saken. Efter

remisstidens utgång tillfrågades dessutom aktörer inom förtroendenätet om de vill yttra sig. De som besvarade förfrågan bekräftade att de inte avger separat utlåtande utan förenar sig med intresseorganisationernas (Finanssiala ry eller FiCom) utlåtanden. Responsen från medborgarna omfattade sammanlagt 524 utlåtanden inom utsatt tid. Utlåtandena och ett sammandrag av dem finns i statsrådets projektportal (projekt-ID VM092:00/2021). En klar majoritet av de organisationer som svarade ansåg att de mål och lösningar som föreslås i propositionen överlag kunde understödas. I utlåtandena ansåg man att eftersom digitala tjänster och elektronisk kommunikation snabbt utvecklats och blivit vanligare finns det ett behov av en självägd digital identitet i såväl offentliga som privata elektroniska tjänster.

I remissvaren lyftes det upprepade gånger fram att när den nationella e-legitimationen och tjänster i anslutning till den utvecklas bör det eIDAS-ändringsförslag och den utveckling av lagstiftningen om europeisk digital identitet som samtidigt pågår på EU-nivå beaktas. På grundval av remissvaren har motiveringen till regeringens proposition kompletterats så att förhållandet mellan den föreslagna lagstiftningen och eIDAS-ändringsförslaget framgår tydligare av propositionen. På grundval av Konkurrens- och konsumentverkets remissvar har konsekvenserna för konkurrensen kompletterats med en beskrivning av förhållandet mellan förslagen i propositionen och identifieringsmarknadens utveckling.

Även Myndigheten för digitalisering och befolkningsdata lyfte i sitt utlåtande fram att lagstiftningen i Finland inte får utgöra ett hinder för genomförandet av en europeisk e-identitetsplånbok. Myndigheten sade i sitt utlåtande att en stark koppling av den digitala identiteten till de nuvarande fysiska identifieringshandlingarna skulle i framtiden förhindra ett fullödigt nyttjande av finländska digitala identitetsplånböcker. Enligt utlåtandet borde redan den lösning som genomförs nu bygga på en av Myndigheten för digitalisering och befolkningsdata bestyrkt digital identitet med en livscykel som grundar sig på lösningens informationssäkerhet och som är separat från e-legitimationen. På grund av remissvaret har de bestämmelser som föreslås i regeringens proposition ändrats så att det bevis för kärnidentitet som Myndigheten för digitalisering och befolkningsdata producerar har en självständig informationssäkerhetsrelaterad giltighetstid. Sålunda är giltighetstiden för beviset för kärnidentitet inte bunden till giltighetstiden för den identitetshandling som ligger till grund för e-legitimationen.

I remissvaren efterlystes en möjlighet för aktörer i den privata sektorn att skapa tjänster som grundar sig på den kärnidentitet som staten skapar. Även kommunikationsministeriet betonade i sitt utlåtande att beviset för kärnidentitet borde planeras så att det i framtiden kan nyttjas också i plånboksapplikationer som den privata sektorn producerar och således möjliggöra utveckling av motsvarande produkter och konkurrens även inom den privata sektorn. Motiveringen till propositionen har preciserats till följd av remissvaren så att det framgår klart av propositionen att målet är att i framtiden göra det möjligt för den privata sektorn att nyttja beviset för kärnidentitet som grund för tjänster som den producerar. Det föreslås ändå inga ändringar i de bestämmelser som ingår i propositionen.

Myndigheten för digitalisering och befolkningsdata påpekade i sitt utlåtande att propositionen borde ta ställning till hur det är möjligt för medborgaren att försäkra sig om tjänstens identitet när han eller hon visar sina personuppgifter. Utifrån Myndigheten för digitalisering och befolkningsdatas utlåtande har propositionen kompletterats med nya bestämmelser i den föreslagna lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata. Till lagförslaget fogades en ny 8 §, där det föreskrivs om autentisering av en förlitande part samt registret över uppgifter i anslutning till autentiseringen och en ny 26 § där det föreskrivs om förlitande parters anmälningsplikt.

Finanssiala ry och Konkurrens- och konsumentverket framförde i sina utlåtanden att i den föreslagna lagstiftningen är det fråga om ett identifieringsverktyg som innehas och används av medborgarna och om reglering av det och av denna orsak borde rättigheterna och skyldigheterna för innehavaren av en e-legitimation och ett identifieringsverktyg för fysiska personer framgå exakt av lagstiftningen. Den föreslagna lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata har på grundval av remissvaren utökats med en ny 28 § där det föreskrivs om begränsningar av ansvaret vid obehörig användning av applikationen för digital identitet.

När det gäller e-tjänstverktyget för utlänningar var en utmaning som lyftes fram i remissvaren att elektroniska tjänster själva måste bestämma om de godkänner tillträde till sina tjänster med e-tjänstverktyget när e-tjänstverktygets tillförlitlighet inte når upp till nivån för stark autentisering. Enligt remissvaren kunde det vara ändamålsenligt att föreskriva särskilt om de uppgifter som förutsätter användning av ett e-tjänstverktyg med högre tillitsnivå. Det föreslås ändå inga ändringar i propositionen utifrån remissvaren, eftersom en sådan reglering kunde begränsa möjligheten att nyttja e-tjänstverktyget vid identifiering i elektroniska tjänster. De som tillhandahåller elektroniska tjänster har bästa förutsättningar att bedöma vilka tjänster som kan tillhandahållas personer som använder ett e-tjänstverktyg som grundar sig på distansregistrering för identifiering. Av denna orsak är det ändamålsenligt att elektroniska tjänster själva utifrån en riskbedömning beslutar hur e-tjänstverktyget kan nyttjas i deras tjänster.

Flera remissinstanser ansåg att användningen av e-tjänstverktyget för utlänningar är utmanande, ifall verktyget inte får samma ställning som stark autentisering. De bestämmelser som föreslås i regeringens proposition har ändrats utifrån remissvaren så att det framgår klarare att det kan finnas två slags e-tjänstverktyg med olika tillförlitlighet beroende på om e-tjänstverktyget grundar sig på enbart distansregistrering eller identifiering ansikte mot ansikte. Dessutom har de föreslagna bestämmelserna kompletterats så att e-tjänstverktyget får ställning som stark autentisering när personen har identifierats ansikte mot ansikte varvid identifiering av personen som sker med hjälp av e-tjänstverktyget kan förmedlas i förtroendenätet enligt autentiseringslagen.

Dataombudsmannen ansåg i sitt utlåtande att det är bra att de personuppgiftsansvariga samt de personuppgiftsansvarigas ansvar har definierats klart och med beaktande av det nationella handlingsutrymme som dataskyddsförordningen tillåter i förslaget i fråga om de nu aktuella behandlingsåtgärderna. Enligt justitieministeriets utlåtande hänför sig de viktigaste kompletteringsbehoven i propositionen till bedömning av dataskydds- och informationssäkerhetsriskerna och ministeriet framförde i sitt utlåtande flera detaljerade anmärkningar och preciseringsförslag till lagstiftningsförslagen om dataskydd och motiveringen till dem. Bestämmelserna i regeringens proposition och motiveringen till dem har kompletterats på de sätt som föreslås i justitieministeriets utlåtande. Också propositionens bedömning av konsekvenserna för skyddet av personuppgifter och informationssäkerheten har kompletterats på grund av remissvaren.

Vad gäller behandling av ansiktsbilder anser justitieministeriet i sitt utlåtande att de föreslagna bestämmelserna i ljuset av å ena sidan lagförslagen och deras specialmotivering samt å andra sidan definitionen i artikel 4.1 i dataskyddsförordningen och skäl 51 i ingressen klart innebär att det är fråga om behandling av biometriska uppgifter. Enligt justitieministeriet kräver motiveringen till lagstiftningsordningen ändringar och komplettering i detta avseende. Under den fortsatta beredningen av regeringens proposition har det på grundval av justitieministeriets remissvar gjorts en bedömning av huruvida behandlingen av ansiktsbilder innebär behandling av biometriska uppgifter . Trots justitieministeriets bedömning har man i propositionen hållit fast vid den tidigare bedömningen i propositionen enligt vilken det inte är fråga om behandling av biometriska uppgifter. Propositionens motivering som gäller lagstiftningsordningen har dock kompletterats i detta avseende.

I flera utlåtanden understöddes att lagen skulle få ett klart krav på säkerheten och godkännandeförfarandet för informationssystemet för digital identitet. I Transport- och kommunikationsverket Traficoms utlåtande ansågs det viktigt och värt att understöda att lagen innehåller bestämmelser om informationssäkerhetskrav och att Myndigheten för digitalisering och befolkningsdata ska höra Traficom innan myndigheten meddelar ett beslut om informationssäkerhetskrav. Polisstyrelsen lyfte dock i sitt utlåtande fram behovet av noggrannare bestämmelser om den övergripande säkerheten hos e-legitimationen så att även säkerheten hos lösningarna i anslutning till dess användning vid uträttande av ärenden på plats tydligt beaktas. I regeringens proposition föreslås det ändå inte några noggrannare bestämmelser om säkerhetskraven på e-legitimation på grund av remissvaret. Sådana detaljerade bestämmelser är inte ändamålsenliga när tekniken utvecklas och standarderna ändras och uppdateras med jämna mellanrum. I den föreslagna lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata har det på grund av Polisstyrelsens remissvar gjorts ett tillägg till 5 §, enligt vilket Myndigheten för digitalisering och befolkningsdata ska höra även Polisstyrelsen innan den meddelar ett beslut om krav på informationssäkerhet.

Särskilt arbets- och näringsministeriet, Konkurrens- och konsumentverket och FiCom uttalade sig om propositionens konsekvenser för konkurrensen. Särskilt Konkurrens- och konsumentverket samt FiCom framförde kritiska anmärkningar. I utlåtandena ansågs det sannolikt att lösningen kan vara förenad med ekonomisk verksamhet som måste separeras från myndighetsverksamheten. I utlåtandena konstaterades det dessutom att i framtiden kan tillhandahållandet av plånboksapplikationer bli ekonomisk verksamhet i en rådande konkurrenssituation på marknaden, och staten får inte på grund av den föreslagna reformen få ogrundat företräde på marknaden. Också i Traficoms, Elisas och Telias utlåtanden konstaterades att konsekvenserna för förtroendenätets marknad och tekniska verksamhet inte hade bedömts tillräckligt djupgående. I utlåtandena framfördes att det är oklart hur det nya verktyget kommer att påverka marknaden och priserna för identifieringstjänster. Propositionens konsekvenser för konkurrensen och för aktörerna i förtroendenätet har kompletterats avsevärt på grundval av remissvaren.

I remissvaren sågs det som en brist hos propositionen att den inte innehåller något förslag till nationell lösning för stark autentisering i telefontjänster. I regeringens proposition har det inte intagits några bestämmelser om uträttande av ärenden per telefon på grund av remissvaren, eftersom det inte är propositionens målsättning att föreslå några egentliga lösningar på denna utmaning. I detta sammanhang bör det ändå konstateras att förslagen enligt regeringens proposition inte på något sätt hindrar eller begränsar möjligheten att i Finland utveckla lösningar för stark autentisering för uträttandet av ärenden per telefon.

I propositionen gjordes dessutom flera andra tekniska ändringar på grund av remissvaren. Dessutom har konsekvensbedömningen i propositionen kompletterats på grund av remissvaren.

Medborgarresponsen på den föreslagna lagstiftningen var nästan undantagslöst kritisk. I responsen lyfte man särskilt fram oro för att finska staten skulle utvecklas till en kontrollstat och för att digitala identitetshandlingar skulle bli obligatoriska, åsikter om att systemet är onödigt samt tvivel beträffande informationssäkerheten. Orsaken till responsen föreföll vara felaktiga tolkningar av projektets mål och den föreslagna lagstiftningens innehåll. Propositionens mål är inte att öka statens kontrollmöjligheter i förhållande till medborgarna utan tvärtemot att förbättra medborgarnas möjlighet att hantera sina egna uppgifter bättre och säkrare. E-legitimationen, e-tjänstverktyget för utlänningar och identifieringsverktyget för fysiska personer är inte obligatoriska och ingen behöver ta något av dem i bruk mot sin vilja. På grundval av remissvaren har strävan varit att lyfta fram dessa saker tydligare i regeringens proposition.

### 6.2 Den fortsatta beredningen

I flera utlåtanden tog man ställning till användningsområdet för identifieringsverktyget för fysiska personer. I princip understöddes också möjlighet att kunna nyttja identifieringsverktyget för fysiska personer även i den privata sektorns tjänster. Möjligheten att utvidga användningsområdet utreddes under den fortsatta beredningen. Av utredningarna framgick det emellertid att det vore utmanande att utvidga användningsområdet särskilt på grund av konkurrensrättsliga frågor, eftersom det redan finns motsvarande identifieringsverktyg på marknaden. Av denna orsak föreslås det inga ändringar i användningsområdet för identifieringsverktyget för fysiska personer i propositionen. Användningsbehovet i fråga om identifieringsverktyget för fysiska personer följs dock upp.

Diskrimineringsombudsmannen påpekade i sitt utlåtande att de riktlinjer och rutiner som innebär att identifieringsverktyg för stark autentisering inte kan beviljas personer med funktionsnedsättning som anlitar assistent är problematiska med avseende på diskrimineringslagen. Enligt remissvaret borde man överväga möjligheten att i propositionen förtydliga att det inte är fråga om obehörig användning av verktyget eller överlåtelse av det för att användas av någon annan när en assistent till en person med funktionsnedsättning på hans eller hennes begäran hjälper honom eller henne att använda verktyget. Under den fortsatta beredningen utreddes om det skulle vara möjligt att göra den föreslagna preciseringarna inom de gränser som den nationella och EU-regleringen tillåter. På grund av att tolkningen hänför sig till EU-regleringen tillfrågades också andra medlemsstater i EU om deras åsikter. På grund av svaren har man i andra medlemsstater tolkat EU:s förordning om tillitsnivåer på samma sätt som i Finland och identifieringsverktyg har inte beviljats personer som i praktiken inte förmår eller juridiskt inte kan använda identifieringsverktyget självständigt. Av denna orsak föreslås inga ändringar i propositionen.

Det är viktigt att främja jämlika möjligheter att sköta ärenden elektroniskt, trots att det inom ramen för denna proposition inte har varit möjligt att lösa alla de utmaningar med detta som i remissvaren lyfts fram . I fortsättningen bör olika alternativa sätt att lösa utmaningarna utredas. Alternativ som bör utredas är möjligheterna att ändra den nationella regleringen till exempel så att vissa krav på EU-nivå inte förutsätts på nationell nivå eller så att det skapas förutsättningar för att utveckla och använda fullmakter. I det sammanhanget vore det också ändamålsenligt att ytterligare utreda användningsområdet för identifieringsverktyget för fysiska personer med avseende på användningsbehov och likabehandling. Ur jämlikhetssynvinkel skulle det vara ändamålsenligt att i det sammanhanget utreda möjligheterna att på vissa villkor i samband med utkomststöd få en betalningsförbindelse för anskaffning av identifieringsverktyget för fysiska personer

## 7 Specialmotivering

### 7.1 Lag om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata

#### 1 kap. Allmänna bestämmelser

**1 §.** *Tillämpningsområde.* Paragrafen innehåller bestämmelser om lagens tillämpningsområde. Enligt paragrafen innehåller lagen bestämmelser om de tjänster för digital identitet som produceras av Myndigheten för digitalisering och befolkningsdata och om nyttjande av sådana tjänster. Med tjänster för digital identitet avses ett informationssystem för digital identitet, bevis för kärnidentitet, e-tjänstverktyg för utlänningar, en tjänst för hantering av digital identitet samt ett avläsargränssnitt och kontrollapplikationer.

**2 §.** *Definitioner.* Paragrafen innehåller de väsentliga begrepp som används i lagen och definitioner av dem. Enligt *1 punkten* avses i lagen med tjänster för digital identitet ett informationssystem för digital identitet, bevis för kärnidentitet, e-tjänstverktyg för utlänningar, en tjänst för hantering av digital identitet, ett avläsargränssnitt och kontrollapplikationer. Samtliga dessa tjänster ska produceras av Myndigheten för digitalisering och befolkningsdata. Enligt *2 punkten* avses med kärnidentitet en sådan helhet av personuppgifter registrerade i befolkningsdatasystemet med vars hjälp identiteten allmänt kan specificeras och som består av de uppgifter som avses i 13 § 1 mom. 1 och 2 punkten i lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata. Dessa uppgifter är en persons fullständiga namn och personbeteckning, födelsetid och individuella nummer samt en teknisk identifieringskod och en elektronisk kommunikationskod. Enligt *3 punkten* avses i lagen med bestyrkta uppgifter personuppgifter som verifierats av en myndighet på elektronisk väg. Det är fråga om uppgifter som härrör från informationsresurser eller register som administreras av myndigheten, och vilkas äkthet och oföränderlighet har verifierats tekniskt. Enligt *4 punkten* avses med e-legitimation en av polisen beviljad identitetshandling som avses i 3 § i lagen om e-legitimation och som utfärdas av polisen. Enligt *5 punkten* avses med teknisk plattform användarens mobila terminal, som innehåller en e-legitimation eller ett e-tjänstverktyg för utlänningar. Enligt *6 punkten* avses med applikation för digital identitet en applikation som innehavaren av en identitetshandling har på sin mobila terminal och som gör det möjligt att använda en e-legitimation eller ett e-tjänstverktyg för utlänningar. Personen laddar själv ned applikationen i sin telefon, varefter det är möjligt att ta i bruk handlingarna. Enligt *7 punkten* avses i lagen med förlitande part en fysisk eller juridisk person för vilken innehavaren av en e-legitimation eller ett e-tjänstverktyg för utlänningar styrker sin identitet eller visar bestyrkta uppgifter. För juridiska personers del är det fråga om olika elektroniska tjänster eller fysiska kundserviceställen där det finns behov av att identifiera en person eller bestyrka vissa uppgifter som gäller honom eller henne för tillhandahållandet av tjänster. Syftet med den förlitande partens behandling av uppgifter är inte av betydelse för definitionen, utan det väsentliga är att innehavaren av en e-legitimation eller ett e-tjänstverktyg för utlänningar har behov av att styrka sin identitet eller visa bestyrkta uppgifter i anslutning till den, och att den förlitande parten i sin tur behöver kunna lita på dessa uppgifter. Enligt *8 punkten* avses med uträttande av ärenden på plats att ärenden uträttas på så sätt att innehavaren av en e-legitimation och den förlitande parten samtidigt är närvarande på samma plats och innehavaren av e-legitimationen visar upp sin i identitetshandlingen bestyrkta identitet eller andra bestyrkta uppgifter gällande honom eller henne till den förlitande parten. Det är fråga om interaktion ansikte mot ansikte där innehavaren av en e-legitimation styrker sin identitet eller visar bestyrkta uppgifter i anslutning till den för en förlitande part. Det har ingen betydelse om handlingen visas för en annan fysisk person i privatlivet eller till exempel för en representant för en näringsidkare. Med uträttande av ärenden på plats avses ändå inte till exempel situationer där en person är fysiskt närvarande i en lokal, men kommunicerar med en automat eller någon annan teknisk terminal.

**3 §.** *Personuppgiftsansvarig för tjänster för digital identitet.* I paragrafen föreskrivs det om personuppgiftsansvariga för digital identitet. Med tjänster för digital identitet avses ett informationssystem för digital identitet, bevis för kärnidentitet, e-tjänstverktyg för utlänningar, en tjänst för hantering av digital identitet samt ett avläsargränssnitt och kontrollapplikationer. Separata bestämmelser om datainnehållet i dessa register ingår i en egen paragraf, men i denna paragraf bestäms det om den personuppgiftsansvarige för respektive register och om det nationella handlingsutrymmet i anslutning till registerföringen enligt dataskyddsförordningen. Detta handlingsutrymme tillämpas således på alla de register för tjänster för digital identitet som Myndigheten för digitalisering och befolkningsdata producerar.

Enligt artikel 4.7 i dataskyddsförordningen avses med personuppgiftsansvarig 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. Om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt inom ramen för det nationella handlingsutrymmet enligt artikel 6.3 i dataskyddsförordningen, kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt. Inom ramen för det nationella handlingsutrymmet enligt dataskyddsförordningen är det möjligt att föreskriva om ändamålet med behandlingen enligt artikel 6.1 c och e, som ska vara nödvändig för att utföra en uppgift av allmänt intresse eller för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. Det nationella handlingsutrymmet möjliggör särskilda bestämmelser, genom vilka tillämpningen av dataskyddsförordningen anpassas bland annat i fråga om lagenligheten hos den personuppgiftsansvariges databehandling, de sammanslutningar till vilka och de ändamål för vilka personuppgifter får lämnas ut samt behandlingsåtgärder och förfaranden. Dessutom ska medlemsstaternas nationella rätt uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas. Till personuppgiftsansvarig ska i vilket fall som helst utses en sådan aktör som faktiskt utövar den bestämmanderätt som hör till den personuppgiftsansvarige och som kan uppfylla de förpliktelser som hör till den personuppgiftsansvarige. Den rättsliga grunden för behandling av personuppgifter i samband med produktionen av tjänster för digital identitet är artikel 6.1 c i dataskyddsförordningen.

Enligt paragrafen är Myndigheten för digitalisering och befolkningsdata personuppgiftsansvarig för behandlingen av personuppgifter i samband med produktionen av tjänster för digital identitet och svarar till denna del för de förpliktelser som dataskyddsförordningen ålägger den personuppgiftsansvarige. Behandlingen av personuppgifter i samband med produktionen ska omfatta bland annat tillräcklig informationssäkerhet för personuppgifterna samt sammanställande av personuppgifter som är nödvändiga för att producera tjänsterna för att ett informationssystem för digital identitet ska kunna tillhandahållas. Enligt paragrafen andra mening har Myndigheten för digitalisering och befolkningsdata dock inte rätt att lämna ut personuppgifter som behandlas i samband med produktionen av tjänster för digital identitet till en förlitande part. Här har man utnyttjat dataskyddsförordningens nationella handlingsutrymme och föreskrivit om utlämnande av personuppgifter som en behandlingsåtgärd utanför Myndigheten för digitalisering och befolkningsdatas personuppgiftsansvar. Uppvisandet av personuppgifter som behandlas i tjänster för digital identitet, i praktiken informationssystemet för digital identitet, ska helt och hållet kontrolleras av den fysiska personen själv: han eller hon ska själv kunna besluta för vilka aktörer och i vilka sammanhang han eller hon styrker sin identitet och visar sina bestyrkta uppgifter.

Informationssystemet för digital identitet, som ingår i tjänsterna för digital identitet, gör det möjligt att använda e-legitimation enligt 3 § i lagen om digitala identitetshandlingar som produceras av polisen. I 5 § i lagen om e-legitimation föreskrivs om registret över e-legitimation, som förs av polisen och för vilket polisen är personuppgiftsansvarig.

## 2 kap. Väsentliga krav på informationssystemet för digital identitet och bedömning av kraven

**4 §.** *Informationssystemet för digital identitet.* I paragrafen föreskrivs det om informationssystemet för digital identitet, som är en viktig ny tjänst för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata. I 1 *mom.* föreskrivs att Myndigheten för digitalisering och befolkningsdata ska producera en applikation för digital identitet samt ett sådant informationssystem för digital identitet som består av ett bakomliggande system för applikationen. Informationssystemet ska bestå av en applikation som en fysisk person installerat på sin tekniska plattform och ett tillhörande bakomliggande system som administreras av Myndigheten för digitalisering och befolkningsdata. Enligt det föreslagna momentet ska med hjälp av

informationssystemet för digital identitet kunna visas bestyrkta uppgifter för elektroniska tjänster eller för en terminal som används vid kundkontakter. Med uppvisande av bestyrkta uppgifter avses att en fysisk person som nyttjar informationssystemet för digital identitet visar bestyrkta uppgifter för en förlitande part i anslutning till uträttande av ärenden antingen i e-tjänster eller på plats. Med termen ”visa” hänvisas till situationer där den registrerade på grundval av egen prövning ger sina uppgifter till en förlitande part.

Enligt förslaget till 2 *mom.* är avsikten med informationssystemet för digital identitet att göra det möjligt att producera och nyttja e-tjänstverktyg för utlänningar och den e-legitimation som avses i lagen om e-legitimation. Det föreslås alltså att samma informationssystem ska fungera som teknisk implementering av såväl e-legitimation som e-tjänstverktyg för utlänningar. Informationssystemet ska användas för att producera e-legitimation till exempel så att innehavaren av en e-legitimation enligt lagen om e-legitimation, dvs. en fysisk person som använder en mobilapplikation på sin tekniska plattform, styrker sin identitet elektroniskt för en förlitande part och beslutar i detta sammanhang att visa sina bestyrkta uppgifter för den förlitande parten. Bestyrkta uppgifter ska också kunna visas med informationssystemet för digital identitet i anslutning till uträttande av ärenden på plats, så att en fysisk person som använder en mobilapplikation styrker sin identitet för en förlitande part med mobilapplikationen och visar därefter de bestyrkta uppgifter som behövs för den förlitande parten genom att nyttja kontaktlös läsning.

**5 §**. *Kvalitets- och informationssäkerhetskrav*. I paragrafen föreskrivs de huvudsakliga kvalitets- och informationssäkerhetskrav som gäller informationssystemet för digital identitet. Myndigheten för digitalisering och befolkningsdata ska i egenskap av myndighet iaktta de grundläggande krav på informationssäkerhet inom den offentliga förvaltningen som föreskrivs i 4 kap. i informationshanteringslagen när den producerar informationssystemet för digital identitet. Den föreslagna paragrafen innehåller särskilda krav som gäller informationssystemet för digital identitet och som går utöver och preciserar de grundläggande krav på informationssäkerhet som föreskrivs i informationshanteringslagen. Avsikten med bestämmelserna är således inte att avvika från de allmänna bestämmelserna i informationshanteringslagen.

I *1 mom.* föreskrivs det att informationssystemet alltid ska vara tillgängligt, och det ska ha de reservsystem som behövs med tanke på störningar. Avsikten med bestämmelsen är att säkerställa att en störning eller ett avbrott i informationssystemet inte äventyrar de tjänster som ska produceras med dess hjälp, eller säkerheten för de uppgifter som ingår i det. Myndigheten för digitalisering och befolkningsdata ska vidta de åtgärder som behövs för att informationssystemets funktion ska kunna säkerställas under alla förhållanden. Härmed avses särskilt sådana reservsystem med vilkas hjälp funktionen kan säkras under störningar. Kravet på informationssystemets oavbrutna användbarhet förutsätter emellertid i praktiken också förberedelser i organisationens verksamhet.

I *2 mom.* ingår särskilda krav på informationssystemets informationssäkerhet. Myndigheten för digitalisering och befolkningsdata ska genom administrativa och tekniska åtgärder sörja för informationssystemets informationssäkerhet så att kraven uppfylls. Med administrativa åtgärder avses att administreringen av informationssystemet eller myndighetens verksamhet ordnas på det sätt som kraven förutsätter. Med tekniska åtgärder avses tekniska förfaranden och lösningar. Enligt 2 mom. *1 punkten* ska Myndigheten för digitalisering och befolkningsdata sörja för att informationssystemet och den information som behandlats där är tillgängliga endast för dem som har rätt att använda systemet och informationen. Enligt *2 punkten* ska Myndigheten för digitalisering och befolkningsdata sörja för att informationen och informationssystemet inte kan ändras av andra än dem som har rätt till detta. Förutsättningen är central för de tjänster som produceras med hjälp av informationssystemet för digital identitet. Tillförlitligheten hos e-legitimationen och e-tjänstverktyget för utlänningar baserar sig på att uppgifterna är oföränderliga

och uppdaterade. Enligt *3 punkten* ska Myndigheten för digitalisering och befolkningsdata sörja för att informationen och informationssystemet kan nyttjas endast av dem som har rätt att använda informationen och systemet. Enligt *4 punkten* ska Myndigheten för digitalisering och befolkningsdata sörja för att informationen och informationssystemet tål sådana avancerade hot mot informationssäkerheten som kan förväntas. Myndigheten för digitalisering och befolkningsdata ska i sin verksamhet säkerställa att den har aktuell information om eventuella hot som riktar sig mot systemets funktion och om den tekniska utvecklingen. Informationssystemets säkerhet ska utvärderas och utvecklas regelbundet. Enligt *5 punkten* ska Myndigheten för digitalisering och befolkningsdata sörja för att sådana betydande kränkningar av och hot mot informationssäkerheten som riktas mot informationssystemet kan upptäckas. Bestämmelsen förutsätter att Myndigheten för digitalisering och befolkningsdata tar i bruk de tekniska och administrativa åtgärder som behövs för att avvikelser i systemets funktion ska upptäckas och med anledning av dem vidtar tillräckliga åtgärder för att förhindra eventuella hot.

Vissa krav i 2 mom. i den föreslagna paragrafen motsvarar vissa krav på behandlingen av personuppgifter i dataskyddsförordningen. Skyddet för personuppgifter bör säkerställas i första hand med stöd av dataskyddsförordningen och den nationella allmänna lagstiftningen och det ska inte föreskrivas nationellt om sådant som det redan föreskrivs om i den allmänna dataskyddsförordningen. För att säkerställa informationssystemets informationssäkerhet förutsätts dock att även andra personuppgifter än de som avses i artikel 4.1 i dataskyddsförordningen skyddas, så till denna del gäller de föreslagna bestämmelserna inte som sådana behandlingen av personuppgifter, utan det är i första hand fråga om att säkerställa informationssäkerheten för annan information för att skydda den information som behandlas. Att det föreskrivs om informationssäkerhetskrav påverkar ändå inte den personuppgiftsansvariges skyldighet enligt den allmänna dataskyddsförordningen att genomföra lämpliga informationssäkerhetsåtgärder eller den personuppgiftsansvariges ansvar för behandlingen av personuppgifter i anslutning härtill. Till den del som de särskilda kraven ändå gäller personuppgifter är det fråga om att i en enstaka situation inom ramen för det nationella handlingsutrymmet precisera korrekthetsprincipen enligt artikel 5.1 d i dataskyddsförordningen samt reglerna om integritet och konfidentialitet enligt artikel 5.1 f. .

I *3 mom.* föreskrivs det om skyldighet för Myndigheten för digitalisering och befolkningsdata att besluta om närmare tekniska krav på informationssystemet och om krav på informationssäkerhet. Det ska vara myndighetens uppgift att fastställa närmare tekniska krav på informationssystemet och krav på informationssäkerhet. Kraven ska dock grunda sig på denna lag, EU:s förordning om elektronisk identifiering och allmänt kända nationella eller internationella standarder. Myndigheten för digitalisering och befolkningsdata beslutar om de standarder, tekniska specifikationer eller kriterier som ska tillämpas för att uppfylla och bedöma kraven. Sådana standarder och bedömningskriterier är till exempel Katakri, dvs. den nationella kriteriesamlingen för säkerhetsauditering samt internationella ISO 27001 Ledningssystem för informationssäkerhet. Innan Myndigheten för digitalisering och befolkningsdata beslutar om krav på informationssäkerhet ska den höra Transport- och kommunikationsverket och i fråga om de tekniska specifikationerna av e-legitimationen Polisstyrelsen. Syftet med hörandet är att säkerställa att de tekniska krav och krav på informationssäkerhet som Myndigheten för digitalisering och befolkningsdata beslutat om motsvarar de krav på informationssäkerhet som används allmänt i bedömningsarbetet, att de har beretts korrekt och att de stämmer överens med de krav, allmänt kända standarder och kriterier för bedömning av informationssäkerheten som föreskrivs för informationssystemet och för det identifieringssystem enligt 6 § som producerats i systemet.

**6 §**. *Krav på identifieringssystemet*. I paragrafen föreskrivs det om kraven på det identifieringssystem som ingår i informationssystemet för digital identitet. Eftersom informationssystemet möjliggör produktion av både e-legitimationen och e-tjänstverktyget för utlänningar, bör kraven

på informationssystemet bedömas separat för dessas del. Enligt *1 mom.* ska identifieringssystemet åtminstone uppfylla kraven för tillitsnivån väsentlig enligt artikel 8.2 b i EU:s förordning om elektronisk identifiering. Att kraven uppfylls är en förutsättning för att identifieringssystemet ska kunna nyttjas för att producera e-legitimation. Närmare krav bestäms i enlighet med kommissionens genomförandeförordning (EU) 2015/1502 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.

I *2 mom.* föreskrivs det om ett undantag från 1 mom. så att identifieringssystemet inte behöver uppfylla registreringskraven enligt tillitsnivån hög eller väsentlig i fråga om e-tjänstverktyg för utlänningar. Med registreringskraven avses de tekniska specifikationerna och förfarandena enligt avsnitt ”2.1. Inskrivning” i förordningen om tillitsnivåer. Undantaget ska dock gälla identifieringssystemets funktion eller administration endast till den del som det är fråga om förfaranden och tekniska lösningar som gäller enbart e-tjänstverktyg för utlänningar.

**7 §.** *Information som ska offentliggöras före ibruktagandet av informationssystemet.* Enligt förslaget till *1 mom.* ska Myndigheten för digitalisering och befolkningsdata innan informationssystemet tas i bruk offentliggöra den information som föreskrivs i momentet. Med ibruktagande av informationssystemet avses när informationssystemet tillhandahålls första gången och det således är möjligt att ta i bruk e-legitimation och e-tjänstverktyg för utlänningar. Myndigheten för digitalisering och befolkningsdata kan enligt det föreslagna momentet själv bestämma hur den offentliggör informationen. Det kan göras till exempel på myndighetens webbplats. Avsikten är att informationen kommer till sådana aktörers kännedom och görs tillgängliga för dem som i sin verksamhet tänker nyttja de tjänster som baserar sig på informationssystemet, dvs. i praktiken e-legitimationen eller e-tjänstverktyget för utlänningar.

Enligt förslaget till 1 mom. *1 punkten* ska datum från och med vilket det är möjligt för en förlitande part att nyttja informationssystemet offentliggöras. Avsikten är att de som ska nyttja informationssystemet ska ha klar vetskap om från och med när informationssystemet kan nyttjas. Exempelvis förtroendenätets tillhandahållare av identifieringstjänster kan på så vis få information om från och med när det är möjligt att nyttja e-legitimation vid inledande identifiering eller förmedla identifieringstransaktioner som gäller dess användare i förtroendenätet.

Enligt förslaget till 1 mom. *2 punkten* ska skyldigheten också gälla informationssystemets egenskaper och en beskrivning av de tekniska gränssnitt och metoder för testning som tillhandahålls. Avsikten är att offentliggörandet av denna information ska göra det möjligt att nyttja informationssystemet och därmed också e-legitimationen och e-tjänstverktyget för utlänningar så enkelt och snabbt som möjligt. Aktörer som nyttjar e-tjänstverktyget för utlänningar och e-legitimation kan vara till exempel tillhandahållare av identifieringstjänster samt andra digitala tjänster i förtroendenätet. När det gäller informationssystemets egenskaper ska tillkännagivandet innehålla uppgifter om de omständigheter som behövs för tjänsten för identifieringsförmedling när e-legitimation nyttjas i förtroendenätet. Tillkännagivandet ska innehålla information om vilka identifieringskoder för en person som fås via e-legitimationen. Identifieringskoderna indelas i obligatoriska och valfria enligt kommissionens genomförandeförordning (EU) 2015/1501 som gäller gränsöverskridande identifiering och som preciserar EU:s eIDAS-förordning. När det gäller tekniska gränssnitt och metoder för testning ska det åtminstone tillkännages enligt vilket protokoll gränssnitt tillhandahålls.

Enligt förslaget till 1 mom. *3 punkten* ska också uppgift om en utförd bedömning av överensstämmelse med kraven tillkännages. Bestämmelser om bedömning av överensstämmelse med

kraven ingår i 10 § i den föreslagna lagen. Enligt den ska informationssystemets överensstämmelse med kraven visas med ett intyg som utfärdas av ett bedömningsorgan för informationssäkerhet. Tillkännagivandet kan alltså innehålla bedömningsorganets intyg som bevis på utförd bedömning av överensstämmelse med kraven. Informationen om bedömning av överensstämmelse med kraven behövs för att de som nyttjar e-legitimation och e-tjänstverktyg för utlänningar ska kunna försäkra sig om att det informationssystem som hänför sig till produktionen av dem uppfyller de krav som ställs på det.

Enligt förslaget till 1 mom. *4 punkten* ska Myndigheten för digitalisering och befolkningsdata tillkännage även eventuella andra villkor som är nödvändiga för verksamheten. Eventuella andra villkor som är nödvändiga för verksamheten kan vara till exempel rättigheter och skyldigheter för andra tillhandahållare av identifieringstjänster än sådana som hör till förtroendenätet, dvs. oregistrerade, och Myndigheten för digitalisering och befolkningsdata samt ansvar mellan förlitande parter, dvs. nyttjare, och deras eventuella tjänsteleverantörer. Bestämmelser om rättigheter och skyldigheter för identifieringstjänster i förtroendenätet vid nyttjande och förmedling av e-legitimation och e-tjänstverktyget för utlänningar finns i autentiseringslagen.

Enligt *2 mom.* ska Myndigheten för digitalisering och befolkningsdata utan dröjsmål offentliggöra ändringar i den information som avses i 1 mom. Ett tillkännagivande ska också göras när verksamheten avslutas.

Ett offentliggörande enligt den föreslagna paragrafen kan anses ha två huvudsakliga syften, som baserar sig på syftet med 10 och 12 b § i den nuvarande autentiseringslagen. Eftersom 10 och 12 b § i autentiseringslagen inte är tillämpliga på tillhandahållaren av informationssystemet för digital identitet, behöver det föreskrivas särskilt om vissa grundläggande krav som denne ska uppfylla och vilkas uppfyllande denne ska tillkännage för dem som tänker använda de tjänster som produceras med hjälp av informationssystemet.

**8 §.** *Autentisering av en förlitande part.* I *1 mom.* bestäms det om kraven på informationssäkerhet i en situation där e-legitimation eller e-tjänstverktyg för utlänningar nyttjas direkt via ett tekniskt gränssnitt. Genom applikationen för digital identitet ska en förlitande part som avses i 26 § autentiseras på ett informationssäkert sätt när en innehavare av applikationen visar sina bestyrkta personuppgifter. Den förlitande parten kan autentiseras med hjälp av ett godkänt certifikat som beviljats den förlitande parten eller på något annat tillförlitligt och informationssäkert sätt. Myndigheten för digitalisering och befolkningsdata ska med hjälp av teknisk implementering säkerställa att det med hjälp av applikationen för digital identitet är möjligt att kontrollera den förlitande partens godkända certifikat eller någon annan av Myndigheten för digitalisering och befolkningsdata bestämd godkänd autentiseringsmekanism.

Enligt *2 mom.* ska Myndigheten för digitalisering och befolkningsdata i ett beslut som avses i 5 § bestämma vilka autentiseringsmekanismer som ska godkännas för en förlitande part, vilket ska utgöra en del av de mer specifika tekniska kraven på informationssystemet för digital identitet samt kraven på informationssäkerhet som avses i 5 §.

Enligt *3 mom.* ska Myndigheten för digitalisering och befolkningsdata upprätthålla en förteckning över godkända identifieringsmekanismer och en förteckning över icke-godkända autentiseringsmekanismer som är tillgängliga för förlitande parter för att göra det möjligt för en förlitande part att använda innehavarens bestyrkta uppgifter och förhindra obehörig användning. Detta kan betyda till exempel en förteckning över godkända certifikatutfärdare och en förteckning över icke-godkända certifikat som beviljats förlitande parter. Vid certifikatbaserad autentisering ska det med hjälp av applikationen för digital identitet vara möjligt att säkerställa att det certifikat som den förlitande parten använder är ett certifikat som utfärdats av en godkänd

certifikatutfärdare och att certifikatet inte finns på någon spärrlista.**9 §.** *Underrättelse om hot och störningar.* I paragrafen föreskrivs det om skyldighet för Myndigheten för digitalisering och befolkningsdata att underrätta om betydande hot och störningar som riktas mot tjänsternas funktion, informationssäkerheten eller användningen av digital identitet. Dessutom ska det redogöras för de åtgärder som olika aktörer har tillgång till för att avvärja hot och störningar samt de beräknade kostnaderna för åtgärderna. I underrättelsen ska det uppges hur länge störningen eller hotet beräknas pågå. Dessutom ska det uppges när hotet eller störningen upphör. Enligt paragrafen ska underrättelsen riktas till förlitande parter, dem som nyttjar e-legitimationer och e-tjänstverktyg för utlänningar samt innehavare av applikationen för digital identitet, om det anses ändamålsenligt. Den föreslagna paragrafen innehåller inga detaljerade krav på hur underrättelsen ska lämnas. Myndigheten för digitalisering och befolkningsdata ska alltså överväga vilket underrättelsesätt som är effektivt i respektive fall. Enligt den föreslagna paragrafen ska underrättelsen lämnas utan obefogat dröjsmål. Den närmare tidpunkten för underrättelsen är alltså beroende av Myndigheten för digitalisering och befolkningsdatas prövning. Med förlitande part avses alla som nyttjar e-legitimation och e-tjänsteverktyget för utlänningar, dvs. underrättelsen ska riktas till organisationer inom såväl den privata sektorn som den offentliga sektorn.

**10 §**. *Bedömning av överensstämmelse med kraven*. I paragrafen föreskrivs det om påvisande och bedömning av informationssystemets överensstämmelse med kraven. Enligt *1 mom.* ska informationssystemets överensstämmelse med kraven visas med ett intyg som utfärdas av ett bedömningsorgan för informationssäkerhet. Med bedömningsorgan för informationssäkerhet avses av Transport- och kommunikationsverkets godkända bedömningsorgan för överensstämmelse med kraven, på vilkas verksamhet tillämpas lagen om bedömningsorgan för informationssäkerhet (1405/2011). Bestämmelserna om påvisande av informationssäkerhetens överensstämmelse med kraven påverkar inte den personuppgiftsansvariges skyldighet enligt den allmänna dataskyddsförordningens att vidta behöriga informationssäkerhetsåtgärder eller den personuppgiftsansvariges ansvar i anslutning härtill. Bedömningen av informationssäkerheten fungerar som en sådan extra skyddsåtgärd som avses i den allmänna dataskyddsförordningen. Myndigheten för digitalisering och befolkningsdata ska ombesörja konsekvensbedömning avseende dataskydd i enlighet med artikel 35 i dataskyddsförordningen och beakta dataskyddsförordningens krav på informationssäkerhet.

I *2 mom.* föreskrivs om förfarandet när bedömningen utförs. Myndigheten för digitalisering och befolkningsdata ska i egenskap av tillhandahållare av informationssystemet göra ansökan om bedömning. Bedömningsorganet för informationssäkerhet bedömer då efter ansökan i enlighet med den föreslagna lagen och lagen om bedömningsorgan för informationssäkerhet om informationssystemet uppfyller de krav som ställs på det. I momentet föreskrivs dessutom att som bedömningsgrunder ska kraven i den föreslagna lagen användas, särskilt kraven i 5 och 6 §, och de krav som ställs av Myndigheten för digitalisering och befolkningsdata i enlighet med 5 § 3 mom.

I *3 mom.* föreskrivs det att bedömningsorganet ska utfärda ett intyg över bedömningen och ge en tillhörande kontrollrapport. Myndigheten för digitalisering och befolkningsdata ska begära ett utlåtande om bedömningen av Transport- och kommunikationsverket, som övervakar bedömningsorganens verksamhet. Syftet med utlåtandet är att säkerställa att bedömningen uppfyller de krav som ställs i lagen om bedömningsorgan för informationssäkerhet. Bedömningen är i regel också förknippad med tolkningsfrågor och utlåtandeinstrumentet gör det möjligt för Transport- och kommunikationsverket att vid behov delta i rådgivningen som gäller tolkningar. Enligt *4 mom.* är bedömningsorganets intyg i kraft högst två år. I praktiken ska Myndigheten för digitalisering och befolkningsdata med stöd av paragrafens 1 och 3 mom. göra informationssystemet till föremål för bedömning av ett bedömningsorgan för informationssäkerhet med

minst två års mellanrum. I momentet föreskrivs det dessutom att bedömningsorganet för informationssäkerhet trots sekretessbestämmelserna av Myndigheten för digitalisering och befolkningsdata kan kräva alla de uppgifter som förutsätts för bedömningen och för upprättandet och upprätthållandet av intyget. På utfärdande av intyget tillämpas i övrigt 9 § 3 mom. i lagen om bedömningsorgan för informationssäkerhet, där det föreskrivs om utfärdande av intyg och om den information som intyget ska innehålla.

**3 kap. Bevis för kärnidentitet**

**11 §.** *Bevis för kärnidentitet.* I paragrafen föreskrivs det om beviset för kärnidentitet och om den information som den ska innehålla. Det föreskrivs om beviset för kärnidentitet i samband med denna lag, eftersom det kan vara ett certifikat eller något annat motsvarande tekniskt bevis, och det är sålunda inte motiverat att placera det bland certifikatbestämmelserna i BDS-lagen med tanke på teknikneutraliteten. Enligt *1 mom.* avses med bevis för kärnidentitet ett av Myndigheten för digitalisering och befolkningsdata producerat bevis med vars hjälp det på ett tillförlitligt sätt kan visas att den som förfogar över bevisat har fått den identitet som kärnidentiteten omfattar registrerad i befolkningsdatasystemet. Beviset för kärnidentitet lämnas alltid till personens eget förfogande i antingen en e-legitimation eller ett e-tjänstverktyg för utlänningar – beviset är inte en självständig tjänst och med stöd av den lagstiftning som nu föreslås är det inte möjligt att utfärda det på någon annan teknisk plattform. Myndigheten för digitalisering och befolkningsdata svarar till denna del för produktion av den tekniska funktionalitet som väsentligt hänför sig till e-legitimationen och e-tjänstverktyg för utlänningar samt för förfarandena i anslutning härtill. Vid produktionen av bevis för kärnidentitet kan Myndigheten för digitalisering och befolkningsdata nyttja de certifikatregistertjänster och spärrlisttjänster som nämns i 61 § 2 mom. 6 punkten i BDS-lagen.

I *2 mom.* föreskrivs det om den information som beviset för kärnidentitet ska innehålla. Ett bevis för kärnidentitet ska enligt 1–6 punkten innehålla personens identifikationskod enligt 11 a § i BDS-lagen (1 punkten), serienummer (2 punkten), det land som utfärdat beviset (3 punkten), bevisets giltighetstid (4 punkten), en öppen nyckel för innehavaren av beviset (5 punkten), samt uppgifter om undertecknaren av beviset (6 punkten). Giltighetstiden för ett bevis för kärnidentitet bestäms i enlighet med de gällande specifikationerna som hänför sig till informationssäkerheten. Kärnidentitetens giltighetstid avgränsas inte exakt i lagen, eftersom de lösningar som hänför sig till informationssäkerheten kan förändras och sålunda också påverka bevisets giltighetstid. Beviset för kärnidentitet kan dock inte vara i kraft om det inte finns sparat på en separat teknisk plattform. Om ett e-tjänstverktyg för utlänningar eller en e-legitimation dras in eller deras giltighet går ut, upphör också giltighetstiden för beviset för kärnidentitet.

I *3 mom.* föreskrivs det om den tillitsnivå enligt artikel 8.2 i eIDAS-förordningen som bevis för kärnidentitet ska uppfylla. Enligt 3 mom. ska ett bevis för kärnidentitet åtminstone uppfylla kraven för tillitsnivån väsentlig enligt artikel 8.2 b i EU:s förordning om elektronisk identifiering. Att kraven uppfylls är en förutsättning för att beviset för kärnidentitet ska kunna nyttjas i e-legitimationer och e-tjänstverktyg för utlänningar. Närmare krav bestäms i enlighet med kommissionens genomförandeförordning (EU) 2015/1502 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.

**12 §.** *Utfärdande av bevis för kärnidentitet.* I paragrafen föreskrivs det om utfärdande av bevis för kärnidentitet, samt om förutsättningarna för utfärdande. Enligt 1 mom. utfärdar Myndigheten för digitalisering och befolkningsdata bevis för kärnidentitet. Beviset utfärdas för en e-legitimation eller ett e-tjänstverktyg för utlänningar, i samband med att de tas i bruk. Beviset

för kärnidentitet överförs till den tekniska plattform som kopplats till det på det sätt som föreskrivs särskilt om ibruktagande av e-tjänstverktyg för utlänningar och e-legitimation.

I *2 mom.* föreskrivs det om förfarandet i anslutning till utfärdande av kärnidentitet. Enligt momentet ska Myndigheten för digitalisering och befolkningsdata ha rätt att, trots sekretessbestämmelserna, för utfärdande av ett bevis för kärnidentitet, få uppgifter om giltigheten för en persons pass eller identitetskort ur det identitetskortsregister som avses i 31 § i lagen om identitetskort eller det passregister som avses i 29 § i passlagen i en situation där beviset ska fogas till en digital identitetshandling.

Enligt *3 mom.* är en förutsättning för registrering av ett bevis för kärnidentitet utöver det som anges i förordningen om tillitsnivåer att personen finns registrerad i befolkningsdatasystemet. En förutsättning för ibruktagande är således att personen bevisligen innehaft den tekniska plattformen vid tidpunkten för utfärdandet av e-legitimationen eller e-tjänstverktyget för utlänningar. När det gäller registrering i befolkningsdatasystemet uppfylls förutsättningarna också genom registrering enligt det förfarande för distansregistrering som avses i 9 a § i BDS-lagen.

**13 §**. *Register i anslutning till bevis för kärnidentitet*. I paragrafen föreskrivs det om register i anslutning till produktion och administration av bevis för kärnidentitet, för vilka Myndigheten för digitalisering och befolkningsdata är personuppgiftsansvarig i enlighet med förslaget till 3 §. Den rättsliga grunden för behandlingen av personuppgifter vid registerföringen är artikel 6.1 c i dataskyddsförordningen. I 1 *mom.* i den föreslagna paragrafen föreskrivs om registret över bevis för kärnidentitet, i vilket den identifikationskod som avses i 11 a § i BDS-lagen samt andra nödvändiga tekniska uppgifter som behövs vid användningen av certifikatet förs in. Andra nödvändiga tekniska uppgifter som behövs vid användningen av certifikatet är åtminstone certifikatets serienummer, det land som utfärdat certifikaten, certifikatens giltighetstider, öppna nycklar för innehavarna av certifikat samt uppgifter om Myndigheten för digitalisering och befolkningsdata som undertecknaren av certifikaten.

I 2 *mom.* föreskrivs det om registret över tekniska plattformar med koppling till personer, dvs. plattformsregistret. I plattformsregistret, som förs av Myndigheten för digitalisering och befolkningsdata, förs det in identifieringsuppgifter som specificerar en person, tekniska uppgifter om de tekniska plattformar, dvs. mobila terminaler, med koppling till personen samt uppgifter om utrustningen, till exempel uppgifter med hjälp av vilka utrustningen kan identifieras. I plattformsregistret kan dessutom föras in andra nödvändiga uppgifter med koppling till personers tekniska plattformar som behövs för att producera kärnidentiteten. Uppgifterna i plattformsregistret skiljer plattformarna jämte innehavare från varandra, också i det fallet att samma person har flera plattformar. Uppgifterna i plattformsregistret behövs dessutom särskilt för att utreda fel och missbruk samt spåra felaktiga funktionskedjor. De tekniska uppgifterna om mobila terminaler kan således anses omfattas av principerna i artikel 5 i dataskyddsförordningen inklusive kravet på att personuppgifterna ska vara relevanta.

## 4 kap. E-tjänstverktyg för utlänningar

**14 §.** *E-tjänstverktyg för utlänningar.* I paragrafen föreskrivs det om Myndigheten för digitalisering och befolkningsdatas uppgift att producera och tillhandahålla e-tjänstverktyg för utlänningar. E-tjänstverktyget för utlänningar är ett verktyg som är avsett att visa uppgifter om identitet och andra bestyrkta uppgifter. E-tjänstverktyget för utlänningar är alltså i princip avsett för sådana utländska medborgare som har behov av att uträtta ärenden elektroniskt i finländska e-tjänster. Med hjälp av verktyget kan andra än finska medborgare styrka i befolkningsdatasystemet registrerade uppgifter om identitet samt visa bestyrkta uppgifter i elektroniska tjänster. E-

tjänstverktyget för utlänningar är ändå inte en med pass eller personkort jämförbar identitetshandling.

**15 §.** *Utfärdande av e-tjänstverktyg för utlänningar.* I paragrafen föreskrivs det om beviljande av e-tjänstverktyg för utlänningar. Enligt *1 mom.* utfärdar Myndigheten för digitalisering och befolkningsdata ett e-tjänstverktyg för utlänningar antingen i samband med att personen personligen besöker myndigheten eller i samband med det förfarande för distansregistrering som avses i 9 a § i BDS-lagen. Myndigheten för digitalisering och befolkningsdata får bevilja ett e-tjänstverktyg för utlänningar till en utländsk medborgare som har fått finsk personbeteckning.

Enligt *2 mom.* ska Myndigheten för digitalisering och befolkningsdata identifiera en person med hjälp av ett resedokument som avses i 9 a § i BDS-lagen när ett e-tjänstverktyg för utlänningar utfärdas för personen i samband med ett personligt besök hos myndigheten. Vid identifiering ansikte mot ansikte kan Myndigheten för digitalisering och befolkningsdata verifiera den sökandes identitet, dvs. göra inledande identifiering ansikte mot ansikte. I samband med identifiering ska man dessutom försäkra sig om att uppgifter om personen har registrerats i befolkningsdatasystemet och om att personen har en personbeteckning. Förutsättningen för att e-tjänstverktyg ska utfärdas är alltså att personen har tilldelats en personbeteckning. Vid identifiering ansikte mot ansikte kan tillitsnivån på e-tjänstverktyget för utlänningar vara högre än för ett verktyg som baserar sig på enbart distansregistrering. Innehavaren av ett verktyg kan också efter förfarandet för distansregistrering besöka myndigheten personligen och identifiera sig där, varvid det är möjligt att höja tillitsnivån på hans eller hennes e-tjänstverktyg.

I *3 mom.* föreslås ett undantag från det som föreskrivs i förvaltningslagen. Om ett e-tjänstverktyg för utlänningar utfärdas, får sökanden inte något separat förvaltningsbeslut eller någon besvärsanvisning. Utfärdande av ett e-tjänstverktyg är i praktiken ett tecken på ett positivt förvaltningsbeslut, och det finns inte något behov av en separat besvärsanvisning eller ett separat beslut med tanke på sökandens rättsskydd. Villkoren för e-tjänstverktygets användning samt andra för sökanden väsentliga omständigheter ska delges i samband med ansökan om verktyget. I fråga om ett negativt beslut ges sökanden dock ett förvaltningsbeslut samt besvärsanvisning i enlighet med förvaltningslagen.

**16 §.** *Uppgifter som ingår i e-tjänstverktyg för utlänningar*. I paragrafen föreskrivs det om datainnehållet i e-tjänstverktyg för utlänningar. Enligt *1 mom.* ska innehavaren av ett e-tjänstverktyg för utlänningar lämnas en kopia av de uppgifter i befolkningsdatasystemet som gäller personen i fråga till hans eller hennes eget förfogande. Med eget förfogande avses att de uppgifter som lämnats till innehavaren av ett e-tjänstverktyg för utlänningar efter utlämnandet är e-tjänstverktygets innehavares egna uppgifter, och myndigheten har ingen möjlighet att bestämma var och för vilka ändamål personen visar sina egna uppgifter. Myndigheten har inte heller åtkomst till de uppgifter som lämnats till personen efter det att de har lämnats till hans eller hennes tekniska plattform, som innehåller e-tjänstverktyget för utlänningar. En verifierad kopia av uppgifterna ska lämnas fysiskt till personens tekniska plattform, och efter utlämnandet ska den inte längre förvaras i myndighetens informationssystem. De ursprungliga registeruppgifterna, utifrån vilka de bestyrkta uppgifter som lämnas till personen upprättas, blir dock kvar i myndighetens register och myndigheten svarar fortfarande för dessa ursprungliga uppgifter. Den verifierade kopian av uppgifterna lagras fysiskt i säkerhetselementen i e-verktygets innehavares tekniska plattform, dvs. mobila terminal, och myndigheten har inte åtkomst till de uppgifter som finns där. Vid behandlingen av de uppgifter som lämnats till dessa personers tekniska plattform tillämpas inte lagstiftningen om skydd för personuppgifter, eftersom den fysiska personen behandlar dem som sina egna personuppgifter i enlighet med artikel 2.2 c i dataskyddsförordningen enbart som ett led i verksamhet av rent privat natur eller som har samband med hans

eller hennes hushåll. På behandlingen av dessa uppgifter tillämpas inte heller informationshanteringslagen, eftersom uppgifterna inte är myndighetshandlingar enligt 5 § 2 mom. i offentlighetslagen då de inte längre innehas av myndigheten. Den personuppgiftsansvarige som lämnar bestyrkta uppgifter till personen själv svarar dock för uppgifternas integritet och tillförlitlighet i enlighet med artikel 5.1 f i dataskyddsförordningen, så att om överlämnandet av uppgifter till personen själv misslyckas eller uppgifterna är felaktiga vilar ansvaret fortfarande på myndigheten.

Ett e-tjänstverktyg för utlänningar ska innehålla de uppgifter om en fysisk person som specificeras i momentet sådana som de ingår i befolkningsdatasystemet. Ett e-tjänstverktyg för utlänningar ska enligt 1–5 punkten innehålla personens förnamn (*1 punkten*), efternamn (*2 punkten*), födelsetid (*3 punkten*), personbeteckning (*4 punkten*), och åldersbevis som grundar sig på födelsetiden (*5 punkten*). I 5 punkten avses med åldersbevis bevis som kan användas när personen styrker sin ålder i tjänsterna. I samband med en kundkontakt visas då till exempel endast information om personen är myndig eller inte, i stället för att visa exakt information om personens ålder. För att ge ut åldersbevis beräknar Myndigheten för digitalisering och befolkningsdata de åldersbevis som förs in i applikationen på basis av födelsetiden samt laddningstidpunkten.

Enligt *2 mom.* ska Myndigheten för digitalisering och befolkningsdata bestyrka de styrkta uppgifter som avses i 1 mom. innan de lämnas till personens eget förfogande i e-tjänstverktyget för utlänningar. Uppgifterna ska bestyrkas på ett sådant sätt att den förlitande parten kan försäkra sig om att uppgifterna är riktiga och aktuella genom att kontrollera giltigheten för certifikatet. Det ska vara möjligt att lita på de bestyrkta uppgifterna i ett e-tjänstverktyg för utlänningar på samma sätt som om uppgifterna skulle lämnas ut ur register hos Myndigheten för digitalisering och befolkningsdata. I paragrafen preciseras det dessutom att Myndigheten för digitalisering och befolkningsdata inte har rätt att behandla de bestyrkta uppgifter som har lämnats till innehavaren av ett e-tjänstverktyg för utlänningar efter det att uppgifterna har lämnats till personen i fråga. Syftet med bestämmelsen är att betona att uppgifterna lämnas till personens eget förfogande. Myndigheten för digitalisering och befolkningsdata har fortfarande rätt att behandla samma uppgifter i sina egna register, men efter att uppgifterna har lämnats har myndigheten inte rätt att behandla de kopior av uppgifterna i fråga som lämnats till personen.

**17 §.** *Nyttjande av e-tjänstverktyg för utlänningar.* I paragrafen bestäms det hur e-tjänstverktyg för utlänningar kan nyttjas. E-tjänstverktygets tillitsnivå kan vara antingen låg eller väsentlig beroende på den inledande identifieringen har gjorts. I *1 mom.* bestäms det om nyttjande av e-tjänstverktyget som ett verktyg med tillitsnivån låg. I momentet sägs att om ett e-tjänstverktyg har utfärdats i samband med det förfarande för distansregistrering som anges i 9 a § i BDS-lagen, får en förlitande part nyttja verktyget i sina elektroniska tjänster i de fall då lagstiftningen inte förutsätter stark autentisering som avses i autentiseringslagen.

Bestämmelser om förfarandet för distansregistrering finns i 9 a § i BDS-lagen och det handlar om samma process som processen för utfärdande av e-tjänstverktyg för utlänningar. I enlighet med 9 a § i BDS-lagen är den viktigaste skillnaden mellan förfarandet för distansregistrering och traditionella registreringsförfaranden att vid distansregistrering identifieras en person inte alls ansikte mot ansikte hos myndigheten. Förfarandet baserar sig i stället på elektronisk avläsning av en handling. Förfarandet förutsätter att den person som begär att bli registrerad har ett resedokument, i vars tekniska del det är möjligt att avläsa hans eller hennes ansiktsbild och andra uppgifter som förutsätts vid registreringen. Det säkerställande av identiteten som ingår i förfarandet uppnår inte samma tillitsnivå som identifiering ansikte mot ansikte. Bestämmelser om de uppgifter som ska insamlas i samband med distansregistrering ingår i 9 b § i BDS-lagen.

När processen för utfärdande av ett e-tjänstverktyg för utlänningar grundar sig på förfarandet för distansregistrering är verktyget vad tillitsnivån beträffar inte lika tillförlitligt som sådan identifiering av en person som grundar sig på ett identifieringsverktyg för stark autentisering. En utländsk medborgare kan nyttja e-tjänstverktyget när han eller hon uträttar ärenden i e-tjänster, men verktygets förlitande part bedömer huruvida denne godkänner nyttjande av ett verktyg som grundar sig på förfarandet för distansregistrering och uppgifter som visas på detta sätt i sin e-tjänst.

I *2 mom.* föreskrivs det om nyttjande av ett e-tjänstverktyg som grundar sig på identifiering ansikte mot ansikte. Om Myndigheten för digitalisering och befolkningsdata har identifierat innehavaren av ett e-tjänstverktyg för utlänningar i enlighet med 17 § i autentiseringslagen, får den förlitande parten nyttja detta verktyg för stark autentisering i enlighet med bestämmelserna i den lagen. Identifiering ansikte mot ansikte gör det i praktiken möjligt att antingen utfärda ett e-tjänstverktyg till en person som inte har något verktyg från förr eller att höja verktygets tillitsnivå från låg till väsentlig. Ett e-tjänstverktyg med nivån väsentlig är i praktiken ett verktyg som kan jämställas med stark autentisering och den kan nyttjas i förtroendenätet på det sätt som föreskrivs om nyttjande av verktyget i autentiseringslagen.

**18 §.** *Visande av bestyrkta uppgifter i anslutning till e-tjänster.* I paragrafen föreskrivs det om användning av e-tjänstverktyg för utlänningar i anslutning till e-tjänster. E-tjänstverktyg för utlänningar gör det möjligt att styrka identiteten och visa bestyrkta uppgifter i samband med identifiering i såväl den offentliga som den privata sektorns e-tjänster. I samband med e-tjänster väljer innehavaren av e-tjänstverktyget själv vilka bestyrkta uppgifter som han eller hon vill visa den förlitande parten, och det är inte fråga om utlämnande av information ur myndighetens register, utan personen visar själv sina personuppgifter elektroniskt och direkt för de aktörer som gör det möjligt att använda e-tjänstverktyget i sina e-tjänster. I praktiken används e-tjänstverktyg för utlänningar i anslutning till e-tjänster på så sätt att Myndigheten för digitalisering och befolkningsdata producerar ett gränssnitt som tillhandahålls förlitande parter och som gör det möjligt att använda det bevis för kärnidentitet och de bestyrkta personuppgifter samt det åldersbevis som ingår i e-tjänstverktyget direkt i tjänster som nyttjar applikationen. Personen styrker själv sin identitet i e-tjänsten och kan i samband med identifieringstransaktionen välja de uppgifter som han eller hon vill visa den förlitande parten. I anslutning till e-tjänster lämnas emellertid alltid till e-tjänsten information om verktygets tillitsnivå, för att e-tjänsten ska kunna bedöma om identifieringen är tillräcklig och tillförlitlig med avseende på den e-tjänst som kräver identifiering.

Utgångspunkten för regleringen är i enlighet med paragrafen innehavarens rätt att själv välja vilka bestyrkta uppgifter som han eller hon vill visa den förlitande parten. Annan lagstiftning kan begränsa denna rätt. En sådan situation förekommer i praktiken till exempel när ett e-tjänstverktyg för utlänningar nyttjas via Suomi.fi-identifikation för att uträtta ärenden i myndighetens elektroniska tjänster. När e-tjänstverktyget nyttjas via Suomi.fi-identifikation kan innehavaren av e-tjänstverktyget visa Suomi.fi-identifikation endast uppgifterna i beviset för kärnidentitet och Suomi.fi-identifikation fungerar i övrigt i enlighet med den gällande lagen och hämtar övriga uppgifter om personen som finns i befolkningsdatasystemet direkt ur befolkningsdatasystemet.

**19 §.** *Registret över e-tjänstverktyg för utlänningar.* I paragrafen föreskrivs det om det register som ska föras över e-tjänstverktyg för utlänningar för vilket Myndigheten för digitalisering och befolkningsdata är personuppgiftsansvarig i enlighet med förslaget till 3 §. Registret ska föras för tillhandahållande och produktion av e-tjänstverktyg för utlänningar. Registret ska innehålla information e-tjänstverktyg för utlänningar, deras innehavare och e-tjänstverktygens giltighet.

Den rättsliga grunden för behandlingen av personuppgifter i anslutning till förande av registret är artikel 6.1 c i dataskyddsförordningen.

**20 §.** *Giltigheten för e-tjänstverktyg för utlänningar.* I paragrafen föreskrivs det om giltigheten för e-tjänstverktyg för utlänningar, som ska vara i kraft högst fem (5) år från utfärdandet. Att en maximal giltighetstid fastställs betyder i praktiken att verktyget ska utfärdas utifrån säkerhetsfaktorer. E-tjänstverktygets giltighetstid kan vara under fem år, om det konstateras vara nödvändigt på grund av säkerhetsskäl.

**21 §.** *Förnyande av e-tjänstverktyg för utlänningar.* I paragrafen bestäms det om förutsättningarna för att förnya e-tjänstverktyg för utlänningar. Myndigheten för digitalisering och befolkningsdata kan förlänga giltighetstiden för ett e-tjänstverktyg för utlänningar på begäran av innehavaren av verktyget. När verktygen förnyas ska kraven i avsnitt 2.2.4 i bilagan till förordningen om tillitsnivåer uppfyllas. I avsnitt 2.2.4 i bilagan ingår olika krav för tillitsnivåerna låg, väsentlig och hög. Ett e-tjänstverktyg ska förnyas i enlighet med kraven i bilagan beroende på verktygets tillitsnivå. Om det är fråga om ett verktyg med tillitsnivån låg, kan det förnyas utifrån bilagans krav på förnyande av verktyg med tillitsnivån låg. Om det är fråga om ett verktyg med tillitsnivån väsentlig eller högre, ska man iaktta det som bestäms i bilagan om höjning av det aktuella verktygets tillitsnivå.

**22 §.** *Indragning av e-tjänstverktyg för utlänningar.* I *1 mom.* föreskrivs det om indragning av e-tjänstverktyg för utlänningar både på begäran av innehavaren av verktyget och på initiativ av Myndigheten för digitalisering och befolkningsdata. I samband med att verktyget dras in ska också det bevis för kärnidentitet som fogats till verktyget dras in.

Enligt *2 mom.* ska Myndigheten för digitalisering och befolkningsdata återkalla e-tjänstverktyget för utlänningar på begäran av dess innehavare. Dessutom föreskrivs det om rätt för Myndigheten för digitalisering och befolkningsdata att dra in e-tjänstverktyget eller förhindra användningen av det, om myndigheten har skäl att misstänka att e-tjänstverktyget används av någon annan än den som det har utfärdats för eller att säkerheten vid användningen av e-tjänstverktyget annars har äventyrats.

Myndigheten för digitalisering och befolkningsdata ska så snart som möjligt underrätta innehavaren om att e-tjänstverktyget har dragits in eller användningen av det förhindrats samt om tidpunkten för och orsakerna till detta. Detta motsvarar bestämmelserna i 26 § 2 mom. i autentiseringslagen, enligt vilka leverantören av identifieringsverktyget så snart som möjligt ska underrätta innehavaren av identifieringsverktyget om att identifieringsverktyget har återkallats eller användningen av det förhindrats samt om tidpunkten för och orsakerna till detta.

**23 §.** *Skötsel av uppgifter som gäller utfärdande och indragning av e-tjänstverktyg för utlänningar inom ramen för samservice.* Med stöd av paragrafen kan också andra myndigheter sköta kundserviceuppgifter som hänför sig till e-tjänstverktyg för utlänningar. I *1 mom.* föreskrivs det om möjlighet att sköta uppgifter i anslutning till ibruktagandet av e-tjänstverktyg för utlänningar med stöd av samservicelagen. Enligt förslaget till 1 mom. får Myndigheten för digitalisering och befolkningsdata överföra biträdande uppgifter som gäller utfärdande och indragning av e-tjänstverktyg för utlänningar och uppdatering av registeruppgifter om sådana verktyg till att skötas inom ramen för samservice. I dessa uppgifter kan ingå ibruktagande av e-tjänstverktyget, anslutning av e-tjänstverktyget till den tekniska plattformen samt indragning av e-tjänstverktyget på innehavarens begäran. Uppgiftshelheten skiljer sig inte avsevärt från de uppgifter som ska skötas i enlighet med samservicelagen och innehåller inga uppgifter med anknytning till utövning av offentlig makt.

På uppgifter som ska skötas inom ramen för samservice tillämpas i övrigt bestämmelserna i samservicelagen. Enligt 8 § i samservicelagen ska ett avtal mellan två eller flera myndigheter om ordnande av samservice ingås skriftligen för viss tid eller tills vidare. I avtalet ska överenskommas om bland annat vilka kundservicefunktioner avtalet gäller och i vilken omfattning de sköts inom ramen för samservice. Dessutom ska det överenskommas om till exempel de praktiska arrangemangen kring skyldigheter vid behandlingen av sekretessbelagda uppgifter och personuppgifter.

När man kommer överens om behandlingen av personuppgifter ska de krav som följer av dataskyddsförordningen naturligtvis beaktas. I artikel 28 i förordningen föreskrivs det bland annat om personuppgiftsansvarigas och personuppgiftsbiträdens skyldigheter. Enligt artikeln ska ett uppdragsförhållande regleras genom ett avtal om behandlingen eller ”en annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt”, om det inte föreskrivs entydigt om användarorganisationens uppgifter genom lag. Trots att den personuppgiftsansvarige i princip ansvarar för behandlingen av personuppgifter och de personuppgiftsbiträden som organisationen anlitar, kan enligt förordningen också personuppgiftsbiträdet bli självständigt ansvarigt för brott mot förordningens bestämmelser.

Enligt förslaget till *3 mom.* ska samservicens uppdragstagare överföra ett ärende till Myndigheten för digitalisering och befolkningsdata för behandling, om uppdragstagaren inte ens efter ytterligare utredning kan aktivera innehavarens identitet eller koppla identiteten till e-tjänstverktyget eller på begäran av innehavaren dra in verktyget. Myndigheten för digitalisering och befolkningsdata ska då överta behandlingen av ärendet och fatta det slutliga beslutet i ärendet.

**5 kap. Nyttjande av tjänster för digital identitet**

**24 §.** *Tjänsten för hantering av digital identitet.* I paragrafen bestäms det att Myndigheten för digitalisering och befolkningsdata ska producera en separat elektronisk tjänst för myndigheternas bruk med hjälp av vilken bevis för kärnidentitet, e-tjänstverktyg för utlänningar och e-legitimation hanteras. Det ska vara möjligt att använda hanteringstjänsten för att aktivera och ta i bruk e-legitimation och e-tjänstverktyg för utlänningar, för att länka dem till en teknisk plattform samt för att dra in verktyg. Hanteringstjänsten ska kunna nyttjas av sådana myndighetsaktörer som har till uppgift att utföra ovannämnda åtgärder. Hanteringstjänsten ska vara en stödtjänst i anslutning till hanteringen av e-legitimation samt e-tjänstverktyg för utlänningar. Personuppgifterna överförs via förvaltningstjänsten men lagras inte i den.

**25 §.** *Avläsargränssnitt och kontrollapplikation.* I *1 mom.* föreskrivs det att Myndigheten för digitalisering och befolkningsdata ska producera och tillhandahålla ett avläsargränssnitt och en kontrollapplikation, som förlitande parter ska använda för att kontrollera e-legitimationen vid uträttandet av ärenden på plats. Med avläsargränssnitt och tillhörande kontrollapplikation avses en sådan teknisk implementering eller lösning, med vars hjälp det är möjligt att läsa uppgifter i en e-legitimation i en annan enhet eller ett annat system. Kontrollapplikationen kan vara till exempel en separat kontrollapplikation, såsom kontrollapplikationen för covidintyg och avläsargränssnittet till exempel ett kontrollgränssnitt som integreras i förlitande parters system.

I *2 mom.* föreskrivs det om möjlighet för någon annan aktör att producera kontrollapplikationen. Myndigheten för digitalisering och befolkningsdata ska dock godkänna en kontrollapplikation som producerats av någon annan aktör innan den kan användas för kontroll av identitet och bestyrkta uppgifter i anslutning till uträttande av ärenden på plats. Myndigheten för digitalisering och befolkningsdatas godkännande behövs för att det ska kunna säkerställas att applikationen är pålitlig och informationssäker. I *3 mom.* förutsätts det att Myndigheten för digitalisering

och befolkningsdata meddelar närmare föreskrifter om de krav som ska ställas på informationssäkerheten hos de kontrollapplikationer som produceras av andra aktörer. Det ska krävas informationssäkerhet på motsvarande nivå som i fråga om Myndigheten för digitalisering och befolkningsdatas eget avläsargränssnitt.

**26 §.** *Förlitande parters anmälningsplikt.* I paragrafen föreslås bestämmelser om förlitande parters anmälningsplikt och om skyldighet för Myndigheten för digitalisering och befolkningsdata att föra ett register över de förlitande parter som gjort anmälan samt om skyldighet att föra och offentliggöra en förteckning över dem. I *1 mom.* bestäms det att en förlitande part ska göra anmälan om den förlitande parten har för avsikt att nyttja e-legitimation eller e-tjänstverktyg för utlänningar med hjälp av ett direkt tekniskt gränssnitt. Det är fråga om ett direkt tekniskt gränssnitt när den förlitande parten själv implementerar det tekniska gränssnittet i sin e-tjänst för nyttjande av e-legitimation eller e-tjänstverktyg för utlänningar, och ingen annan aktör eller tjänst fungerar som förmedlare av de uppgifter som ska visas. Det är inte fråga om ett direkt tekniskt gränssnitt till exempel när den förlitande parten nyttjar e-legitimation eller e-tjänstverktyg genom förmedling av en i 2 § 5 punkten i autentiseringslagen avsedd leverantör av tjänster för identifieringsförmedling eller en i 3 § 1 mom. 4 punkten i lagen om stödtjänster avsedd stödtjänst. Det är dock fråga om ett direkt tekniskt gränssnitt i de fall där förtroendenätets leverantörer av förmedlingstjänster implementerar gränssnitt som behövs för förmedling av uppgifter i e-legitimationer eller e-tjänstverktyg till andra förlitande parter.

Anmälan ska göras innan e-legitimation eller e-tjänstverktyg för utlänningar börjar nyttjas. Anmälan ska också göras om det inträffar förändringar i uppgifterna. Anmälningsplikten innebär inte att det krävs tillstånd att nyttja e-legitimation eller e-tjänstverktyg, utan innebär endast en skyldighet att informera om avsikten att ta i bruk verktygen. Myndigheten för digitalisering och befolkningsdata kan således inte förhindra att e-legitimation eller e-tjänstverktyg nyttjas på den grunden att den anmälan som avses i paragrafen inte har gjorts till myndigheten.

Syftet med anmälningsplikten är att Myndigheten för digitalisering och befolkningsdata som den som tillhandahåller den applikation för digital identitet som gör det möjligt att använda e-legitimation och e-tjänstverktyg ska ha klar vetskap om vilka aktörer som direkt nyttjar e-legitimation eller e-tjänstverktyg. Detta är av betydelse särskilt i situationer där Myndigheten för digitalisering och befolkningsdata i enlighet med förslaget till 9 § är skyldig att underrätta förlitande parter om störningar och avvikande situationer.

I *2 mom.* bestäms det om de uppgifter som åtminstone ska ingå i anmälan. Dessa uppgifter är den förlitande partens namn, den förlitande partens fullständiga kontaktuppgifter samt uppgifter om de tillhandahållna tjänster där e-legitimation eller e-tjänstverktyg för utlänningar kommer att nyttjas. Enligt *3 mom.* ska den förlitande parten utan dröjsmål göra en anmälan om ändringar i de uppgifter som avses i 2 mom. I *4 mom.* sägs att Myndigheten för digitalisering och befolkningsdata är personuppgiftsansvarig för de uppgifter som avses i 2 mom. Dessutom bestäms det om skyldighet för Myndigheten för digitalisering och befolkningsdata att föra och offentliggöra en förteckning över de förlitande parter som har gjort den anmälan som avses i paragrafen. Myndigheten för digitalisering och befolkningsdata kan offentliggöra förteckningen till exempel på sin webbplats. Avsikten är att erbjuda innehavarna av e-legitimation och e-tjänstverktyg information om vilka förlitande parter som gör det möjligt att visa uppgifter med hjälp av e-legitimation eller e-tjänstverktyg i sina tjänster, trots att det inte är fråga om en uttömmande förteckning.

**27 §.** *Skyldigheter för innehavare av applikationen för digital identitet.* I paragrafen föreskrivs det om de skyldigheter för innehavare av applikationen för digital identitet som gäller förvaring och användning av applikationen. Enligt *1 mom.* ska en innehavare av applikationen för digital

identitet förvara applikationen omsorgsfullt. Omsorgsplikten gäller särskilt de specificerande uppgifter med vilkas hjälp det är möjligt att använda applikationen, såsom PIN-koden eller en annan motsvarande kod eller identifikator. När man bedömer vilka försiktighetsåtgärder som rimligen kan förutsättas av innehavaren av applikationen, måste man beakta att applikationen ingår i personens mobila enhet, som innehavaren använder ofta och har med sig. Till rimliga försiktighetsåtgärder hör till exempel att man på det sätt som omständigheterna förutsätter ser till att man har enheten med applikation i behåll. Vad som är omsorgsfulla försiktighetsåtgärder bedöms som en helhet. Omsorgsplikten för innehavaren av applikationen börjar när han eller hon har tagit i bruk applikationen för digital identitet.

I 1 mom. föreskrivs det dessutom om förbud mot att överlåta applikationen för digital identitet för att användas av någon annan. Den digitala identitetshandling eller det e-tjänstverktyg för utlänningar som ingår i applikationen för digital identitet är avsedd endast för att styrka identiteten för den person som är kopplad till identitetshandlingen eller verktyget och för att visa bestyrkta uppgifter som gäller den personen. Enligt de lagstiftningsförslag som ingår i propositionen kan en e-legitimation eller ett e-tjänstverktyg för utlänningar dras in om e-legitimationen eller e-tjänstverktyget används av någon annan än innehavaren.

I *2 mom.* föreskrivs det om skyldighet för innehavaren av applikationen för digital identitet att göra en anmälan, om den tekniska plattformen har förkommit, obehörigen har kommit i någon annans besittning eller obehörigen har använts. I paragrafen avses att en sådana teknisk plattform, dvs. mobil enhet, har förkommit där applikationen för digital identitet har tagits i bruk. Anmälan ska göras utan obefogat dröjsmål till Myndigheten för digitalisering och befolkningsdata efter det att innehavaren av applikationen har upptäckt saken. Innehavarens ansvar för obehörig användning av applikationen upphör efter det att anmälan har gjorts. Huruvida innehavaren av applikationen har gjort anmälan utan obefogat dröjsmål bedöms från fall till fall med beaktande av omständigheterna. Det fastställs ingen bestämd form för anmälan. Myndigheten för digitalisering och befolkningsdata ska se till att det är möjligt att göra anmälan alla dagar på året och vid alla tider på dygnet.

**28 §.** *Begränsningar av ansvaret vid obehörig användning av applikationen för digital identitet.* I paragrafen bestäms om det ansvar som innehavaren av applikationen för digital identitet har i situationer där en annan person använder eller har använt applikationen för digital identitet obehörigen. Paragrafen ska tillämpas till exempel när en mobil terminal där applikationen för digital identitet har tagits i bruk har förkommit eller stulits och den person som hittat eller stulit den lyckas använda den e-legitimation eller det e-tjänstverktyg för utlänningar som ingår i applikationen för digital identitet. I 27 § i autentiseringslagen ingår för närvarande motsvarande bestämmelser om det ansvar som innehavaren av ett identifieringsverktyg har för obehörig användning av identifieringsverktyget. I betaltjänstlagen bestäms på motsvarande sätt om det ansvar som den som använder en betaltjänst har för obehörig användning av betalningsmedlet.

I *1 mom.* bestäms det uttömmande om de situationer där innehavaren av applikationen för digital identitet ansvarar för obehörig användning av den e-legitimation eller det e-tjänstverktyg för utlänningar som ingår i applikationen. Innehavaren av applikationen kan enligt 1 punkten bli ansvarig för sådan obehörig användning som beror på att innehavaren av applikationen har överlåtit applikationen till någon annan. Det är fråga om sådan överlåtelse som avses i bestämmelsen när innehavaren av applikationen medvetet och frivilligt har överlåtit kontrollen över applikationen till någon annan. Bestämmelsen gäller alltså inte till exempel situationer där innehavaren av applikationen tillfälligt lämnar i någon annans förvar en väska som innehåller en mobil terminal med applikationen.

Enligt 2 punkten kan innehavaren av applikationen bli ansvarig för obehörig användning av applikationen, om det beror på hans eller hennes vårdslöshet, som inte är lindrig, att den tekniska plattformen har förkommit, obehörigen kommit i någon annans besittning eller obehörigen har använts. I bestämmelsen avses med teknisk plattform en sådan mobil terminal som innehåller applikationen för digital identitet. Enligt 3 punkten kan innehavaren av applikationen dessutom bli ansvarig för obehörig användning av applikationen om han eller hon har försummat sin skyldighet enligt förslaget till 27 § att utan obefogat dröjsmål efter det att saken har upptäckts göra en anmälan till Myndigheten för digitalisering och befolkningsdata om att den tekniska plattformen har förkommit, obehörigen har kommit i någon annans besittning eller att applikationen obehörigen har använts.

I *2 mom.* bestäms det om situationer där innehavaren av applikationen för digital identitet ändå inte är ansvarig för obehörig användning av applikationen, trots att det är fråga om att någon grund för ansvar som anges i 1 mom. föreligger. Enligt 1punkten är innehavaren av applikationen inte ansvarig för obehörig användning av applikationen till den del applikationen har använts efter det att innehavaren har gjort anmälan enligt förslaget till 27 § till Myndigheten för digitalisering och befolkningsdata. Enligt 2 punkten är innehavaren av applikationen inte heller ansvarig för obehörig användning av applikationen, om han eller hon inte har kunnat göra anmälan enligt 27 § på grund av att Myndigheten för digitalisering och befolkningsdata har försummat sin skyldighet att se till att det är möjligt att när som helst göra anmälan.

**6 kap. Särskilda bestämmelser**

**29 §.** *Sökande av ändring.* I *1 mom.* bestäms det om rätt att begära i förvaltningslagen avsedd omprövning i fråga om sådana beslut av Myndigheten för digitalisering och befolkningsdata som gäller sådant utfärdande av e-tjänstverktyg för utlänningar som avses i 15 § eller sådan indragning av e-tjänstverktyg för utlänningar som avses i 22 § 2 mom. avsett återkallelse av sådana verktyg. Bestämmelsen behövs eftersom det ska föreskrivas separat om i fråga om vilka beslut omprövning får begäras. Enligt 2 mom. finns bestämmelser om sökande av ändring i förvaltningsdomstol i lagen om rättegång i förvaltningsärenden (808/2019).

**30 §.** *Ikraftträdande.* I *1 mom.* föreskrivs det om lagens ikraftträdande. Paragrafens *2 mom.* innehåller en övergångsbestämmelse enligt vilken Myndigheten för digitalisering och befolkningsdata ska meddela de föreskrifter som avses i 25 § 3 mom. i anslutning till kontrollapplikationer som produceras av andra aktörer inom 4 månader efter ikraftträdandet av den föreslagna lagen. I praktiken betyder övergångsbestämmelsen att andra aktörer inte kan producera kontrollapplikationer innan Myndigheten för digitalisering och befolkningsdata har meddelat behövliga föreskrifter. Ikraftträdandet behöver ske stegvis, för att Myndigheten för digitalisering och befolkningsdata ska kunna säkerställa de krav som behövs i anslutning till informationssäkerheten genom myndighetens egen kontrollapplikation.

**7.2 Lag om e-legitimation**

**1 kap. Allmänna bestämmelser**

**1 §**. *Lagens syfte*. Lagens syfte framgår av förslaget till 1 §. Enligt paragrafen innehåller lagen bestämmelser om e-legitimation som utfärdas för finska medborgare och utlänningar som vistas i Finland. I lagen föreskrivs det om bland annat de uppgifter om ska ingå i e-legitimationen, ibruktagande och användning av e-legitimationen samt om dess giltighet. En e-legitimation är en digital handling som är avsedd att styrka identiteten och visa bestyrkta uppgifter i anslutning till den, och som en person kan få tillgång till när han eller hon har ett gällande finskt pass eller personkort.

**2 §**. *Definitioner*. Paragrafen innehåller de väsentliga begrepp som används i lagen och definitioner av dem. Enligt *1 punkten* avses i lagen med bestyrkta uppgifter personuppgifter som verifierats av en myndighet på elektronisk väg. Det är fråga om uppgifter som härrör från informationsresurser eller register som administreras av myndigheten, och vilkas äkthet och oföränderlighet har verifierats tekniskt. Enligt *2 punkten* avses i lagen med förlitande part en fysisk eller juridisk person för vilken innehavaren av en e-legitimation styrker sin identitet eller visar bestyrkta uppgifter och som behöver försäkra sig om att uppgifterna är riktiga. För juridiska personers del handlar det om olika slags elektroniska tjänster eller fysiska serviceställen där man har behov av att identifiera en person eller styrka vissa uppgifter som gäller honom eller henne för tillhandahållandet av tjänsten. Syftet med den förlitande partens behandling av uppgifter är inte av betydelse, utan det väsentliga är att innehavaren av en e-legitimation är tvungen att styrka sin identitet eller visa bestyrkta uppgifter i anslutning till den, och att den förlitande parten i sin tur behöver kunna lita på dessa uppgifter. Enligt *3 punkten* avses i lagen med innehavare av en e-legitimation en person som har tagit i bruk en e-legitimation. Enligt *4 punkten* avses med teknisk plattform en mobil terminal som innehavaren av en e-legitimation förfogar över och i vilken e-legitimationen har tagits i bruk. Enligt 1 mom. *5 punkten* avses med uträttande av ärenden på plats att ärenden uträttas på så sätt att innehavaren av en e-legitimation och den förlitande parten samtidigt är närvarande på samma plats och innehavaren av e-legitimationen visar upp sin i identitetshandlingen bestyrkta identitet eller andra bestyrkta uppgifter som gäller honom eller henne för den förlitande parten. Det är fråga om interaktion ansikte mot ansikte där innehavaren av en e-legitimation har behov av att styrka sin identitet eller visa bestyrkta uppgifter i anslutning till den för en förlitande part. Det har ingen betydelse om handlingen visas för en annan fysisk person i privatlivet eller till exempel för en representant för en näringsidkare eller en myndighet. Med uträttande av ärende på plats avses ändå inte till exempel situationer där en person är fysiskt närvarande i en lokal, men kommunicerar med en automat eller någon annan teknisk terminal. Enligt 1 mom. *6 punkten* avses med bevis för kärnidentitet ett bevis som avses i 11 § i lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata.

**3 §**. *E-legitimation*. I paragrafen finns bestämmelser om e-legitimationen och om dess syfte och funktion. I *1 mom.* föreskrivs det att en e-legitimation är en identitetshandling som är avsedd att styrka identiteten och visa bestyrkta uppgifter i anslutning till e-tjänster och vid uträttande av ärenden på plats. En e-legitimation är alltså i princip en handling som styrker identiteten på samma sätt som identitetskort och pass. Den ska kunna användas och godkännas i syfte att styrka identiteten på samma sätt som identitetskort och pass. Polisen ska ändå inte fatta något separat beslut om utfärdande eller ibruktagande av en e-legitimation. Däremot uppkommer rätt till en e-legitimation med stöd av ett giltigt identitetskort eller pass på det sätt som bestäms i förslagen till 1 a § i lagen om identitetskort och 3 d § i passlagen.

Dessutom bestäms det i 1 mom. att e-legitimation produceras av polisen. Den föreslagna bestämmelsen behövs, eftersom också Myndigheten för digitalisering och befolkningsdata deltar i den tekniska implementeringen av e-legitimationen som en del av implementeringen av informationssystemet för digital identitet. För att säkerställa tydliga roller för polisen och Myndigheten för digitalisering och befolkningsdata behöver det föreskrivas att e-legitimationen är polisens produkt. Bestämmelsen behövs dessutom för att det inte ska uppstå oklarhet beträffande om även någon annan aktör kan producera en sådan e-legitimation som avses i den föreslagna regleringen. Avsikten är att endast polisen ska ha möjlighet att producera en e-legitimation.

I *2 mom.* bestäms det om att e-legitimationen tillhandahålls med hjälp av en sådan applikation för digital identitet som avses i 2 § 6 punkten i lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata. E-legitimationen ska

alltså användas med hjälp av den applikation för digital identitet som Myndigheten för digitalisering och befolkningsdata producerar och en e-legitimation ska vara bunden till den mobila terminal där applikationen har installerats. Det ska alltså inte vara möjligt att ta i bruk en e-legitimation i någon annan applikation än en sådan som avses i momentet.

I *3 mom.* sägs det att med avvikelse från vad som i 34 § i passlagen och i 34 § i lagen om identitetskort föreskrivs om avgifter för pass och identitetskort kan det bestämmas att avgiften för e-legitimation underskrider självkostnadsvärdet. Bestämmelsen gör det möjligt att självkostnadsvärdet för e-legitimationen inte överförs till fullt belopp till priserna på pass och identitetsbevis, vilket är huvudregeln i lagen om grunderna för avgifter till staten. Bestämmelsen behövs för att säkerställa att kundpriserna på pass och identitetskort stiger måttfullt till följd av utvecklingen av e-legitimationen. Eftersom e-legitimationen inte kan separeras från identitetsbeviset eller passet och sålunda inte är en separat prestation från passet eller identitetsbeviset, utan passets eller identitetskortets digitala uttrycksform, skulle det vara oskäligt att ta ut ett separat pris för den. I praktiken ska alltså den myndighet som utfärdar passet eller identitetskortet svara för den avgift som tas ut för e-legitimationen. Till denna del motsvarar bestämmelsen också det som föreskrivs om medborgarcertifikat i 72 § i lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata.

## 2 kap. Uppgifter som ingår i e-legitimationer samt e-legitimationernas giltighetstid

**4 §**. *Uppgifter som ingår i e-legitimationer*. I paragrafen föreskrivs det om uppgifter som ingår i e-legitimationer. Enligt *1 mom.* ska till innehavaren av en e-legitimation lämnas en kopia av de uppgifter i identitetskortsregistret enligt 31 § i lagen om identitetskort (663/2016) eller i passregistret enligt 29 § i passlagen (671/2006) som gäller personen i fråga till hans eller hennes eget förfogande. I momentet specificeras de uppgifterom en fysisk person, sådana som de ingår i identitetskortsregistret eller passregistret, som en e-legitimation ska innehålla. Vilketdera register som används som källregister för uppgifterna i en e-legitimation beror på vilket register som innehåller de nyaste uppgifterna om personen. Identitetshandlingar förfaller inte enligt lag i en situation där personuppgifter ändras. Av denna orsak förekommer det i praktiken situationer där en person har ett giltigt pass och identitetskort, men personuppgifterna i dem skiljer sig från varandra. Det är ändå ändamålsenligt att de nyaste uppgifterna lämnas för e-legitimationen, varvid uppgifterna inte nödvändigtvis är desamma som i den myndighetshandling som använts för att styrka identiteten i samband med ibruktagandet av e-legitimationen. Detta är motiverat eftersom det pass eller identitetskort som visas i samband med ibruktagandet är avsett att möjliggöra identifiering av användaren och är inte avgörande för de uppgifter som visas i e-legitimationen.

Att uppgifterna lämnas till personens eget förfogande, dvs. är självvägd, betyder att de uppgifter som lämnats till innehavaren av e-legitimationen efter utlämnandet är innehavarens egna uppgifter. Detta betyder att myndigheten inte har någon möjligt att bestämma var och för vilka ändamål personens egna uppgifter kan visas. Myndigheten har inte heller åtkomst till de uppgifter som lämnats till personen efter att de har lämnats till hans eller hennes tekniska plattform, som innehåller e-legitimationen. En verifierad kopia av uppgifterna ska lämnas fysiskt till personens tekniska plattform, och efter utlämnandet ska den inte längre förvaras i myndighetens informationssystem. De ursprungliga registeruppgifterna, utifrån vilka de bestyrkta uppgifter som lämnas till personen upprättas, blir dock kvar i myndighetens register och myndigheten svarar fortfarande för dessa ursprungliga uppgifter. Den verifierade kopian av uppgifterna lagras fysiskt i säkerhetselementen i e-legitimationens innehavares tekniska plattform, dvs. mobila terminal, och myndigheten har inte åtkomst till de uppgifter som finns där. Situationen motsvarar till exempel de uppgifter i identitetskortsregistret som kopierats till det fysiska identitetskort som överlämnas till personen, och efter att identitetskortet överlämnats är uppgifterna inte

längre myndighetshandlingar och identitetskortsmyndigheten är inte längre personuppgiftsansvarig för dem. Vid behandlingen av de uppgifter som lämnats till dessa personers tekniska plattform tillämpas inte lagstiftningen om skydd för personuppgifter, eftersom den fysiska personen behandlar dem som sina egna personuppgifter i enlighet med artikel 2.2 c i dataskyddsförordningen enbart som ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll, varvid behandlingen av dessa uppgifter står utanför det materiella tillämpningsområdet för dataskyddslagstiftningen. På behandlingen av dessa uppgifter tillämpas inte heller informationshanteringslagen, eftersom uppgifterna inte är myndighetshandlingar enligt 5 § 2 mom. i offentlighetslagen då de inte längre innehas av myndigheten. Den personuppgiftsansvarige som lämnar bestyrkta uppgifter till personen själv svarar dock för uppgifternas integritet och tillförlitlighet i enlighet med artikel 5.1 f i dataskyddsförordningen, så att om överlämnandet av uppgifter till personen själv misslyckas eller uppgifterna är felaktiga vilar ansvaret fortfarande på myndigheten.

I 1 mom. föreskrivs det dessutom om det detaljerade innehållet i de uppgifter som ska lämnas till innehavaren av en e-legitimation. En e-legitimation ska enligt *1—8 punkten* innehålla personens förnamn (1 punkten), efternamn (2 punkten), födelsetid (3 punkten), uppgift om personens könstillhörighet (4 punkten), uppgift om finskt medborgarskap (5 punkten), personbeteckning eller någon annan identifikationskod på nationell nivå (6 punkten), ansiktsbild som sparats i pass- och identitetskortsregistret (7 punkten), giltighetstid för ett giltigt finskt pass eller identitetskort (8 punkten), och handlingens identifieringskod (9 punkten). När uppgifternas detaljerade innehåll bestäms är det fråga om att nyttja det nationella handlingsutrymmet enligt artikel 6.3 dataskyddsförordningen, för enligt den punkten kan vilken typ av uppgifter som ska behandlas regleras mer ingående i den nationella lagstiftningen.

I *2 mom.* föreskrivs det att polisen ska verifiera de bestyrkta uppgifter som avses i 1 mom. innan de utlämnas ur pass- eller identitetskortsregistret till personens eget förfogande i e-legitimationen. Uppgifterna ska styrkas på ett sådant sätt att den förlitande parten kan försäkra sig om att uppgifterna är riktiga och aktuella genom att kontrollera uppgifternas giltighet. Det ska vara möjligt att lita på bestyrkta uppgifter i en e-legitimation på samma sätt som på uppgifter som är antecknade i ett pass eller identitetskort. I 2 mom. konstateras också uttryckligen att polisen inte längre har rätt att behandla samma bestyrkta uppgifter som har lämnats till innehavaren av en e-legitimation efter det att uppgifterna har lämnats till personen i fråga. Syftet med regleringen är att ytterligare betona att uppgifterna lämnas till personens eget förfogande, och polisen har inte längre rätt att behandla uppgifter som lämnats till personen i fråga.

I *3 mom.* föreskrivs att certifikat som hänför sig till säkerställandet av äktheten och integriteten hos uppgifterna enligt förslaget till 1 mom. utfärdas av Myndigheten för digitalisering och befolkningsdata. I 3 mom. föreskrivs också att Myndigheten för digitalisering och befolkningsdata dessutom lämnar innehavaren av en e-legitimation åldersbevis som grundar sig på födelsetiden. Med åldersbevis avses bevis som kan användas när personen styrker sin ålder i tjänsterna. I samband med en kundkontakt visas då till exempel endast information om personen är myndig eller inte, i stället för att visa exakt information om personens ålder. För att ge ut åldersbevis beräknar Myndigheten för digitalisering och befolkningsdata de åldersbevis som förs in i applikationen på basis av födelsetiden.

I *4 mom.* föreskrivs det att uppgifterna i en e-legitimation uppdateras på innehavarens uttryckliga begäran. I 4 mom. föreskrivs emellertid också att de uppgifter som ingår i en e-legitimation alltid ska vara aktuella och motsvara de uppgifter som finns i polisens identitetskortsregister eller passregister. Om uppgifterna inte är aktuella ska det inte vara möjligt att använda e-legitimationen. Informationssystemet för digital identitet ska med jämna mellanrum kontrollera att uppgifterna är aktuella. Om det upptäcks att de bestyrkta uppgifterna har förändrats till exempel

i och med beviljandet av ett nytt pass eller identitetskort, ska innehavaren av e-legitimationen begära att uppgifterna uppdateras för att det ska vara möjligt att fortsätta använda e-legitimationen. Användningen av en e-legitimation förhindras om uppgifterna inte är aktuella. Det ska vara möjligt att fortsätta att använda e-legitimationen om innehavaren uppdaterar uppgifterna i den.

**5 §.** *Register över e-legitimationer.* I *1 mom.* ingår bestämmelser om polisens uppgift som personuppgiftsansvarig för e-legitimationer. I registret får de uppgifter som avses i 4 § 1 mom. 1–9 punkten föras in till den del det är fråga om en person har rätt att ta i bruk en e-legitimation. I registret förs det dessutom in uppgifter om e-legitimationerna, deras innehavare och giltighet. Registret ska föras för tillhandahållande och produktion av e-legitimation. I registret förs det in uppgifter som de personer som har rätt att ta i bruk en e-legitimation, inte bara om dem som faktiskt har tagit i bruk identitetshandlingen. I praktiken innehåller registret personuppgifter i fråga om de personer som har ett giltigt pass eller identitetskort. Polisen ska vara personuppgiftsansvarig för registret. Den rättsliga grunden för behandlingen av personuppgifter är artikel 6.1 c i dataskyddsförordningen. På polisens behandling av personuppgifter tillämpas på allmänt plan dataskyddsförordningen och därutöver tillämpas på användning, rätt till insyn och utlämnande av de uppgifter som behandlas i registret de bestämmelser som finns i lagen om behandling av personuppgifter i polisens verksamhet (616/2019).

På grundlagsutskottets initiativ utökades passlagen under riksdagsbehandlingen med en bestämmelse (35 § 3 mom.) om individualisering av pass inom Finlands gränser. Enligt grundlagsutskottet är det motiverat att förutsätta att individualiseringen av passet sker i Finland dels med tanke på uppgifternas art, dels för att de skyldigheter som följer av allmänna förvaltningslagar och bestämmelserna om straffrättsligt tjänsteansvar blir tillämpliga på serviceproducenten när denne sköter offentliga förvaltningsuppgifter. Enligt 35 § 3 mom. i passlagen ska serviceproducenten i Finland utföra individualiseringen av passet samt kontrollen av passets kvalitet och av att passets innehåll är korrekt innan passet levereras. På motsvarande sätt ska enligt 22 § 4 mom. i lagen om identitetskort serviceproducenten i Finland utföra individualiseringen av identitetskortet samt kontrollen av kortets kvalitet och av att kortets innehåll är korrekt innan kortet levereras.

I en e-legitimation används uppgifter som har förts in i registret och som specificerar pass och identitetskort. Ibruktagandet av det nya verktyget betyder inte att man ska avvika från bestämmelserna om behandling av uppgifter. Syftet med bestämmelserna är att skydda kritisk information. Behovet av skydd är lika stort oberoende av om specificeringen gäller uppgifterna i en fysisk eller digital identitetshandling. Innehållet i pass- och identitetskortsregistret är en kritisk informationsresurs med avseende på allmän säkerhet och ordning, och därför ska behandlingen av uppgifterna ske inom Finlands gränser. Om det handlar om uppgifter som specificerar pass och identitetskort eller därmed jämförbara uppgifter eller om överföring av sådana uppgifter, ska uppgifterna inte flyttas utanför Finlands gränser.

I *2 mom.* föreslås bestämmelser om förvaringstiden för uppgifterna i registret. Uppgifterna i registret ska raderas senast tio år efter det att en persons rätt till en e-legitimation har upphört. En förvaringstid på tio år är i linje med förvaringstiden enligt lagen om behandling av personuppgifter i polisens verksamhet.

**6 §.** *Ibruktagande av e-legitimationer.* Paragrafen innehåller bestämmelser om ibruktagande av e-legitimationer. I *1 mom.* föreskrivs det om sätten att ta i bruk e-legitimation. En e-legitimation kan för det första tas i bruk hos en behörig passmyndighet eller en behörig myndighet som utfärdar identitetskort. Med behörig myndighet avses utöver polisen de myndigheter som uppräknas i passlagens 6 § om ansökan om pass. En e-legitimation ska dock inte kunna tas i bruk

hos utrikesministeriet. Utan en uttrycklig begränsning skulle vem som helst kunna ta i bruk en e-legitimation hos utrikesministeriet. Utrikesministeriet utfärdar emellertid endast diplomat- och tjänstepass och har förberett sig på att utfärda endast sådana och ordnat sin kundserviceverksamhet utifrån det. Av denna orsak är det nödvändigt att uttryckligen utesluta utrikesministeriet från de myndigheter hos vilka en e-legitimation kan tas i bruk.

Enligt 1 mom. kan en e-legitimation också tas i bruk på elektronisk väg. Då förutsätts stark autentisering som avses i 2 § 1 punkten i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009). Vid ibruktagande på elektronisk väg förutsätts dessutom att uppgifterna i den tekniska delen på personens giltiga pass eller identitetskort fjärravläses med hjälp av en teknisk plattform och jämförs med uppgifterna enligt den starka autentiseringen och att dessa uppgifter motsvarar varandra.

I *2 mom.* sägs att i samband med ibruktagandet av en e-legitimation kopplar polisen det bevis för kärnidentitet som har utfärdats av Myndigheten för digitalisering och befolkningsdata till den fysiska personen.

**7 §.** *Ibruktagande av e-legitimationer för minderåriga.* I paragrafen föreskrivs det om ibruktagande av e-legitimation när den som tar i bruk handlingen är minderårig. I *1 mom.* sägs att för ibruktagande av e-legitimation för minderåriga fordras vårdnadshavarnas samtycke. Med stöd av bestämmelsen ska det således vara möjligt för minderåriga att ta i bruk e-legitimation, men det ska i regel förutsätta samtycke av den minderårigas vårdnadshavare. Den som är minderåriga ska alltså i princip inte kunna ta i bruk en e-legitimation självständigt.

I *2 mom.* föreskrivs det om ett undantag från kravet enligt 1 mom. Enligt momentet ska ibruktagande av en e-legitimation ändå inte förutsätta vårdnadshavarnas samtycke när det är fråga om en minderårig person som har fyllt 15 år. Avsikten är således att göra det möjligt för en minderåriga som har fyllt 15 år att ta i bruk en e-legitimation självständigt utan att det förutsätts samtycke av hans eller hennes vårdnadshavare.

**8 §.** *Giltigheten för e-legitimationer.* I paragrafen föreskrivs det om giltigheten för en e-legitimationer. I *1 mom.* föreslås att en e-legitimation upphör att gälla ett år efter det att den identitetshandling som e-legitimationen grundar sig på har upphört att gälla. I *2 mom.* sägs att med identitetshandling avses den handling som har utfärdats i enlighet med passlagen eller lagen om identitetskort och med stöd av vilken en person har rätt till en e-legitimation.

Syftet med regleringen är att också e-legitimationen alltid ska vara i kraft när en person har ett giltigt pass eller identitetskort, på grund av vilket personen har rätt till en e-legitimation. E-legitimationen behöver alltså inte tas i bruk på nytt varje gång ett nytt identitetskort eller pass som ger rätt till en e-legitimation har utfärdats för personen, utan e-legitimationen fortsätter att gälla utan avbrott. Oavbruten giltighet förutsätter enligt bestämmelsen emellertid att personen skaffar ett nytt pass eller identitetskort som ger rätt till en e-legitimation inom ett år från det att personens alla dylika handlingar har upphört att gälla. En e-legitimation upphör alltså att gälla ett år efter det att personens identitetshandlingar som ger rätt till en e-legitimation har upphört att gälla och förutsatt att personen inte under årets lopp skaffat en ny sådan identitetshandling.

**9 §.** *Indragning av e-legitimationer.* Paragrafen innehåller bestämmelser om situationer då e-legitimationer dras in och om vilken myndighet som har rätt att dra in e-legitimationen i envar situation. I 1 *mom.* föreskrivs det att en e-legitimation dras in om innehavaren begär det. I dessa situationer är det polisen som drar in handlingen. En e-legitimation dras också in om innehavaren av e-legitimationen anmäler att den tekniska plattformen har förkommit eller obehörigen har kommit i någon annans besittning. I dessa situationer kan utöver polisen även Myndigheten

för digitalisering och befolkningsdata dra in e-legitimationen. I dessa situationer behöver Myndigheten för digitalisering och befolkningsdata ha rätt att dra in e-legitimationen, för enligt 27 § i den föreslagna lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata ska innehavaren av applikationen för digital identitet göra en anmälan uttryckligen till Myndigheten för digitalisering och befolkningsdata om den tekniska plattformen har förkommit eller obehörigen har kommit i någon annans besittning, eller om applikationen obehörigen har använts. För att obehörig användning av e-legitimationen ska kunna förhindras så snabbt som möjligt bör Myndigheten för digitalisering och befolkningsdata ha rätt att dra in e-legitimationen genast efter att ha fått anmälan.

I *2 mom.* sägs att en e-legitimation dessutom kan dras in om den innehåller ett uppenbart fel, om den identitetshandling som e-legitimationen grundar sig på dragits in, om e-legitimationen används av någon annan än innehavaren eller om säkerheten vid användningen av e-legitimationen annars har äventyrats. I dessa situationer är det polisen som drar in e-legitimationen.

En e-legitimation dras in genom att det bevis för kärnidentitet som ingår i handlingen dras in. Myndigheten för digitalisering och befolkningsdata är behörig att dra in beviset för kärnidentitet som kopplats till innehavaren av e-legitimationen. Indragning av en e-legitimation ska förhindra dess användning omedelbart efter att indragningen har gjorts.

**3 kap. Användning av e-legitimationer**

**10 §.** *Visande av bestyrkta uppgifter i anslutning till uträttande av ärenden på plats.* Paragrafen innehåller bestämmelser om användning av e-legitimation i anslutning till e-tjänster. E-legitimation gör det möjligt att visa uppgifter som styrker identiteten och andra bestyrkta uppgifter i samband med identifiering i såväl den offentliga som den privata sektorns e-tjänster. Enligt *1 mom.* väljer innehavaren av verktyget själv vilka bestyrkta uppgifter som han eller hon vill visa den förlitande parten i anslutning till e-tjänster, om inte något annat föreskrivs i någon annan lag. Då är det inte fråga om utlämnande av information ur myndighetens register, utan personen själv visar sina personuppgifter elektroniskt och direkt för de aktörer som gör det möjligt att använda e-legitimationen i sina e-tjänster. I praktiken används e-legitimation i anslutning till e-tjänster på så sätt att Myndigheten för digitalisering och befolkningsdata producerar ett gränssnitt som tillhandahålls förlitande parter och som gör det möjligt att använda det bevis för kärnidentitet och de bestyrkta personuppgifter samt det åldersbevis som ingår i e-legitimationen direkt i tjänster som nyttjar applikationen. Personen styrker själv sin identitet i e-tjänsten och kan i samband med identifieringstransaktionen välja de uppgifter som han eller hon vill visa den förlitande parten. I anslutning till e-tjänster lämnas emellertid alltid till e-tjänsten information om att det är fråga om en identitetshandling som polisen utfärdat.

Utgångspunkten för regleringen är i enlighet med paragrafen innehavarens rätt att själv välja vilka bestyrkta uppgifter som han eller hon vill visa den förlitande parten. Annan lagstiftning kan begränsa denna rätt. En sådan situation förekommer i praktiken till exempel när en e-legitimation nyttjas via Suomi.fi-identifikation för att en person vill styrka sin identitet i myndighetens e-tjänster. När identitetshandlingen nyttjas via Suomi.fi-identifikation kan innehavaren visa Suomi.fi-identifikation endast uppgifterna i beviset för kärnidentitet. Likaså förutsätter nyttjande av e-legitimation och styrkande av personuppgifter via förtroendenätet att vissa uppgifter lämnas till förmedlingstjänster. Sådana uppgifter är till exempel den kod som specificerar personen och personens för- och efternamn.

Enligt *2 mom.* lämnas i anslutning till e-tjänster emellertid alltid information om den koppling som polisen gjort till personens kärnidentitet. Med hjälp av denna kan den part som förlitar sig

på e-legitimationen försäkra sig om att e-legitimationen och de bestyrkta uppgifterna i den är tillförlitliga.

**11 §.** *Visande av bestyrkta uppgifter vid uträttande av ärenden på plats.* I paragrafen föreskrivs det om möjlighet att använda e-legitimation för att styrka identiteten och visa bestyrkta uppgifter i e-legitimationen också i anslutning till uträttande av ärenden på plats. I *1 mom.* föreskrivs det om möjligheterna att själv kontrollera vilka uppgifter i e-legitimationen som visas då man uträttar ärenden på plats. Enligt det ska innehavaren av en e-legitimation ha möjlighet att själv välja de bestyrkta uppgifter som han eller hon vill visa den förlitande parten. I anslutning till uträttande av ärenden på plats ska en ansiktsbild emellertid alltid visas. Ansiktsbilden behöver visas, för att den förlitande parten ska kunna försäkra sig om att uppgifterna hör till den person som visar dem genom att jämföra ansiktsbilden med personen.

I *2 mom.* föreskrivs det om rätt för den förlitande parten att vid behov kontrollera giltigheten för beviset för kärnidentitet i det register för bevis för kärnidentitet som avses i 12 § i lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata. Kontrollen sker i praktiken via en kontrollapplikation eller ett avläsargränssnitt i den förlitande partens system. I paragrafen föreskrivs det att giltigheten för beviset för kärnidentitet får kontrolleras vid behov. Giltigheten för beviset för kärnidentitet behöver inte kontrolleras i samtliga fall och därför föreskrivs det inte om obligatorisk kontroll. Giltigheten för beviset för kärnidentitet behöver inte kontrolleras till exempel i en situation där det räcker för kontrollören att säkerställa kopplingen till ansiktsbilden och de utlämnade uppgifterna samt underskriften.

**4. kap. Särskilda bestämmelser**

**12 §.** *Sökande av ändring.* I paragrafen ingår bestämmelser om sökande av ändring. Enligt *1 mom.* får omprövning begäras i fråga om beslut av polisen som gäller sådan indragning av e-legitimation som avses i 9 § 2 mom. I dessa situationer är det fråga om återkallelse på initiativ av polisen. Bestämmelser om omprövningsförfarandet finns i förvaltningslagen (434/2003). Enligt 2 mom. finns bestämmelser om sökande av ändring i förvaltningsdomstol i lagen om rättegång i förvaltningsärenden (808/2019).

### 7.3 Lagen om ändring av lagen om stark autentisering och betrodda elektroniska tjänster

**2 §.** *Definitioner*. I 1 mom. *2 punkten* i den gällande lagen definieras stark autentisering. Definitionen förblir i sak oförändrad, men för tydlighetens skull utökas den med ett omnämnande av verktyg för digital identitet. Definitionen av verktyg för digital identitet fogas till 2 § som ny 13 punkt. Vid tillhandahållande av verktyg för digital identitet är det fråga om en ny typ av tjänst, vars funktionsprinciper avviker från sådan stark autentisering som tillhandahålls för närvarande. Bestämmelsen behövs alltså för att det ska vara klart att också verktyg för digital identitet är en sådan elektronisk metod som avses i definitionen av stark autentisering.

Enligt bestämmelsen är identifiering som grundar sig på ett verktyg för digital identitet stark autentisering när den uppfyller kraven på tillitsnivån väsentlig eller hög enligt artikel 8 i eIDAS-förordningen. Av denna orsak kan de e-tjänstverktyg för utlänningar som avses i 14 § i lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata vara verktyg för digital identitet endast när innehavaren har identifierats på det sätt som avses i 17 § i autentiseringslagen. E-tjänstverktyg för utlänningar kan också utfärdas i samband med förfarande för distansregistrering, men då uppfyller verktyget inte kraven på tillitsnivån väsentlig eller hög i artikel 8 i eIDAS-förordningen. Av denna orsak är identifiering som grundar sig på ett e-tjänstverktyg för utlänningar som har utfärdats i samband med förfarandet för distansregistrering inte sådan stark autentisering som avses i denna lag.

För närvarande förutsätts det på andra ställen i lagstiftningen att stark autentisering används för att få åtkomst till vissa tjänster, till exempel vid ansökan om konsumentkrediter enligt konsumentskyddslagen (38/1978). Avsikten är att det i fortsättningen ska vara möjligt att med hjälp av verktyg för digital identitet identifiera sig i tjänster där lagstiftningen förutsätter stark autentisering.

Till den gällande paragrafens 1 mom. fogas en ny *12 punkt*, där leverantör av tjänster för digital identitet definieras. Med leverantör av digital identitet avses den aktör som producerar sådana tjänster för digital identitet som avses i lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata och som inte är en sådan leverantör av identifieringstjänster som avses i 3 punkten. I praktiken avses med leverantör av tjänster för digital identitet Myndigheten för digitalisering och befolkningsdata. I 4 § i lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata föreskrivs det att Myndigheten för digitalisering och befolkningsdata ska producera ett sådant informationssystem som behövs för att nyttja verktyg för digital identitet. Det är således Myndigheten för digitalisering och befolkningsdatas uppgift att tillhandahålla tjänster för digital identitet. I de tjänster för digital identitet som Myndigheten för digitalisering och befolkningsdata tillhandahåller ingår emellertid också sådana verktyg som inte kan nyttjas vid stark autentisering enligt autentiseringslagen. Autentiseringslagen tillämpas således inte på exempelvis e-tjänstverktyg för utlänningar som avses i 4 kap. i lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata när innehavaren av verktyget har identifierats i samband med de förfarande för distansregistrering som anses i 9 a § i lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata.

Genom definitionen skapas en ny roll i autentiseringslagen. I den gällande lagen definieras leverantör av identifieringsverktyg samt leverantör av tjänster för identifieringsförmedling, som bägge är leverantörer av identifieringstjänster. Leverantören av tjänster för digital identitet skiljer sig från de i lagen avsedda leverantörerna av identifieringstjänster på så vis att i de tjänster som leverantören av tjänster för digital identitet tillhandahåller är det i första hand fråga om digital identitet. Det informationssystem för digital identitet som produceras av Myndigheten för digitalisering och befolkningsdata innehåller emellertid också ett identifieringssystem. De verktyg för digital identitet som leverantören av tjänster för digital identitet producerar kan således också användas för att styrka identiteten.

Leverantören av tjänster för digital identitet blir inte heller en part i det nationella förtroendenätet för stark autentisering, utan tillhandahåller verktyg för digital identitet som ett identifieringsverktyg för förtroendenätets identifieringstjänster med stöd av särskilda bestämmelser. Verksamheten och skyldigheterna för leverantören av tjänster för digital identitet i förtroendenätet skiljer sig således från verksamheten och rollerna för de leverantörer av identifieringstjänster som definieras i den gällande lagen. Av denna orsak är det motiverat att föreskriva separat om rollen för leverantören av tjänster för digital identitet.

Leverantören av tjänster för digital identitet ska begreppsmässigt skilja sig från leverantörer av identifieringstjänster också därför att leverantörer av identifieringstjänster i lagens 10 § har ålagts skyldighet att göra anmälan till Transport- och kommunikationsverket och samtidigt ansluta sig till förtroendenätet. På leverantören av tjänster för digital identitet tillämpas inte heller flera andra sådana bestämmelser i autentiseringslagen som gäller leverantörer av identifieringstjänster. I autentiseringslagen föreskrivs till exempel inte om säkerhetskrav på verktygen, bedömning av överensstämmelse med kraven, skyldighet att lagra uppgifter, tillhandahållande till användare och ansvarsbegränsningar.

Trots att leverantören av tjänster för digital identitet inte har rollen som leverantör av identifieringsverktyg i förtroendenätet, är det ändå för användarens del fråga om liknande verksamhet som den verksamhet som bedrivs av leverantörer av identifieringsverktyg som fungerar i förtroendenätet. För tydlighetens skull konstateras det i definitionen att leverantören av tjänster för digital identitet inte är en leverantör av identifieringstjänster.

Till 1 mom. fogas också en ny *13 punkt*, där verktyg för digital identitet definieras. Med verktyg för digital identitet avses både en i 3 § i lagen om e-legitimation avsedd e-legitimation och ett i 14 § i lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata avsett e-tjänstverktyg för utlänningar. E-tjänstverktyg för utlänningar kan emellertid användas för i autentiseringslagen avsedd stark autentisering endast om innehavaren har identifierats i enlighet med 17 §. E-tjänstverktyg för utlänningar kan också utfärdas i samband med det förfarande för distansregistrering som anges i 9 a § i lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata. Identifiering som grundar sig på förfarandet för distansregistrering är emellertid inte ett lika tillförlitligt sätt att identifiera verktygets innehavare som inledande identifiering som gjorts i enlighet med 17 § i autentiseringslagen. Elektronisk identifiering som grundar sig på ett e-tjänstverktyg för utlänningar som utfärdats i samband med förfarandet för distansregistrering är därför inte sådan stark autentisering som avses i autentiseringslagen och identifieringstransaktioner som grundar sig på den kan inte förmedlas i förtroendenätet.

**7 b §.** *Information om giltighet för pass, identitetskort samt bevis för kärnidentitet i e-legitimation.* Paragrafen utökas med en informativ hänvisning till kontroll av giltigheten för bevis för kärnidentitet i e-legitimationer. På det sätt som beskrivs senare i samband med 17 § och 17 b §, kan leverantörer av identifieringsverktyg nyttja en e-legitimation för inledande identifiering av en person när ett nytt identifieringsverktyg för stark autentisering utfärdats för honom eller henne. Leverantören av identifieringstjänster kan då få information om giltigheten för det bevis för kärnidentitet som ingår den digitala e-legitimation som används vid inledande identifiering antingen via den kontrollapplikation som avses i 25 § i lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata eller ur det register i anslutning till bevis för kärnidentitet som avses i 13 § i den lagen. Myndigheten för digitalisering och befolkningsdatas register i anslutning till bevis för kärnidentitet är offentligt, och där kan man granska giltigheten för ett bevis för kärnidentitet som lagrats i en e-legitimation till exempel via deras e-tjänst. Vid uträttande av ärenden på plats är det möjligt att använda en e-legitimation genom att nyttja antingen ett sådant avläsargränssnitt eller en sådan kontrollapplikation som avses i 25 § i lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata. Om man vid uträttande av ärenden på plats nyttjar till exempel ett avläsargränssnitt som är integrerat i kassasystemet, måste det ses till att en kontrollfunktion integreras i kassasystemet, dvs. att systemet kontrollerar giltigheten för e-legitimationen i registret över bevis för kärnidentitet samtidigt som det avläser uppgifterna i e-legitimationen. Vid uträttande av ärenden på plats kan man emellertid också nyttja den kontrollapplikation som Myndigheten för digitalisering och befolkningsdata gett ut, och som kontrollerar giltigheten för e-legitimationen samtidigt som den visar användaren de uppgifter som avlästs i e-legitimationen.

Dessutom utökas paragrafen med en skyldighet för leverantörer av identifieringsverktyg att säkerställa att det pass eller identitetskort eller den e-legitimation som används vid inledande identifiering är giltigt. I praktiken gäller skyldigheten endast situationer där den inledande identifieringen grundar sig på ett finskt pass, identitetskort eller e-legitimation. Enligt 17 § i autentiseringslagen kan inledande identifiering också grunda sig på officiella identitetshandlingar som beviljats av vissa andra länders myndigheter, men det är inte möjligt att kontrollera dessa handlingars giltighet på elektronisk väg. Skyldigheten att säkerställa giltigheten för den handling

som används vid inledande identifiering gäller endast sådana situationer av inledande identifiering som avses i 17 §, dvs. situationer där identiteten hos den som ansöker om ett identifieringsverktyg för stark autentisering säkerställs i samband med att det nya identifieringsverktyget beviljas. Giltigheten ska i första hand kontrolleras innan identifieringsverktyget beviljas och överlåts till den sökande. Om det ändå inte är möjligt att kontrollera giltigheten i samband med den inledande identifieringen till exempel på grund av en störning i teleförbindelserna eller något annat it-avbrott, kan giltigheten också kontrolleras i efterhand. Leverantören av identifieringsverktyget ska dock säkerställa att identifieringsverktyget inte kan användas innan giltigheten har kontrollerats. Identifieringsverktyget kan sålunda överlåtas till den sökande innan giltigheten har kontrollerats, men då ska verktyget aktiveras för användning först senare.

Möjlighet att kontrollera giltigheten för det pass eller identitetskort som används vid inledande identifiering i polisens informationssystem har funnits ända sedan 2017, men leverantörerna av identifieringsverktyg har nyttjat den endast sällan. Bestämmelserna har således inte förbättrat säkerheten hos beviljandet av identifieringsverktyg, utan det har varit beroende av identifieringstjänstens egen riskbedömning om giltigheten kontrollerats. Kommunikationsutskottet har funnit det viktigt att försöka förhindra missbruk i anslutning till förnyande och beviljande av identifieringsverktyg för stark autentisering med alla till buds stående medel och att eventuella lagstiftningsbehov följs (KoUB 6/2021 rd). Skyldigheten för leverantörer av identifieringsverktyg att säkerställa informationen om giltigheten för en handling via polisens informationssystem, Myndigheten för digitalisering och befolkningsdatas kontrollapplikation eller registret i anslutning till bevis för kärnidentitet kan förbättra säkerheten hos beviljandet av identifieringsverktyg, om giltigheten i fortsättningen alltid kontrolleras. Det tas inte ut någon avgift för att kontrollera passets eller identitetskortets giltighet i polisens informationssystem, men det kan förutsätta att leverantören av identifieringsverktyget inrättar en anslutningsserver till den nationella serviceportalen.

**12 e §.** *Skyldigheter som leverantören av tjänster för digital identitet har i förtroendenätet*. Paragrafen är ny och gäller endast leverantören av tjänster för digital identitet. Enligt förslaget till *1 mom.* ska leverantören av tjänster för digital identitet erbjuda leverantörer av tjänster för identifieringsförmedling tillträdesrätt till det informationssystem för digital identitet som avses i 4 § i lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata, så att leverantörerna kan förmedla de identifieringstransaktioner som grundar sig på verktyg för digital identitet till e-tjänster. För tydlighetens skull konstateras det att paragrafen gäller endast förmedling av identifieringstjänster som grundar sig på verktyg för digital identitet. Informationssystemet för digital identitet nyttjas också för produktion och användning av e-tjänstverktyg för utlänningar som avses i 4 kap. i lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata när den som använder verktyget har identifierats i samband med det förfarande för distansregistrering som anges i 9 a § i lagen om i lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata. E-tjänstverktyg för utlänningar som utfärdats med stöd av förfarandet för distansregistrering hör dock inte till autentiseringslagens tillämpningsområde och de identifieringstransaktioner som grundar sig på dem kan inte förmedlas via förtroendenätet.

Det är fråga om bestämmelser genom vilka leverantören av tjänster för digital identitet åläggs skyldighet att ge tjänster för identifieringsförmedling tillträdesrätt till identifieringstjänsten. Motsvarande skyldighet gäller enligt den gällande lagen leverantörer av identifieringsverketyg som är medlemmar i förtroendenätet. Autentiseringslagen är emellertid tillämplig endast på sådana leverantörer av tjänster för identifieringsförmedling som är medlemmar i förtroendenätet, så paragrafen är inte tillämplig på förmedling av identifieringstransaktioner som grundar sig på

verktyg för digital identitet som tillgängliggörs av andra leverantörer av tjänster för identifieringsförmedling än sådana som hör till förtroendenätet. Verktyg för digital identitet kan emellertid nyttas även utanför förtroendenätet på det sätt som föreskrivs i 7 § i lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata.

Leverantören av tjänster för digital identitet blir alltså inte part i det nationella förtroendenätet för stark autentisering. På det sätt som förklarats i samband med 2 §, handlar verksamheten för leverantören av tjänster för digital identitet om skapandet av digitala identiteter och om verktyg för styrkande av dessa identiteter och som staten beviljar som ett led i produktionen av offentliga tjänster.

Leverantören av tjänster för digital identitet ska tillhandahålla leverantörer av tjänster för identifieringsförmedling avgiftsfritt tillträdesrätt till informationssystemet för digital identitet. Enligt 12 c § i den gällande lagen ska leverantörer av tjänster för identifieringsförmedling betala en ersättning för tillträdesrätt till identifieringstjänsten till leverantörer av identifieringstjänster som är medlemmar i förtroendenätet. Leverantören av tjänster för digital identitet blir emellertid inte part i förtroendenätet, och ersättningsskyldigheten enligt 12 c § är inte tillämplig på nyttjande av tillträdesrätten till informationssystemet för digital identitet.

Syftet med bestämmelserna är att säkerställa att verktygen för digital identitet kan nyttjas i hela samhället, trots att leverantören av tjänster för digital identitet inte är med i förtroendenätet enligt autentiseringslagen. Genom skyldigheten att tillhandahålla tjänsten till leverantörer av tjänster för identifieringsförmedling säkerställs att e-tjänster fortfarande kan skaffa identifiering av kunderna på ett samlat sätt utan att behöva separata tekniska gränssnitt eller ett separat avtal med leverantören av tjänster för digital identitet.

Bestämmelserna tar ändå inte ställning till ansvarsfördelningen mellan leverantören av tjänster för digital identitet och den förlitande part som nyttjar identiteten via förtroendenätets förmedlingstjänst. Förtroendenätets identifieringstjänster och tjänster för identifieringsförmedling svarar för sina identifieringstjänster gentemot användare och förlitande parter i enlighet med autentiseringslagen (t.ex. skyldighet enligt 15 § för leverantörer av identifieringsverktyg att informera den som ansöker om ett identifieringsverktyg och omsorgsplikt enligt 18 § 2 mom. för leverantörer av identifieringstjänster att vidta rättsliga åtgärder i anslutning till hinder och begränsningar).

I förslaget till *1 mom.* ingår en informativ hänvisning till lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata. I 7 § i den lagen föreskrivs om information som ska offentliggöras före ibruktagandet av informationssystemet för digital identitet. Leverantören av tjänster för digital identitet åläggs inte att offentliggöra leveransvillkoren för tillträdesrätt till informationssystemet för digital identitet, men leverantören ska ändå tillhandahålla det i enlighet med den information som leverantören har lämnat på förhand.

Enligt förslaget till *2 mom.* ska leverantören av tjänster för digital identitet själv bestämma vilka tekniska gränssnitt och standarder som ska användas vid tillhandahållandet av informationssystemet för digital identitet. Enligt den gällande lagen är aktörerna i förtroendenätet skyldiga att samarbeta sinsemellan för att samordna teknisk praxis. Detta har ansetts nödvändigt i förtroendenätet, för att olika identifieringstjänster faktiskt ska kunna koppla samman sina tjänster utan att behöva olika tekniska implementeringar med olika identifieringstjänster. Tillhandahållaren av tjänster för digital identitet berörs dock inte av någon motsvarande samarbetsskyldighet. Interoperabiliteten mellan informationssystemet för digital identitet, som produceras för att nyttja

e-legitimation, och förtroendenätets identifieringstjänster främjas genom skyldigheten att i förhand tillhandahålla den information gällande informationssystemet för digital identitet som avses i 7 § 2 mom. i lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata. På basen av denna information kan andra leverantörer av identifieringstjänster bygga upp behövliga tekniska gränssnitt för att nyttja digital identitet.

**16 §.** *Anmälningar av leverantörer av identifieringstjänster om hot och störningar som riktas mot verksamheten eller skyddet av uppgifter*. Till paragrafen fogas ett nytt *3 mom.*, som gäller möjlighet för leverantörer av identifieringstjänster att underrätta också leverantören av tjänster för digital identitet om hot och störningar som riktas mot verksamheten eller skyddet av uppgifter. Trots att leverantören av tjänster för digital identitet inte ingår i förtroendenätet, ska det vara möjligt att nyttja verktyg för digital identitet i förtroendenätet. Leverantören av tjänster för digital identitet behöver således få information om hot och störningar som riktas mot användningen av identiteten. Leverantören av identifieringstjänster ska trots sekretessbestämmelserna utan obefogat dröjsmål lämna den information som avses i 1 mom. också till leverantören av tjänster för digital identitet. Dessutom får leverantören av identifieringstjänster trots sekretessbestämmelserna lämna leverantören av tjänster för digital identitet information som avses i 2 mom. och information som hänför sig till utredning av hot och störningar. Bestämmelser om skyldigheten för leverantören av digital identitet att lämna motsvarande information till leverantören av identifieringstjänster finns i 16 a §. I statsrådets förordning om förtroendenätet för leverantörer av tjänster för stark autentisering (169/2016) föreskrivs det att en leverantör av identifieringstjänster som hör till förtroendenätet svarar för utredningen av störningssituationer i förtroendenätet. Informationsutbyte mellan leverantören av identifieringstjänsten och leverantören av tjänster för digital identitet kan behövas för att utreda hot och störningar.

**16 a §.** *Anmälningar av leverantören av tjänster för digital identitet om hot och störningar som riktas mot verksamheten eller skyddet av uppgifter.* Paragrafen är ny och gäller endast anmälningsskyldighet för leverantören av digital identitet. I *1 mom.* åläggs leverantören av tjänster för digital identitet skyldighet att anmäla betydande hot och störningar som riktas mot informationssäkerheten och dataskyddet i fråga om verktyg för digital identitet eller användningen av en digital identitet och anmäla avbrott i tjänsterna samt lämna information som hänför sig till utredning av hot och störningar. Dessutom ska anmälan göras om de åtgärder som olika aktörer har tillgång till för att avvärja hot och störningar samt om de beräknade kostnaderna för åtgärderna.

Enligt *1 mom.* ska anmälan göras både till de leverantörer av identifieringstjänster som är medlemmar i förtroendenätet och till Transport- och kommunikationsverket. Leverantörerna av identifieringstjänster i förtroendenätet kan nyttja verktyg för digital identitet, varför de behöver känna till hot och störningar som riktas mot användningen av dem samt avbrott i tjänsten.

Trots att Transport- och kommunikationsverket inte övervakar leverantören av tjänster för digital identitet allmänt, behövs ändå anmälan till Transport- och kommunikationsverket, eftersom Transport- och kommunikationsverket övervakar verksamheten i förtroendenätet, där det också är möjligt att nyttja verktyg för digital identitet. Avsikten är att den myndighet som övervakar förtroendenätet ska känna till sådana hot och störningar som avses i bestämmelsen. Transport- och kommunikationsverket kan till exempel vid behov delta i spridningen av informationen, så att sådan information som kan förhindra ytterligare skador ska spridas så snabbt som möjligt.

Den föreslagna paragrafen innehåller inga detaljerade krav på hur informationen ska ges. Leverantören av tjänster för digital identitet ska således överväga vad som är det effektivaste sättet att ge information i respektive situation. Enligt den föreslagna paragrafen ska anmälan göras

utan obefogat dröjsmål. Tidpunkten för informationen är således beroende av prövning som görs av leverantören av tjänster för digital identitet.

I *2 mom.* föreskrivs det hur leverantörer av identifieringstjänster och leverantören av tjänster för digital identitet får behandla uppgifter som de fått med stöd av 1 mom. och 16 § 3 mom. Bestämmelser om grunderna för behandling av information som utbyts mellan leverantörer av identifieringstjänster som är medlemmar i förtroendenätet ingår i 12 a § 5 mom. i autentiseringslagen. Emellertid ska också uppgifter som utbyts mellan leverantörer av identifieringstjänster och leverantören av tjänster för digital identitet behandlas endast för det ändamål för vilket den har lämnats. Dessutom får uppgifterna behandlas endast av den som arbetar hos eller för en leverantör av identifieringstjänster och som nödvändigt behöver uppgifterna i sitt arbete.

**17 §.** *Identifiering av en fysisk person som ansöker om identifieringsverktyg.* Det föreslås att *2 mom.* ändras så att när identifieringen av en person vid inledande identifiering sker endast utifrån en identitetshandling som utfärdats av en myndighet, kan leverantören av identifieringsverktyget verifiera personens identitet också genom en e-legitimation. Enligt 3 § i lagen om e-legitimation är en e-legitimation en identitetshandling som är avsedd för att styrka identiteten. Närmare bestämmelser om nyttjande av e-legitimation vid inledande identifiering finns i 17 b §.

I 4 *mom*. föreskrivs det om så kallade kedjor av inledande identifiering, dvs, skyldighet för en leverantör av identifieringsverktyg att göra det möjligt att använda ett identifieringsverktyg för stark autentisering beviljat av denne för inledande identifiering vid ansökan om ett identifieringsverktyg för stark autentisering på motsvarande eller lägre tillitsnivå. Till momentet fogas för tydlighetens skulle också ett omnämnande av leverantör av tjänster för digital identitet och verktyg för digital identitet. En leverantör av identifieringsverktyg ska således göra det möjligt att använda ett identifieringsverktyg för stark autentisering som denne beviljat för inledande identifiering i samband med ibruktagande av ett verktyg för digital identitet. För tydlighetens skull konstateras att bestämmelser om den ersättning som tas ut för kedjor av inledande identifiering ingår i 17 § 7 mom., som gäller temporärt. Prisbestämmelsen är också tillämplig på situationer där ett identifieringsverktyg för stark autentisering används för ibruktagande av ett verktyg för digital identitet.

**17 b §.** *E-legitimation vid inledande identifiering*. Paragrafen är ny och gäller endast nyttjande av e-legitimation vid inledande identifiering. Enligt den föreslagna paragrafen ska leverantören av tjänster för digital identitet göra det möjligt för leverantörer av identifieringsverktyg att använda e-legitimation för inledande identifiering när de beviljar en sökande ett nytt identifieringsverktyg för stark autentisering. Det är alltså fråga om elektronisk inledande identifiering som grundar sig på en e-legitimation för beviljande av ett nytt identifieringsverktyg för stark autentisering, dvs. en så kallad inledande identifieringskedja.

Med leverantör av identifieringsverktyg avses i enlighet med 10 § i autentiseringslagen tjänsteleverantörer som gjort anmälan. Bestämmelsen gäller endast situationer där det genom e-legitimation skapas ett annat identifieringsverktyg för stark autentisering, dvs. ett identifieringsverktyg som i enlighet med 2 § 1 punkten i autentiseringslagen motsvarar tillitsnivån väsentlig enligt artikel 8.2 b i eIDAS-förordningen eller tillitsnivån hög enligt artikel 8.2 c i den förordningen. Autentiseringslagen är tillämplig endast på leverantörer av identifieringsverktyg som är medlemmar i förtroendenätet, så paragrafen är inte tillämplig på användningen av e-legitimation för att bevilja andra identifieringsverktyg än sådana som hör till förtroendenätet.

Leverantören av tjänster för digital identitet ska göra det möjligt att avgiftsfritt använda e-legitimation för inledande identifiering, dvs. leverantören kan inte ta ut ersättning i enlighet med 17 § 7 mom. i autentiseringslagen av leverantörer av identifieringsverktyg.

Vad som i 7§ i lagen om tjänster för digital identitet föreskrivs om den information som ska offentliggöras innan informationssystemet för digital identitet tas i bruk tillämpas också på användning av e-legitimation vid inledande identifiering. Sålunda specificerar leverantören av tjänster för digital identitet till exempel de tekniska gränssnitt och standarder som används för att nyttja e-legitimation vid inledande identifiering.

**42 a §.** *Transport- och kommunikationsverkets uppgifter*. Det föreslås att 3 *mom*. *2 punkten* ändras så att Transport- och kommunikationsverkets uppgift att anmäla system för elektronisk identifiering till Europeiska kommissionen begränsas till identifieringstjänster som anmälts i enlighet med 10 § i autentiseringslagen. Transport- och kommunikationsverkets uppgift att anmäla system till elektronisk identifiering till Europeiska kommissionen gäller således inte redskap för digital identitet.

### 7.4 Lagen om ändring av 16 och 22 § i lagen om behandling av personuppgifter i polisens verksamhet

**16 §.** *Polisens rätt att få uppgifter ur vissa register och informationssystem.* Det föreslås att *1 mom.* ändras så att det utökas med en ny *16 punkt*, med stöd av vilken polisen har rätt att få uppgifter som är nödvändiga för beviljande av bevis för kärnidentitet och produktion av e-legitimation i enlighet med lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata samt uppgifter för utredning av misstänkt missbruk av personuppgifter, identitetsstölder eller andra motsvarande brott och för förebyggande av sådana brott. Samtidigt görs en teknisk ändring i 1 mom. *15 punkten* så att det inte blir en punkt mellan punkterna. I övrigt görs inga ändringar i paragrafen.

**22 §.** *Övrigt utlämnande av personuppgifter till myndigheter.* Det föreslås att 1 *mom.* ändras så att det utökas med en ny *18 punkt*, med stöd av vilken polisen trots sekretessbestämmelserna genom en teknisk anslutning eller som en datamängd får lämna ut sådana personuppgifter som avses i 5–8, 11 och 12 § för en uppgift som myndigheten har enligt lag till Myndigheten för digitalisering och befolkningsdata för produktion och administration av det informationssystem för digital identitet och de bevis för kärnidentitet som avses i lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata. Samtidigt görs det en teknisk ändring i 1 mom. *17 punkten* så att det inte blir en punkt mellan punkterna. Dessutom har man i den svenska lagen tillagt ”tjänstgöringsuppdrag”. I och med ändringen motsvarar den svenska lagtexten den finska.

### 7.5 Lagen om ändring av lagen om identitetskort

**1 a §.** *E-legitimation.* Paragrafen är ny. Enligt *1 mom.* ger ett identitetskort rätt till en i lagen om e-legitimation avsedd e-legitimation som utfärdas av en myndighet som utfärdar identitetskort. En person har alltså direkt rätt att få en e-legitimation, om ett identitetskort har utfärdats för honom eller henne. Polisen fattar inte något separat beslut om ibruktagande av en e-legitimation. En e-legitimation tas i bruk på det sätt som föreskrivs i den föreslagna lagen om e-legitimation. Enligt *2 mom.* ger ibruktagandet av en e-legitimation inte rätt till ett temporärt identitetskort eller ett identitetskort för minderårig som utfärdats för en person som är under 15 år.

Dessutom föreslås en övergångsbestämmelse för ikraftträdandet av lagen, enligt vilken giltiga identitetskort som har utfärdats före ikraftträdandet av denna lag också ger rätt att ta i bruk en e-legitimation.

### 7.6 Lagen om ändring av passlagen

**3 d §.** *E-legitimation.* Paragrafen är ny. Enligt *1 mom.* ger ett pass rätt till en i lagen om e-legitimation avsedd e-legitimation som utfärdats av en passmyndighet. En person har alltså direkt rätt att få en e-legitimation, om han eller hon har beviljats ett pass. Polisen fattar inte något separat beslut om ibruktagande av en e-legitimation. En e-legitimation tas i bruk på det sätt som föreskrivs i den föreslagna lagen om e-legitimation. Enligt *2 mom.* ger ibruktagandet av en e-legitimation inte rätt till ett tillfälligt pass eller ett nödpass.

Dessutom föreslås en övergångsbestämmelse för ikraftträdandet av lagen, enligt vilken pass som har utfärdats före ikraftträdandet av denna lag också ger rätt att ta i bruk en e-legitimation.

### 7.7 Lagen om ändring av lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata

#### 6 b kap. Identifieringsverktyg för fysiska personer

**69 e §**. *Identifieringsverktyg för fysiska personer*. I paragrafen föreskrivs om ett nytt identifieringsverktyg för fysiska personer. Det är fråga om ett fysiskt identifieringsverktyg som produceras av Myndigheten för digitalisering och befolkningsdata och som i första hand är avsett för personer som inte kan eller vill använda andra verktyg som staten tillhandahåller för åtkomst till den offentliga förvaltningens elektroniska tjänster. Identifieringsverktyg för fysiska personer tillhandahålls som en stödtjänst enligt lagen om förvaltningens gemensamma stödtjänster för e-tjänster och som en identifieringstjänst för organisationer inom den offentliga förvaltningen enligt EU:s förordning om elektronisk identifiering.

Enligt *1 mom.* ska Myndigheten för digitalisering och befolkningsdata bevilja sådana identifieringsverktyg för elektronisk identifiering av fysiska personer som motsvarar tillitsnivån väsentlig enligt artikel 8.2 b i EU:s förordning om elektronisk identifiering eller tillitsnivån hög enligt artikel 8.2 c i den förordningen. Det föreslagna momentet motsvarar till väsentliga delar definition av stark autentisering enligt 2 § 1 punkten i lagen om stark autentisering och betrodda elektroniska tjänster, och syftet med momentet är att ställa samma informationssäkerhetskrav för identifiering på sådana identifieringsverktyg för fysiska personer som produceras av Myndigheten för digitalisering och befolkningsdata som på de identifieringsverktyg för elektronisk identifiering som redan existerar. Identifieringsverktyget ska ändå inte ingå i autentiseringslagen och sålunda är det inte heller ett identifieringsverktyg för stark autentisering. Det är ändå en sådan annan motsvarande informationssäker identifieringstjänst som avses i 6 § 2 mom. i lagen om tillhandahållande av digitala tjänster.

Enligt *2 mom.* överlåter Myndigheten för digitalisering och befolkningsdata identifieringsverktyget för fysiska personer till en person som ett fysiskt verktyg som kan användas utan mobil terminal och chipkort. Momentet lämnar den teknik som används för att förverkliga identifieringsverktyget öppen och är således teknikneutralt skrivet förutom kravet på att verktyget ska ha fysisk form. Syftet med momentet är att på lagnivå föreskriva om ett nytt fysiskt identifieringsverktyg som staten tillhandahåller och som till exempel specialgrupper kan nyttja när de identifierarar sig i den offentliga förvaltningens e-tjänster.

Enligt *3 mom.* tillhandahåller Myndigheten för digitalisering och befolkningsdata identifieringsverktygen för fysiska personer i form av identifieringsverktyg i enlighet med EU:s förordning om elektronisk identifiering, för att användas via den stödtjänst som avses i 3 § 1 mom. 4 punkten i lagen om förvaltningens gemensamma stödtjänster för e-tjänster. Enligt 4 § i lagen om stödtjänster ska Myndigheten för digitalisering och befolkningsdata producera och utveckla de stödtjänster som avses i 3 § 1 mom. 1-7 punkten. I 3 § i lagen om stödtjänster föreskrivs det om stödtjänster och i dess 1 mom. förtecknas de gemensamma stödtjänsterna för e-tjänster. I 3 § 1 mom. 4 punkten föreskrivs det om en sådan tjänst för identifiering av fysiska personer som identifierar en fysisk person som använder den offentliga förvaltningens e-tjänster med hjälp av en tjänst som tillhandahålls av en sådan leverantör av identifieringstjänster som avses i lagen om stark autentisering och betrodda elektroniska tjänster, administrerar identifieringstransaktionen och till användarorganisationen lämnar ut identifieringsuppgifter om en person ur befolkningsdatasystemet.

Enligt 3 mom. i den föreslagna bestämmelsen tillhandahålls således identifieringsverktygen för fysiska personer för användning som en del av den nuvarande Suomi.fi-identifikationen. I 5 § i lagen om stödtjänster föreskrivs det om användning av stödtjänster vid offentliga uppdrag och i dess 1 mom. om skyldighet för statliga förvaltningsmyndigheter, ämbetsverk, inrättningar och affärsverk, kommunala myndigheter, när de sköter sina lagstadgade uppgifter, samt domstolar och andra rättskipningsorgan att använda de stödtjänster som avses i 3 § 1 mom. 1-4, 7 och 8 punkten, om inte myndigheten av tekniska eller funktionella skäl eller av skäl som hänför sig till kostnadseffektiviteten eller informationssäkerheten nödvändigtvis måste använda andra tjänster i sin verksamhet eller i en del av den.

**69 f §**. *Register över identifieringsverktyg för fysiska personer.* I paragrafen föreskrivs det om registret över identifieringsverktyg för fysiska personer. Den rättsliga grunden för behandlingen av personuppgifter i anslutning till förandet av registret är artikel 6.1 c i dataskyddsförordningen. I den föreslagna bestämmelsen föreskrivs det hur de personuppgifter som ska registreras i samband med beviljandet av identifieringsverktyg för fysiska personer ska registreras enligt typ av personuppgift. Regleringen är inte uttömmande, men den är ägnad att ge den registrerade en bild av vilka slags personuppgifter som behandlas, och de uppgifter som ska behandlas bestäms sist och slutligen på grundval av syftet med behandlingen. I vilket fall som helst ska behandlingen av personuppgifter i enlighet med dataskyddsförordningen vara motiverad och förenlig med ändamålet med behandlingen.

Enligt *1 mom.* ska Myndigheten för digitalisering och befolkningsdata för tillhandahållande och produktion av identifieringsverktyg för fysiska personer föra ett register över identifieringsverktygen och över verktygens innehavare. Där föreskrivs det närmare om de uppgifter om identifieringsverktygens innehavare som ska föras in i registret. Uppgifter som ska föras in i registret är de personuppgifter som ingår i den av en myndighet utfärdade identitetshandling som används för kontroll av identiteten samt uppgifter som specificerar identitetshandlingen (1 punkten), de personuppgifter som förmedlas i samband med den elektroniska identifieringsmetod som använts för kontroll av identiteten samt uppgifter om den elektroniska identifieringsmetoden (2 punkten), en identifikationskod som avses in 11 a § i BDS-lagen (3 punkten), en identifieringskod för identifieringsverktyget (4 punkten), kontaktuppgifter för innehavaren av ett identifieringsverktyg för fysiska personer (5 punkten) samt andra än i 1–5 punkten avsedda uppgifter som behövs för tillhandahållande av identifieringsverktyget.

I registret får enligt 1 punkten registreras en fysisk persons personuppgifter, som ingår i den av en myndighet utfärdade identitetshandling som används för kontroll av identiteten samt uppgifter som specificerar identitetshandlingen. Dessa uppgifter registreras endast i och med inledande

identifiering som grundar sig på en handling som utfärdats av en myndighet. Då registreras också en bild av identitetshandlingen eller en bestyrkt avskrift eller kopia av handlingen.

Enligt 2 punkten får i registret registreras de personuppgifter som förmedlas i samband med den elektroniska identifieringsmetod som använts för kontroll av identiteten. Dessa uppgifter är i praktiken sådana uppgifter som förmedlas till Myndigheten för digitalisering och befolkningsdata när den använder en identifieringsmetod som tillhandahålls av någon annan leverantör av identifieringstjänster för inledande identifiering. Dessutom registreras uppgifter om den använda identifieringsmetoden.

I 3–5 punkten föreskrivs det att i registret ska registreras en persons identifikationskod samt en identifieringskod för identifieringsverktyget och behövliga kontaktuppgifter, för att det ska vara möjligt att till exempel informera innehavaren av identifieringsverktyget om att identifieringsverktyget återkallats eller användningen förhindrats.

I 6 punkten föreskrivs det om möjligheten att i registret föra in också andra uppgifter som behövs för tillhandahållande av identifieringsverktyg för fysiska personer. Eftersom det är fråga om en ny tjänst, är det ännu inte i detta skede omöjligt att uttömmande definiera alla uppgifter som ska behandlas. Beroende på till exempel metoden för inledande identifiering av en person kan man för tillhandahållandet av identifieringsverktyget behöva behandla även andra uppgifter än de som avses i 1–6 punkten. Till den del tillhandahållandet av identifieringsverktyget gäller det fysiska verktyget kan det förutsätta att även andra uppgifter behandlas till exempel för att säkerställa informationssäkerheten. Dessutom bör man beakta att när ett identifieringsverktyg tillhandahålls kan det finnas behov av att till exempel komplettera uppgifterna om personen med sådana uppgifter som fås från personen själv och som inte framgår av en av en myndighet utfärdad identitetshandling eller som inte förmedlas från en annan tjänsteleverantörs identifieringstjänst som använts för elektronisk inledande identifiering.

Enligt *2 mom.* finns bestämmelser om behandling av personuppgifter inom tjänsteproduktionen i fråga om identifieringsverktyget för fysiska personer, om krav som gäller identifieringsverktyget och användningen av det och om styrningen av tjänsteproduktionen i 3–5 kap. i lagen om stödtjänster. I 3 kap. i lagen om stödtjänster föreskrivs det om behandling av personuppgifter och andra uppgifter inom tjänsteproduktionen, i lagens 4 kap. om krav som gäller stödtjänsterna och användningen av dem och i lagens 5 kap. om styrning. Eftersom identifieringsverktyget för fysiska personer tillhandahålls i form av en stödtjänst enligt lagen om stödtjänster, är det ändamålsenligt att det föreskrivs i lagen om stödtjänster om databehandling inom tjänsteproduktionen och om krav som gäller tjänsteproduktionen och om styrningen av tjänsteproduktionen.

**69 g §.** *Styrkande av sökandens identitet.* I paragrafen föreskrivs det om förfarandet i anslutning till beviljande av identifieringsverktyg. Enligt *1 mom.* beviljar Myndigheten för digitalisering och befolkningsdata på ansökan ett identifieringsverktyg till en fysisk person. Vid ansökan om identifieringsverktyg är det fråga om ett förvaltningsbeslut, på vilket tillämpas den sedvanliga behandlingsprocessen enligt förvaltningslagen.

I *2 mom.* föreskrivs det om inledande identifiering antingen personligen eller elektroniskt. Myndigheten för digitalisering och befolkningsdata ska identifiera den som ansöker om ett identifieringsverktyg omsorgsfullt innan beslutet om beviljande fattas. Enligt momentet ska identifieringen av en fysisk person göras antingen personligen hos myndigheten eller elektroniskt på ett sådant sätt att de krav uppfylls som gäller för tillitsnivån väsentlig eller hög enligt avsnitt 2.1.2 i bilagan till förordningen om tillitsnivåer för elektronisk identifiering. I det föreslagna momentet hänvisas det till avsnitt 2.1.2 i bilagan till EU:s förordning om tillitsnivåer för elektronisk

identifiering, där det föreskrivs om styrkande och verifiering av en fysisk persons identitet när personen ansöker om ett elektroniskt identitetsverktyg med tillitsnivån väsentlig eller hög.

**69 h §.** *Skötsel av uppgifter som gäller beviljande av identifieringsverktyg inom ramen för samservice*. I paragrafen föreskrivs det om möjligheten att sköta uppgifter som gäller beviljande av identifieringsverktyg med stöd av samservicelagen. Enligt förslaget till 1 mom. kan dessa uppgifter omfatta verifiering av identiteten hos dem som ansöker om identifieringsverktyg och hos innehavare av identifieringsverktyg samt rådgivnings- och stödtjänster i samband med ansökan om identifieringsverktyg. Uppgiftshelheten ingår i de uppgifter som anges i 6 § i samservicelagen och innefattar inga uppgifter med anknytning till utövning av offentlig makt. På en uppgift som utförs inom ramen för samservice tillämpas i övrigt vad som föreskrivs i samservicelagen. Enligt 8 § i samservicelagen ska ett avtal mellan två eller flera myndigheter om ordnande av samservice ingås skriftligen för viss tid eller tills vidare. I avtalet ska överenskommas om bland annat vilka kundservicefunktioner avtalet gäller och i vilken omfattning de sköts inom ramen för samservice. Dessutom ska det överenskommas om till exempel de praktiska arrangemangen kring skyldigheter vid behandlingen av sekretessbelagda uppgifter och personuppgifter.

När man kommer överens om behandlingen av personuppgifter ska de krav som följer av dataskyddsförordningen naturligtvis beaktas. I artikel 28 i förordningen föreskrivs det bland annat om personuppgiftsansvarigas och personuppgiftsbiträdens skyldigheter. Enligt artikeln ska ett uppdragsförhållande regleras genom ett avtal om behandlingen eller ”en annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt”, om det inte föreskrivs entydigt om användarorganisationens uppgifter genom lag. Trots att den personuppgiftsansvarige i princip ansvarar för behandlingen av personuppgifter och de personuppgiftsbiträden som organisationen anlitar, kan enligt förordningen också personuppgiftsbiträdet bli självständigt ansvarigt för brott mot förordningens bestämmelser.

Enligt förslaget till *3 mom.* ska samservicens uppdragstagare överföra ett ärenden till Myndigheten för digitalisering och befolkningsdata för behandling, om uppdragstagaren inte ens efter tilläggsutredningar kan verifiera sökandens identitet. Då ska Myndigheten för digitalisering och befolkningsdata avgöra om identiteten är verifierad och om det är möjligt att bevilja sökanden ett identifieringsverktyg.

**69 i §.** *Information om giltighet för pass och identitetskort.* Enligt den föreslagna paragrafen har Myndigheten för digitalisering och befolkningsdata trots säkerhetsbestämmelserna rätt att via ett tekniskt gränssnitt eller på något annat sätt i elektronisk form få information ur polisens informationssystem om giltighet för pass och identitetskort som används vid inledande identifiering. Syftet med paragrafen är att göra det möjligt att bevilja ett identifieringsverktyg för fysiska personer till en person som har ett giltigt pass eller identitetskort. Myndigheten för digitalisering och befolkningsdata ska ha särskild i lagen föreskriven rätt att få information för att kontrollera dessa uppgifter om giltighet.

**69 j §.** *Skyldighet för Myndigheten för digitalisering och befolkningsdata att lämna uppgifter.* I 1 mom. föreskrivs om de uppgifter som Myndigheten för digitalisering och befolkningsdata ska lämna sökanden innan ett identifieringsverktyg beviljas. Uppgifter ska lämnas om användningen av identifieringsverktyget (*1 punkten*), parternas rättigheter och skyldigheter (*2 punkten*), eventuella ansvarsbegränsningar (*3 punkten*), samt övriga eventuella villkor för användning av identifieringsverktyget (*4 punkten*). Allmänt taget ingår de uppgifter som avses i det föreslagna momentet i Myndigheten för digitalisering och befolkningsdatas villkor för användning av identifieringsverktyget. Lämnandet av uppgifter enligt den föreslagna paragrafen förutsätter emellertid aktiva åtgärder från Myndigheten för digitalisering och befolkningsdata.

Enligt *2 mom.* ska uppgifterna lämnas skriftligen eller elektroniskt så att den som ansöker om ett identifieringsverktyg kan spara och återge dem i oförändrad form.

**69 k §**. *Rätten för Myndigheten för digitalisering och befolkningsdata att återkalla eller förhindra användningen av identifieringsverktyg.* I paragrafen ingår rätt för Myndigheten för digitalisering och befolkningsdata att ingripa i användningen av identifieringsverktyg. Den föreslagna bestämmelsen är motiverad därför att missbruk av någon annans identitet kan ha mycket ödesdigra följder för individen. Myndigheten för digitalisering och befolkningsdatas rätt att återkalla eller förhindra användningen av ett verktyg är begränsad till fem situationer.

Enligt 1 mom. *1 punkten* ska Myndigheten för digitalisering och befolkningsdata ha rätt att återkalla eller förhindra användningen av identifieringsverktyget, om Myndigheten för digitalisering och befolkningsdata har skäl att misstänka att identifieringsverktyget används av någon annan än den som det har beviljats till. En sådan situation kan bero på att innehavaren av identifieringsverktyget har överlåtit verktyget för att användas av någon annan. En sådan situation som avses i punkten kan emellertid också uppstå så att innehavaren av identifieringsverktyget inte själv är medveten om situationen. Enligt *2 punkten* ska det också vara möjligt att återkalla eller förhindra användningen av identifieringsverktyget om Myndigheten för digitalisering och befolkningsdata upptäcker att identifieringsverktyget innehåller ett uppenbart fel. Det är då fråga om Myndigheten för digitalisering och befolkningsdatas eget fel, som inte har upptäckts tidigare. Enligt *3 punkten* får identifieringsverktyg återkallas eller användningen förhindras, om Myndigheten för digitalisering och befolkningsdata har skäl att misstänka att säkerheten vid användningen av identifieringsverktyget har äventyrats. Bestämmelsen omfattar både situationer där äventyrandet av säkerheten gäller bara det aktuella identifieringsverktyget och situationer där användningen av identifieringsverktyget har äventyrats av orsaker som allmänt hänför sig till systemet. Enligt *4 punkten* ska det vara möjligt att återkalla eller förhindra användningen av identifieringsverktyget, om innehavaren av identifieringsverktyget använder det på ett sätt som väsentligt strider mot villkoren för användningen. Man bör dock lägga märke till att överträdelsen ska vara väsentlig för att Myndigheten för digitalisering och befolkningsdata ska kunna utöva sin rätt enligt den föreslagna paragrafen. Enligt *5 punkten* ska det också vara möjligt att återkalla eller förhindra användningen av identifieringsverktyget när innehavaren av identifieringsverktyget har avlidit. Eftersom identifieringsverktyget är personligt, är det på sin plats att Myndigheten för digitalisering och befolkningsdata kan vidta åtgärder för att förhindra att verktyget används i ett sådant fall.

Enligt *2 mom.* ska Myndigheten för digitalisering och befolkningsdata underrätta innehavaren av identifieringsverktyget om att identifieringsverktyget har återkallats eller användning av det förhindrats samt om tidpunkten för och orsakerna till detta. Det är skäl att lämna underrättelsen så snart som möjligt. Bestämmelsen skulle inte innehålla något krav att omedelbart underrätta innehavaren. Orsaken till detta är att ibland kan det vara bättre att först försöka åtgärda till exempel en säkerhetsbrist som Myndigheten för digitalisering och befolkningsdata känner till men som inte är allmänt känd. Tidpunkten för underrättelsen är alltså beroende av Myndigheten för digitalisering och befolkningsdatas prövning. Det står i vilket fall som helst klart att myndigheten är skyldig att sträva efter att minimera eventuella skador.

Enligt *3 mom.* ska Myndigheten för digitalisering och befolkningsdata erbjuda en ny möjlighet att använda identifieringsverktyget eller tillhandahålla innehavaren ett nytt verktyg omedelbart efter det att en sådan orsak som avses i 1 mom. 2 eller 3 punkten inte längre föreligger. När det gäller 1 och 4 punkten ska Myndigheten för digitalisering och befolkningsdata ha frihet att för egen räkning pröva om innehavaren av identifieringsverktyget kan fortsätta att använda verktyget.

**69 l §**. *Skyldigheter för innehavare av identifieringsverktyg för fysiska personer.* I paragrafen föreskrivs om skyldigheter för innehavare av identifieringsverktyg för fysiska personer, vilka är förpliktande för innehavaren av ett identifieringsverktyg i enlighet med de villkor som han eller hon har godkänt. I paragrafen föreskrivs det dessutom om skyldighet för Myndigheten för digitalisering och befolkningsdata att se till att det är möjligt att när som helst göra en anmälan om att identifieringsverktyget har förkommit, obehörigen kommit i någon annans besittning eller obehörigen har använts.

Enligt *1 mom.* ska innehavaren av ett identifieringsverktyg använda verktyget i enlighet med villkoren för användningen. Enligt det föreslagna momentet ska innehavaren också förvara identifieringsverktyget omsorgsfullt. Identifieringsverktyget omfattar också de specificerande uppgifter som behövs för identifieringen, till exempel PIN-koden eller någon annan kod. När man bedömer vilka försiktighetsåtgärder som rimligen kan förutsättas av innehavaren av ett identifieringsverktyg, måste man beakta att identifieringsverktygen i allmänhet är avsedda att användas ofta och man därför måste kunna ha dem med sig. Till de rimliga försiktighetsåtgärder som förutsätts av innehavare av identifieringsverktyg kan man i allmänhet anse att hör till exempel att innehavaren förvarar identifieringsverktyget och de specificerande uppgifter som hänför sig till dess användning på ett sådant sätt att en utomstående inte kan kombinera dem med varandra. Av innehavaren av ett identifieringsverktyg kan ändå inte krävas säkerhetsarrangemang som går orimligt långt. Till exempel att innehavaren förvarar både identifieringsverktyget och koden i sitt hem, betyder inte i sig att han eller hon skulle ha försummat sin omsorgsplikt.

I *2 mom.* föreskrivs det om förbud mot att överlåta identifieringsverktyget för att användas av någon annan. Förbudet mot att överlåta identifieringsverktyget grundar sig på att en väsentlig fråga med tanke på användningen av identifieringsverktyget är uttryckligen att man kan koppla identiteten för en person till ett visst identifieringsverktyg. Av denna orsak är det synnerligen viktigt att identifieringsverktyget inte får överlåtas för att användas av någon annan.

I *3 mom.* föreskrivs det om skyldighet för innehavaren av ett identifieringsverktyg att utan obefogat dröjsmål göra en anmälan till Myndigheten för digitalisering och befolkningsdata, om verktyget obehörigen har kommit i någon annans besittning eller obehörigen har använts. Huruvida innehavaren av identifieringsverktyget har gjort anmälan utan dröjsmål bedöms från fall till fall med beaktande av omständigheterna. I den föreslagna bestämmelsen förskrivs det inte om någon bestämd form för anmälan om ett förkommet identifieringsverktyg.

I *4 mom.* föreskrivs det om skyldighet för Myndigheten för digitalisering och befolkningsdata att se till att det är möjligt att när som helst göra en anmälan enligt 3 mom. Myndigheten för digitalisering och befolkningsdata ska då återkalla identifieringsverktyget eller förhindra användningen av det utan dröjsmål efter det att anmälan har mottagits. Med uttrycket ”när som helst” avses i det föreslagna momentet att innehavaren av identifieringsverktyget ska kunna göra anmälan alla dagar på året och vid alla tider på dygnet. Myndigheten för digitalisering och befolkningsdata kan uppfylla sin skyldighet till exempel genom att ordna telefonjour som är öppen hela tiden. Innehavaren av identifieringsverktyget ska alltid ha faktisk möjlighet att göra anmälan. Innehavaren av identifieringsverktyget ska inte svara för obehörig användning av verktyget efter att anmälan gjorts till Myndigheten för digitalisering och befolkningsdata.

**69 m §.** *Sökande av ändring.* Paragrafen innehåller bestämmelser om beslut i fråga om vilka en person får begära omprövning med stöd av förvaltningslagen. Med stöd av *1 mom.* får omprövning begäras i fråga om sådana beslut av Myndigheten för digitalisering och befolkningsdata som gäller beviljande av i 69 e § avsedda identifieringsverktyg för fysiska personer och 69 k §

avsedd återkallelse av identifieringsverktyg för fysiska personer. Bestämmelser om omprövningsförfarandet finns i förvaltningslagen. Enligt *2 mom.* finns bestämmelser om sökande av ändring i förvaltningsdomstol i lagen om rättegång i förvaltningsärenden (808/2019).

### 7.8 Lagen om ändring av 3 och 9 § i lagen om förvaltningens gemensamma stödtjänster för e-tjänster

**3 §.** Det föreslås att *1 mom. 4 punkten* ändras så att en stödtjänst enligt punkten i fråga kan identifiera en fysisk person som använder den offentliga förvaltningens e-tjänster också med hjälp av en tjänst som avses i 6 b kap. i BDS-lagen. I 6 b kap. i BDS-lagen föreskrivs det om identifieringsverktyg som Myndigheten för digitalisering och befolkningsdata producerar för fysiska personer. Dessutom föreslås det att det felaktiga numret i författningssamlingen på autentiseringslagen rättas.

**9 §.** *Informationskällor som regelbundet utnyttjas inom tjänsteproduktionen.* Det föreslås att paragrafen ändras så att författningsnumret på BDS-lagen stryks. På grund av den föreslagna ändringen av 3 § nämns författningsnumret på BDS-lagen redan en gång, så det behöver inte nämnas på nytt i senare paragrafer.

## 8 Bestämmelser på lägre nivå än lag

I förslaget till lag om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata ges Myndigheten för digitalisering och befolkningsdata nya bemyndiganden att utfärda förordning som gäller informationssäkerhetskrav på tjänster för digital identitet. Det ska vara möjligt att nyttja e-legitimation vid uträttande av ärenden på plats med hjälp av en separat kontrollapplikation. Myndigheten för digitalisering och befolkningsdata producerar en egen kontrollapplikation som kan nyttjas i anslutning till uträttande av ärenden på plats. Dessutom kan andra aktörer producera egna kontrollapplikationer. Myndigheten för digitalisering och befolkningsdata meddelar närmare föreskrifter om de krav som ska ställas på de kontrollapplikationer som produceras av andra aktörer. Det ska krävas informationssäkerhet på motsvarande nivå som i fråga om Myndigheten för digitalisering och befolkningsdatas eget avläsargränssnitt.

Bemyndigandet att meddela föreskrifter ska basera sig på tekniska kravspecifikationer och vara förenligt med kraven på informationssäkerhet. Med stöd av den föreslagna lagen ska Myndigheten för digitalisering och befolkningsdata besluta om närmare tekniska krav på informationssystemet för digital identitet samt om informationssäkerhetskrav. Kraven ska grunda sig på allmänt kända nationella eller internationella standarder. Det är inte ändamålsenligt att föreskriva detaljerat om kraven på informationssäkerhet eftersom standarderna ändras och uppdateras med jämna mellanrum. De närmare tekniska informationssäkerhetskraven på kontrollapplikationen preciseras i och med Myndigheten för digitalisering och befolkningsdatas egen implementering. Det är motiverat att föreskriva om bemyndigande för Myndigheten för digitalisering och befolkningsdata att meddela föreskrifter med beaktande av föreskrifternas tekniska form samt precisering av kraven särskilt genom uppdatering av standarderna och de allmänna informationssäkerhetskraven. Genom bemyndigandet att meddela föreskrifter möjliggörs aktuell överensstämmelse med kraven utan att författningarna behöver ändras. Det är inte ändamålsenligt att på lagnivå reglera detaljerade tekniska lösningar för de tekniska funktioner som ska implementeras, utan strävan med regleringen bör vara en teknikneutral lösning. Bemyndigandet att meddela föreskrifter gör det möjligt för Myndigheten för digitalisering och befolkningsdata att uppdatera kravspecifikationerna med jämna mellanrum.

## 9 Ikraftträdande

Lagarna föreslås träda i kraft den 1 september 2023.

## 10 Verkställighet och uppföljning

Efter ikraftträdandet av de föreslagna lagarna kommer man att följa hur tjänsterna för digital identitet fungerar och används. Nationellt följer man också hur den reform av eIDAS-förordningen som bereds i EU framskrider, man påverkar dess innehåll och utvecklar tjänsterna ytterligare i den riktning som reformen förutsätter. Under de kommande åren kommer detta sannolikt att kräva ändringar även i de lagförslag som ingår i denna proposition.

## 11 Förhållande till andra propositioner

### 11.1 Samband med andra propositioner

Förslagen i propositionen har koppling till regeringens proposition till riksdagen med förslag till lag om ändring av lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata och till lagar som har samband med den, som beretts vid finansministeriet, och det är ändamålsenligt att behandla propositionerna tillsammans. Syftet med den separata propositionen om en reform av personbeteckningen är att reformera personbeteckningssystemet genom att göra det möjligt att bevilja utlänningar personbeteckningar i större utsträckning än för närvarande, genom att möjliggöra elektronisk distansregistrering i befolkningsdatasystemet, genom att utveckla befolkningsdatasystemets identitetshantering samt genom att skapa förutsättningar för införande av en helt ny identifikationskod.

E-legitimation och e-tjänstverktyg för utlänningar grundar sig på en centraliserad av staten garanterad identitet som fås från befolkningsdatasystemet. Eftersom e-tjänstverktyg alltid grundar sig på uppgifter i befolkningsdatasystemet, ska de kunna utfärdas endast för utlänningar vars uppgifter först har registrerats i befolkningsdatasystemet. Den utvidgning av kretsen av utlänningar som registreras i befolkningsdatasystemet och den möjlighet till distansregistrering som föreslås i propositionen om en reform av personbeteckningen har sålunda en fast koppling till genomförandet av detta förslag.

Det bevis för kärnidentitet som ska fogas till e-legitimation och e-tjänstverktyg för utlänningar ska innehålla den nya identifikationskoden som ingår i propositionen om en reform av personbeteckningen. Beviset för kärnidentitet ska vara offentligt och under användningens gång kunna fås från det offentliga certifikatregistret samt från spärrlistan när användningen upphör. Enligt ifrågavarande förslag ska personbeteckningen inte kunna användas som offentlig kod. I propositionen om en reform av personbeteckningen bestäms det om identifikationskoder samt om tilldelande och nyttjande av koderna.

I regeringens proposition till riksdagen med förslag till lag om ändring av lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata och till lagar som har samband med den ingår förslag till bestämmelser som hänvisas till i lagförslag 1 i denna proposition som följer: 11 § 1 punkten, 15 § 1 mom. och 17 § 1 mom.

Vid justitieministeriet bereds som bäst regeringens proposition till riksdagen med förslag till lagstiftning om automatiserat beslutsfattande inom den offentliga förvaltningen. Propositionen innehåller förslag till ny allmän reglering om användningen av automatisering vid behandling

av förvaltningsärenden, särskilt vad gäller beredning och fattande av förvaltningsbeslut. Avsikten är att regleringen ska omfatta behövliga bestämmelser om det tillåtna användningsområdet för automatiserat avgörande av ärenden, kraven på informationssystem, godkännande och övervakning av informationssystem, tillgodoseende av transparens och handlingsoffentlighet samt andra bestämmelser som behövs för att säkerställa god förvaltning, rättssäkerhet och andra grundläggande fri- och rättigheter.

Avsikten är att genomföra det förfarande för distansregistrering som föreslås i propositionen och som gäller utfärdande av e-tjänstverktyg för utlänningar i första hand automatiserat utan tjänstemannabehandling. Vid förfarandet för utfärdande av e-tjänstverktyget är avsikten att iaktta det som kommer att bestämmas i den allmänna reglering om automatiserat beslutsfattande som bereds vid justitieministeriet. De lagförslag som ingår i denna proposition har dock inget egentligt samband med den reglering som föreslås i propositionen i fråga.

### 11.2 Förhållande till budgetpropositionen

Propositionen hänför sig till budgetpropositionen för 2023 och avses bli behandlad i samband med den.

## 12 Förhållande till grundlagen samt lagstiftningsordning

### 12.1 Överföring av uppgifter mellan myndigheter

Enligt propositionen kan vissa uppgifter som hänför sig till Myndigheten för digitalisering och befolkningsdatas registerföring och som anges särskilt i lagen produceras i samarbete mellan myndigheterna som samservice enligt lagens om samservice. Grundlagsutskottet har i flera olika utlåtanden tagit ställning till förslag till bestämmelser om överföring av uppgifter mellan myndigheter. Utskottet har intagit en reserverad hållning till bestämmelser som möjliggör obegränsad överföring av uppgifter till en annan myndighet. Speciellt i samband med bestämmelser som har kopplingar till grundlagen har utskottet krävt att det entydigt eller annars exakt ska framgå av lagstiftningen vem den behöriga myndigheten är, eller att åtminstone principerna för myndigheternas befogenhetsförhållanden och villkoren för att delegera befogenheter ska framgå tillräckligt exakt av lagen (t.ex. GrUU 7/2001 rd, GrUU 21/2001 rd, GrUU 45/2001 rd, GrUU 47/2001 rd, GrUU 52/2001 rd, GrUU 17/2004 rd, GrUU 18/2004 rd, GrUU 24/2006 rd, GrUU 51/2006 rd, GrUU 19/2009 rd och GrUU 21/2009 rd). Dessutom har utskottet i samband med bestämmelser om överföring av uppgifter påpekat att det måste föreskrivas tydligt och i överensstämmelse med lag om personuppgiftsansvariga (t.ex. GrUU 19/2009 rd).

Grundlagsutskottet har intagit en reserverad hållning till bestämmelser som gör det möjligt att överföra befogenheter som innebär utövning av offentlig makt med stöd av avtal. I grundlagsutskottets utlåtande (GrUU 11/2004 rd) konstateras att det inte är oproblematiskt att genom avtal föra över en förvaltningsuppgift som anförtrotts en myndighet till en annan myndighet. Bestämmelser som är beaktansvärda med tanke på saken är grundlagens 21 § om att var och en har rätt att få sin sak behandlad av en domstol som är behörig enligt lag. Betydelsefullt är också 2 § 3 mom. i grundlagen. Där sägs att all utövning av offentlig makt skall bygga på lag och att lag noggrant ska iakttas i all offentlig verksamhet (GrUU 14/2003 rd, GrUU 52/2001 rd, GrUU 11/2002 rd och GrUU 72/2002 rd).

Enligt propositionen ska de registreringsuppgifter som ska skötas i form av samservice anges i lagen. Det handlar om registrerings- och rådgivningsuppgifter enligt lagen om samservice som hänför sig till registreringen av personuppgifter som gäller innehavare av e-tjänstverktyg för utlänningar och identifieringsverktyg för fysiska personer. Dessa uppgifter avviker inte avsevärt

från de uppgifter som det gjorts möjligt att överföra i lagen om samservice. Uppdragstagare enligt lagen om samservice ska sköta de registreringsuppgifter som anges särskilt i lagen i enlighet med de förutsättningar som föreskrivs i lagen och vad som överenskommits närmare i samserviceavtalet samt Myndigheten för digitalisering och befolkningsdatas anvisningar.

Uppdragstagarens serviceråd givare ska sköta till exempel uppgifter i anslutning till aktivering av e-tjänstverktyg för utlänningar och identifieringsverktyg för fysiska personer. Det är fråga om förvaltningsuppgifter som hör till myndigheterna, men till sin karaktär är de bistående av Myndigheten för digitalisering och befolkningsdata, som är uppdragsgivare. Myndigheten för digitalisering och befolkningsdata ska som uppdragsgivare dessutom ge uppdragstagarens anställda sådana anvisningar och sådan utbildning som uppgiften förutsätter. Uppgifterna innebär inte utövning av offentlig makt, eftersom Myndigheten för digitalisering och befolkningsdata förblir personuppgiftsansvarig och behåller ansvaret för beslutanderätten i anslutning till registreringen i situationer där ett beslut ska meddelas en kund hos förvaltningen. Om uppdragstagaren inom samservicen till exempel på grund av avsaknad av utredningar och inte ens efter tilläggsutredningar kan aktivera ett e-tjänstverktyg för utlänningar eller ett identifieringsverktyg för fysiska personer, ska uppdragstagaren överföra ärendet till Myndigheten för digitalisering och befolkningsdata för behandling. Myndigheten för digitalisering och befolkningsdata ska vid behov meddela ett beslut om vägran att registrera eller bevilja ett identifieringsverktyg.

Det är ändamålsenligt att det görs möjligt att sköta de föreslagna bistående uppgifterna inom ramen för samservice. Identifiering av den som ansöker om ett e-tjänstverktyg för utlänningar eller ett identifieringsverktyg för fysiska personer med stöd av lagen och ett samserviceavtal även hos andra myndigheter gör det möjligt för en större användarkrets än nu att nyttja tjänster som tillhandahålls i en elektronisk miljö samt gör det smidigare för utländska medborgare att ta i bruk e-tjänster i samband med myndighetsprocesser.

### 12.2 Skydd för privatlivet och skydd för personuppgifter

*Inledning och nationellt handlingsutrymme*

Propositionen innehåller speciallagstiftning om behandling av personuppgifter. Lagförslagen måste sålunda bedömas med avseende på skyddet för privatlivet i 10 § i grundlagen. Enligt 10 § i grundlagen har var och en rätt till skydd för privatlivet. Enligt 1 mom. är vars och ens privatliv, heder och hemfrid tryggade. Dessutom utfärdas närmare bestämmelser om skydd för personuppgifter genom lag. Grundlagsutskottets vedertagna praxis har varit att lagstiftarens handlingsutrymme begränsas både av den här bestämmelsen och av att skyddet för personuppgifter delvis omfattas också av skyddet för privatlivet, som tas upp i samma moment. På det hela taget handlar det om att lagstiftaren bör tillgodose denna rätt på ett sätt som är godtagbart med avseende på de grundläggande fri- och rättigheterna överlag (se t.ex. GrUU 42/2016 rd, s. 2 och GrUU 12/2016, s. 3).

De föreslagna bestämmelserna är också av betydelse med tanke på EU:s stadga om de grundläggande rättigheterna. I artikel 7 i EU:s stadga om de grundläggande rättigheterna tryggas respekten för privatlivet och i artikel 8 vars och ens rätt till skydd av de personuppgifter som rör honom eller henne. Enligt artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna har envar rätt att åtnjuta respekt för sitt privat- och familjeliv. I Europadomstolens rättspraxis har artikeln ansetts omfatta även skyddet av personuppgifter (GrUU 28/2016 rd, s. 5).

Grundlagsutskottet har reviderat sin ståndpunkt när det gäller kravet på lagbestämmelser om skydd för personuppgifter inom den allmänna dataskyddsförordningens tillämpningsområde. Dataskyddsförordningen föreskriver väsentligt mycket mer detaljerat om skyddet för personuppgifter än dataskyddsdirektivet (95/46/EG) och personuppgiftslagen, som stiftats för att genomföra direktivet. Utskottet har också ansett att det är av relevans att artikel 7 i Europeiska unionens stadga om de grundläggande rättigheterna garanterar skyddet för privatlivet och att artikel 8 tillförsäkrar var och en rätt till skydd av personuppgifter. Utskottet har framhållit att man vid tillämpningen av EU-lagstiftningen om behandling av personuppgifter måste ta hänsyn till de här artiklarna i stadgan och att EU-domstolens domar på dessa punkter är utslagsgivande för det viktigaste innehållet i respekten för privatlivet och skyddet för personuppgifter (GrUU 14/2018, s. 3).

Om man ser till skyddet för personuppgifter har grundlagsutskottet ansett det viktigt att reglera åtminstone syftet med registrering av sådana uppgifter. Dessutom har grundlagsutskottet ansett det viktigt att reglera åtminstone innehållet i uppgifterna, det tillåtna användningsändamålet inklusive rätten att överlåta registrerade uppgifter, den tid uppgifterna finns kvar i registret och den registrerades rättssäkerhet (se t.ex. GrUU 42/2016 rd, s. 2 och GrUU 12/2016, s. 3). Kravet på bestämmelser i lag omfattar också möjligheten att lämna uppgifter med hjälp av en teknisk anslutning. Möjligheten att sammanställa uppgifter kräver också bestämmelser i lag (GrUU 17/2007 rd, s. 3 och GrUU 30/2005 rd, s. 4). Dessutom ska regleringen på lagnivå av behandlingen av personuppgifter vara heltäckande och detaljerad (se t.ex. GrUU 46/2016 rd, s. 5–6 och de utlåtanden som det hänvisas till där).

Grundlagsutskottet har påpekat att bestämmelserna om behandling av personuppgifter är tungrodda och komplicerade (se t.ex. GrUU 2/2018 rd, s. 4–8, 11, GrUU 49/2017 rd, s. 3, GrUU 31/2017 rd, s. 4 och GrUU 71/2014 rd, s. 3). Utskottet har ansett att tillgodoseendet av skyddet för personuppgifter inte längre kan utgå från den nuvarande regleringsmodellen. I stället bör tillgodoseendet av skyddet för personuppgifter enligt utskottet i framtiden i första hand grunda sig på den allmänna dataskyddsförordningen och den nationella allmänna lag som ska stiftas. I det sammanhanget bör man undvika nationell speciallagstiftning, som bör reserveras för situationer då den är dels tillåten enligt dataskyddsförordningen, dels nödvändig för att tillgodose skyddet för personuppgifter (GrUU 2/2018 rd, s. 5).

De bestämmelser om behandlingen av personuppgifter som föreslås i propositionen baserar sig på det nationella handlingsutrymmet enligt artikel 6 i den allmänna dataskyddsförordningen. Medlemsstaternas lagstiftning, som avses i artikel 6.3 i den förordningen, ska uppfylla ett mål av allmänt intresse och stå i proportion till det legitima mål som eftersträvas. Om personuppgifter behandlas för andra ändamål än det ändamål för vilket personuppgifterna samlades in, ska bestämmelserna bedömas mot principen om ändamålsbegränsning på det sätt som anges i artikel 6.4 i dataskyddsförordningen. Bestämmelserna ska vara en nödvändig och proportionell åtgärd för att skydda de mål som avses i artikel 23.1 i den allmänna dataskyddsförordningen. Bestämmelserna ska också stå i proportion till det legitima mål som eftersträvas, i dem ska till centrala delar iakttas rätten till skydd för personuppgifter och i dem ska föreskrivas om lämpliga och särskilda åtgärder för att skydda den registrerades grundläggande rättigheter och intressen.

Enligt grundlagsutskottets utlåtande (GrUU 14/2018 rd) måste behovet av speciallagstiftning bedömas utifrån de hot och risker som behandlingen av personuppgifter orsakar i enlighet med det riskbaserade synsätt som också krävs i dataskyddsförordningen. Ju större risk fysiska personers rättigheter och friheter utsätts för på grund av behandlingen, desto mer motiverat är det med mer detaljerade bestämmelser. Denna omständighet är av särskild betydelse när det gäller behandling av känsliga uppgifter. Grundlagsutskottet har dessutom både före och efter ikraft-

trädandet av dataskyddsförordningen betonat de hot som hänför sig till behandlingen av känsliga personuppgifter. Utskottet anser att allvarliga risker som gäller informationssäkerhet och missbruk av uppgifter kan vara förknippade med omfattande databaser som innehåller känsliga uppgifter och i sista hand kan det vara en persons identitet som är hotad (GrUU 13/2016 rd, s. 4, GrUU 14/2009 rd, s. 3/I).

I konstitutionella analyser av behandlingen av personuppgifter har grundlagsutskottet sett syftet med behandlingen som relevant, eftersom behandlingen möjliggör utövning av offentlig makt gällande individer (GrUU 14/2018 rd, s.6 och GrUU 1/2018 rd, s. 6). Enligt 2 § 3 mom. i grundlagen ska all utövning av offentlig makt bygga på lag. För bestämmelser i lag gäller åter det generella kravet att lagen ska vara exakt och noga avgränsad. Enligt utskottet är regleringen av befogenheter vanligen relevant också i förhållande till de i grundlagen inskrivna grundläggande fri- och rättigheterna (GrUU 51/2006 rd, s. 2/I).

I propositionen har man beaktat det nationella handlingsutrymmet enligt dataskyddsförordningen när det gäller bestämmelserna om registrens datainnehåll och personuppgiftsansvariga: I lagförslag nr 1 föreskrivs det inom ramen för det nationella handlingsutrymmet att Myndigheten för digitalisering och befolkningsdata är personuppgiftsansvarig vid produktionen av tjänster för digital identitet samt vid tillhandahållandet av bevis för kärnidentitet och e-tjänstverktyg för utlänningar. På motsvarande sätt föreskrivs det i lagförslag nr 2 att polisen är personuppgiftsansvarig för registret över e-legitimation. Dessutom har de rättsliga grunderna för behandlingen av personuppgifter i dessa register angetts på det sätt som dataskyddsförordningen förutsätter. Med beaktande av den centrala ställning som de register som avses i lagförslagen har vid behandlingen av uppgifter om finländares identiteter och vid produktionen av nationella identitetshandlingar krävs det mer detaljerade bestämmelser om dessa register och de personuppgiftsansvariga än de allmänna bestämmelser som finns i dataskyddsförordningen. Med tanke på dataskyddsförordningens riskbaserade förhållningssätt är det befogat att införa specialbestämmelser om registren som gäller tjänster för digital identitet och e-legitimation, eftersom det nya digitala sättet att behandla medborgarnas identiteter är förenat med högre risker än normalt när det gäller bland annat informationssäkerheten. Ur denna synvinkel kan man anse att de specialbestämmelser som nu föreslås är nödvändiga för att tillgodose skyddet för personuppgifter.

På de grunder som anförts ovan anses de lagförslag som ingår i propositionen vara behövliga till de delar som gäller behandlingen av personuppgifter med avseende på såväl dataskyddslagen som grundlagen.

*Personuppgifter som behandlas och deras säkerhet*

Grundlagsutskottet har särskilt lyft fram behovet av reglering i de fall där personuppgifterna behandlas av en myndighet (GrUU 15/2018 rd). Enligt artikel 6 c i den allmänna dataskyddsförordningen är behandling av personuppgifter tillåten om behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. Behandlingen av personuppgifter är enligt artikel 6 e laglig om den är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning (se GrUU 14/2018 rd, s. 4).

Grundlagsutskottet har fäst särskild uppmärksamhet vid att inskränkningar i skyddet för privatlivet måste bedömas utifrån de allmänna villkoren för inskränkningar av de grundläggande fri- och rättigheterna (GrUU 42/2016 rd, s. 2–3). Lagstiftarens handlingsutrymme när det föreskrivs om behandlingen av personuppgifter begränsas i synnerhet av att skyddet för personuppgifter

delvis omfattas av skyddet för privatlivet, som tryggas i samma moment i 10 § i grundlagen. Lagstiftaren måste trygga denna rätt på ett sätt som kan betraktas som acceptabelt med tanke på systemet för de grundläggande rättigheterna som helhet.

I lagförslagen föreskrivs det om nya register i anslutning till produktionen av tjänster för digital identitet samt e-legitimation. I dessa register kommer man i huvudsak att behandla personuppgifter som redan finns i myndigheternas befintliga register, såsom sådana uppgifter om personer som finns lagrade i befolkningsdatasystemet samt i identitetskortsregistret enligt 31 §i lagen om identitetskort samt i passregistret enligt 29 § i passlagen. Sådana personuppgifter som behandlas är således bland annat de uppgifter som förtecknas i 13 § 1 mom. i BDS-lagen, såsom personens fullständiga namn, personbeteckning samt teknisk identifieringskod och elektronisk kommunikationskod, samt personens identifikationskod enligt den 11 a § i BDS-lagen som är under beredning. Andra personuppgifter som behandlas är bland annat de i 4 § i lagen om behandling av personuppgifter i polisens verksamhet avsedda behövliga grundläggande uppgifter om en person som är lagrade i identitetskortsregistret och passregistret, såsom en persons namn, födelsetid, födelseort och kön samt personens fotografi, som han eller hon har överlämnat till identitetskorts- eller passmyndigheten när han eller hon ansökt om identitetskort eller pass.

Nya personuppgifter är det bevis för kärnidentitet som föreslås i lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata samt uppgifterna i de register som hänför sig till beviset. Dessa uppgifter motsvarar dock i det första skedet i huvudsak de uppgifter som registreras i samband med Myndigheten för digitalisering och befolkningsdatas certifikattjänster enligt 6 kap. i BDS-lagen. Helt nya uppgifter ingår dock i plattsformsregistret enligt 13 § 2 mom. i lagförslag nr 1, där det för att producera bevis för kärnidentitet förs in identifieringsuppgifter som specificerar en person, tekniska uppgifter om en teknisk plattform med koppling till personen, uppgifter om utrustningen och andra nödvändiga uppgifter. Uppgifter om fysiska personers mobila terminaler har inte tidigare samlats in för att utfärda identitetskort eller pass. Dessa uppgifter är dock nödvändiga för att producera bevis för kärnidentitet, så behandlingen av dem är nödvändig för att tillhandahålla e-legitimation samt e-tjänstverktyg för utlänningar. Det är också av betydelse med tanke på nödvändig insamling av uppgifter att det är frivilligt att ta i bruk e-legitimation och e-tjänstverktyg för utlänning, så tekniska uppgifter om de mobila terminaler kommer inte att samlas in av alla medborgare och personer som vistas i Finland. Dessa uppgifter ska alltså bara samlas in hos personer som vill ta i bruk en e-legitimation eller ett e-tjänstverktyg för utlänningar.

I propositionen har beaktats de förutsättningar som anges i dataskyddsförordningen för behandling av biometriska uppgifter och uppgifter som hör till särskilda kategorier av personuppgifter. Enligt artikel 4.4 i dataskyddsförordningen avses med biometriska uppgifter 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. Enligt artikel 9 i dataskyddsförordningen omfattar behandling av särskilda kategorier av personuppgifter bland annat behandling av biometriska uppgifter för att entydigt identifiera en fysisk person. I skäl 51 i dataskyddsförordningen konstateras dock uttryckligen att behandling av foton inte systematiskt bör anses utgöra behandling av särskilda kategorier av personuppgifter, eftersom foton endast definieras som biometriska uppgifter när de behandlas med särskild teknik som möjliggör identifiering eller autentisering av en fysisk person. Personuppgifter som hör till särskilda kategorier av personuppgifter bör inte behandlas, såvida inte behandling medges i särskilda fall som fastställs i dataskyddsförordningen eller till exempel i syfte att fullgöra en rättslig skyldighet. Utöver de särskilda kraven för sådan behandling, bör de allmänna principerna och andra bestämmelser i dataskyddsförordningen tillämpas, särskilt när det gäller villkoren för laglig behandling.

I en e-legitimation ställs användarens ansiktsbild i digital form till hans eller hennes eget förfogande i hans eller hennes mobila enhet. Bilden används för att identifiera användaren i anslutning till uträttande av ärenden på plats. Identifieringen av användaren bygger på identifierarens ögonmått på motsvarande sätt som i fråga om traditionella officiella identitetshandlingar, såsom pass och identitetskort. Kontrollapplikationen för e-legitimation innehåller inga särskilda tekniska metoder som skulle användas vid identifieringen, utan den bygger alltid på en fysisk persons övervägande som görs utifrån observationer som bygger på ögonmått. E-legitimation möjliggör inte i sig användning av särskilda tekniska metoder. I förslaget som gäller e-legitimation anses således behandling av fotografier således inte vara fråga om i artikel 9 i dataskyddsförordningen avsedd behandling av biometriska uppgifter för att entydigt identifiera en person.

Trots det som sägs ovan är personers fotografier som finns i identitetskortsregistret och passregistret sekretessbelagda uppgifter, varvid särskild försiktighet ska iakttas vid behandlingen av dessa uppgifter. Behandlingen av uppgifter i informationssystem förutsätter att alla parter kan lita på att de tekniska komplicerade informationssystemhelheter som används är förenliga med lagstiftningen vad beträffar principerna, de tekniska lösningarna och implementeringen, och att de uppfyller alla informationssäkerhetskrav. För dem som använder systemet behöver informationssystemhelheterna dessutom vara sinsemellan interoperabla och uppfylla de krav som ställs på praktisk funktionalitet.

Grundlagsutskottet har dessutom betonat kravet på ändamålsbegränsning särskilt i samband med behandlingen av känsliga uppgifter. När det gäller omfattande register med biometriska kännetecken finns det enligt grundlagsutskottet orsak att förhålla sig negativt till att uppgifterna används för ändamål som ligger utanför det syfte som de egentligen samlats in och registrerats för (GrUU 14/2009 rd, s. 4/II). Man kan då bara göra exakt avgränsade och smärre undantag från ändamålsbegränsningen. Bestämmelserna får inte leda till att någon annan verksamhet än den som är förknippad med det ursprungliga användningsändamålet blir det huvudsakliga ändamålet och inte ens ett betydande användningsändamål (se också t.ex. GrUU 14/2017 rd, s. 5–6). Lagen om behandling av personuppgifter i polisens verksamhet, som stiftats med grundlagsutskottets medverkan, innehåller bestämmelser om behandling av uppgifter i registret över identitetskort och passregistret för andra ändamål än de ursprungliga. Enligt 13 § 3 mom. i den lagen får en persons fotografi och namnteckningsprov med den berörda personens samtycke även användas för något annat förvaltningstillstånd eller beslut som personen ansökt om än den handling som fotografiet och namnteckningsprovet har lämnats för.

Utskottet har särskilt understrukit att då ett sådant register som till exempel patientdataregistret finns på flera ställen och innehåller känsliga uppgifter är det extra viktigt att informationssäkerheten fungerar och att åtgärder som förhindrar missbruk införs samtidigt som registret börjar användas (GrUU 41/2010 rd, s. 3/II). Trots att de ansiktsbilder som ingår i uppgifterna i ansökan om pass och identitetskort inte som sådana är biometriska uppgifter, ska särskild försiktighet iakttas när de behandlas på grund av deras särskilda karaktär.

På grund av det som sägs ovan bör i samband med ibruktagandet av e-legitimation särskild uppmärksamhet fästas på att informationssäkerhetsarrangemangen är tillgängliga genast när informationssystemet för digital identitet börjar användas. Tjänsterna för digital identitet och framför allt informationssystemet för digital identitet kan vad risknivån beträffar anses vara jämförbara med patientdatasystem som innehåller känsliga uppgifter, så samma krav på att informationssäkerhetsarrangemangen ska fungera och vara tillgängliga genast när tjänsterna och informationssystemet tas i bruk kan anses motiverade.

I propositionen specificeras de personuppgifter som myndigheterna behandlar och där föreskrivs särskilt om informationssäkerhetskraven på mera detaljerad nivå än dataskyddsförordningens och informationshanteringslagens krav. I 5 § i lagförslag nr 1 föreskrivs detaljerat om kvalitets- och informationssäkerhetskrav på informationssystemet för digital identitet, och i 9 § föreskrivs dessutom om skyldighet för Myndigheten för digitalisering och befolkningsdata att underrätta dem som använder tjänster för digital identitet om olika hot och störningar som riktar sig mot säkerheten. I 10 § i lagförslag nr 1 föreskrivs det dessutom separat om regelbunden bedömning av informationssystemets överensstämmelse med kraven, som ska göras innan informationssystemet tas i bruk. Syftet med de föreskrivna tekniska och organisatoriska åtgärderna är att förhindra missbruk samt olaglig åtkomst av personuppgifter som behandlas i informationssystemet för digital identitet. Särskilda åtgärder är bland annat krav på åtkomsthantering och tillträdesrätt samt särskilda krav på att stå emot avancerade säkerhetshot och att upptäcka betydande säkerhetskränkningar och -hot. Dessutom fungerar det separata kravet på att informationssäkerheten ska bedömas av ett bedömningsorgan för informationssäkerhet som en extra skyddsåtgärd enligt artikel 25 i dataskyddsförordningen. Sålunda har i propositionen beaktats de personuppgifter som behandlas och skyddet för dem på det sätt som dataskyddsförordningen och grundlagsutskottet förutsätter.

*Rätt att få information*

Grundlagsutskottet har bedömt bestämmelser om myndigheternas rätt att få och skyldighet att lämna ut information med avseende på skyddet för privatliv och personuppgifter i 10 § 1 mom. i grundlagen och då noterat bland annat vad och vem rätten att få information gäller och hur rätten är kopplad till nödvändighetskriteriet (GrUU 15/2018 rd). Myndigheternas rätt att få och möjlighet att lämna ut information kan gälla "behövliga uppgifter" för ett visst syfte, om lagen ger en uttömmande förteckning över innehållet i uppgifterna. Om innehållet däremot inte anges i form av en förteckning, ska det i lagstiftningen ingå ett krav på att "uppgifterna är nödvändiga" för ett visst syfte (se t.ex. GrUU 17/2016 rd, s. 2–3). Utskottet har däremot inte ansett att grundlagen tillåter en mycket vag och ospecificerad rätt att få uppgifter, inte ens om den är knuten till nödvändighetskriteriet (GrUU 59/2010 rd, s. 4).

Grundlagsutskottet har understrukit att det vid en särskiljning mellan behövlighet respektive nödvändighet att få eller lämna ut uppgifter är frågan inte bara om omfattningen av innehållet i uppgifterna utan också om att rätten till information, som går före sekretessbestämmelserna, i sista hand går ut på att den myndighet som är berättigad till informationen i och med sina egna behov åsidosätter de grunder och intressen som är skyddade med hjälp av den sekretess som gäller myndigheten som innehar informationen (GrUU 15/2018 rd). Ju mer generella bestämmelserna om rätt till information är, desto större är risken att sådana intressen kan åsidosättas per automatik. Ju fullständigare bestämmelserna kopplar rätten till information till villkor i sak, desto mer sannolikt är det att en enskild begäran om information måste motiveras. Då kan också den som lämnar ut informationen bedöma begäran med avseende på de lagliga villkoren för utlämnandet. Genom att de facto vägra att lämna ut informationen kan den som innehar den göra att det uppstår ett läge där en utomstående myndighet måste undersöka skyldigheten att lämna ut information, det vill säga tolka bestämmelserna. Denna möjlighet är viktig då det gäller att anpassa tillgången till information och sekretessintressena till varandra (GrUU 17/2016 rd, s. 6).

I propositionen har beaktats grundlagsutskottets utlåtandepraxis när det gäller rätt att få information. I propositionen ingår bestämmelser om myndigheternas rätt att få information i lagen om behandling av personuppgifter i polisens verksamhet, där det föreslås att 16 § ändras så att polisen trots sekretessbestämmelserna ska ha rätt att för att utföra sina uppgifter och föra sina

personregister få uppgifter som är nödvändiga för produktion av e-legitimation i enlighet med lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata. På motsvarande sätt ändras lagens 22 § så att polisen trots sekretessbestämmelserna ska ha rätt att lämna ut sådana personuppgifter som avses i 5–8, 11 och 12 § för en uppgift som myndigheten har enligt lag till Myndigheten för digitalisering och befolkningsdata för produktion och administration av det informationssystem för digital identitet och de bevis för kärnidentitet som avses i lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata. Sålunda gäller polisens rätt att få information endast uppgifter som är nödvändiga för att producera e-legitimation och Myndigheten för digitalisering och befolkningsdatas rätt att få information gäller en på förhand specificerad och begränsad datamängd, som Myndigheten för digitalisering och befolkningsdata får behandla endast för de ändamål som anges i lagstiftningen. De föreslagna bestämmelserna anses till denna del stämma överens med grundlagsutskottets utlåtandepraxis när det gäller rätt att få information.

*Rätt att bestämma över information om sig själv och principen om självägd identitet*

Grundlagsutskottet har ansett att rätten att bestämma över information om sig själv bör anses vara central med avseende på skyddet av personuppgifter (se t.ex. GrUU 23/2020 rd, s. 9, GrUU 2/2018 rd, s. 8). Grundlagsutskottet har ansett att självbestämmanderätten är kopplad till ett flertal grundläggande fri- och rättigheter, särskilt till grundlagens 7 § om personlig frihet och integritet och 10 § om skydd för privatlivet (se GrUU 48/2014 rd, s. 2/II).

I de föreslagna lagarna om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata och om e-legitimation lämnas bestyrkta uppgifter om en person i en e-legitimation eller ett e-tjänstverktyg för utlänningar till personens eget förfogande. I fråga om e-tjänstverktyg för utlänningar uppräknas uppgifterna på ett heltäckande sätt i 16 § i lagförslag nr 1 och i fråga om e-legitimation i 4 § i lagförslag nr 2. De uppgifter som lämnas till personens eget förfogande härrör i fråga om e-tjänstverktyg för utlänningar från befolkningsdatasystemet, som Myndigheten för digitalisering och befolkningsdata och Statens ämbetsverk på Åland underhåller med stöd av 4 § i BDS-lagen, och i fråga om e-legitimation från passregistret eller identitetskortsregistret, som polisen för med stöd av 29 § i passlagen eller 31 § i lagen om identitetskort.

Att en persons egna uppgifter lämnas till personens eget förfogande kan på allmänt plan kallas självägd identitet. Med självägd identitet (eng. Self-Sovereign Identity, SSI) avses en modell för behandling av personuppgifter, där en person själv kan administrera hur hans eller hennes personuppgifter som härrör från antingen honom eller henne själv eller en tillförlitlig tredje part visas för en e-tjänst där personuppgifter behövs. I praktiken avses med självägd således att personerna själv förfogar över sina egna personuppgifter.

I propositionen avses med att uppgifter lämnas till en persons eget förfogande ur dataskydds- och informationsrättslig synvinkel att myndigheten lämnar bestyrkta uppgifter, som är både personuppgifter enligt artikel 4.1 i dataskyddsförordningen och myndighetshandlingar enligt 5 § 2 mom. i offentlighetslagen, till personens eget förfogande. Till följd av detta är de uppgifter som lämnats till en person inte längre myndighetshandlingar och myndigheten är inte längre personuppgiftsansvarig för dem. På en persons egen behandling av sina uppgifter tillämpas inte längre lagstiftningen om dataskydd och informationshantering. Personen har rätt att visa sina uppgifter fritt för de personuppgiftsansvariga som han eller hon vill och på dessa aktörers behandling av personuppgifterna tillämpas fullt ut dataskyddsförordningen och, när det är fråga om myndighetsaktörer, lagstiftningen om informationshantering.

Att bestyrkta uppgifter lämnas till en persons eget förfogande motsvarar analogt en situation där en person hämtat ett fysiskt dokument som gäller honom eller henne själv hos en myndighet eller myndigheten postar dokumentet till personens hemadress. Det är således fråga om att överföra ett befintligt tillvägagångssätt till en digital behandlingsmiljö. Någon motsvarande handlingsmodell har emellertid inte tidigare genomförts i en elektronisk behandlingsmiljö, så det behövs en konstitutionell analys av den.

I lagförslaget används emellertid inte separat begreppet ”självsägd identitet”. Detta beror bland annat på att grundlagsutskottet har ansett att man när det handlar om reglering som är känslig med avseende på de grundläggande fri- och rättigheterna och som har anknytning till EU-rätten bör förhålla sig restriktivt till att i lagstiftningen ersätta etablerade begrepp som grundar sig på gällande rätt med nya begrepp som är klart mer diffusa och lätt kan leda till oklarheter vid tolkningen (GrUU 2/2018 rd, s. 8). I utlåtandet tog grundlagsutskottet ställning till begreppet ”Mina data” och konstaterade att det är oklart hur begreppet förhåller sig till det grundlagsenliga skyddet för personuppgifter.

Att personuppgifter lämnas till eget förfogande i en e-legitimation eller e-tjänstverktyg för utlänningar betyder ändå inte att de myndigheter ur vilkas register de bestyrkta uppgifterna lämnas inte längre skulle ansvara för de ursprungliga registeruppgifterna. Det är snarare fråga om att lämna ut ett utdrag över registeruppgifter för vilkas behandling myndigheterna fortfarande svarar i såväl myndighetsrollen som rollen som personuppgiftsansvarig. På motsvarande sätt ansvarar de parter för vilka innehavare av e-legitimation och e-tjänstverktyg för utlänningar visar sina bestyrkta uppgifter för att de behandlas i enlighet med gällande dataskydds- och annan lagstiftningen. Sålunda tillämpas på behandling av personuppgifter som utförs av aktörer i den privata sektorn som vanligt dataskyddsförordningen och på aktörer inom den offentliga sektorn dataskyddsförordningen och annan lagstiftning som är förpliktande för myndigheterna. Den föreslagna modellen med självägd identitet anses vara förenlig med bestämmelserna i grundlagen. Grundlagsutskottet har emellertid inte tidigare behandlat någon sådan modell för behandling av personuppgifter som den som nu föreslås. Sålunda anser regeringen att det skulle vara bra om grundlagsutskottet ger utlåtande om saken.

### 12.3 Jämlikhet

*Inledning*

Regeringens proposition har konsekvenser för jämlikheten, som tryggas i grundlagen. Ett syfte med regeringens proposition är att främja lika möjligheter för finska medborgare och utlänningar som vistas i Finland att använda digitala tjänster och sålunda uträtta ärenden elektroniskt med myndigheter och andra ärenden. Ett centralt syfte med bestämmelserna är att på ett positivt sätt främja i grundlagen avsedd jämlikhet.

Enligt 6 § 1 mom. i grundlagen är alla lika inför lagen. Bestämmelsen uttrycker vid sidan av kravet på juridisk likabehandling även idén om faktisk jämlikhet. I det ingår ett förbud mot godtycke och ett krav på enahanda bemötande i likadana fall. Den allmänna principen om likabehandling kompletteras genom diskrimineringsförbudet i 6 § 2 mom. i grundlagen, enligt vilket ingen utan godtagbart skäl får särbehandlas på grund av kön, ålder, ursprung, språk, religion, övertygelse, åsikt hälsotillstånd eller handikapp eller av någon annan orsak som gäller hans eller hennes person. En sådan annan orsak kan vara till exempel hemort (se RP 309/1993 rd, s. 42–44; se t.ex. GrUU 15/2018 rd, s. 6–7, GrUU 26/2017 rd, s. 36–41 och 44–45, och GrUU 67/2014 rd, s. 3).

Närmare bestämmelser om likabehandling och förbud mot diskriminering ingår i diskrimineringslagen (1325/2014), i vars 2 kap. såväl direkt som indirekt diskriminering förbjuds. Enligt lagens 13 § ska indirekt diskriminering anses förekomma när regler, kriterier eller förfaringssätt som framstår som jämlika kan komma att missgynna någon på grund av en omständighet som gäller honom eller henne som person, om inte regeln, kriteriet eller förfaringssättet har ett godtagbart syfte och medlen för att nå detta syfte är lämpliga och behövliga. Även grundlagsutskottet har betonat att förbudet mot diskriminering gäller också åtgärder som indirekt leder till ett diskriminerande resultat (GrUU 31/2014 rd, s. 3).

Diskriminering förbjuds uttryckligen också i Europakonventionen och i EU:s stadga om de grundläggande rättigheterna. Enligt artikel 14 i Europakonventionen ska åtnjutandet av de fri- och rättigheter som anges i denna konvention tryggas utan åtskillnad av något slag, såsom på grund av kön, ras, hudfärg, språk, religion, politisk eller annan åskådning, nationell eller social härkomst, tillhörighet till nationell minoritet, förmögenhet, börd eller ställning i övrigt. Inom EU-rätten har principen om likabehandling fastställts i artikel 20 i Europeiska unionens stadga om de grundläggande rättigheterna, enligt vilken alla människor är lika inför lagen. Ett förbud mot diskriminering ingår i artikel 21.1, där all diskriminering på grund av bland annat kön, ras, hudfärg, etniskt eller socialt ursprung, genetiska särdrag, språk, religion eller övertygelse, politisk eller annan åskådning, tillhörighet till nationell minoritet, förmögenhet, börd, funktionshinder, ålder eller sexuell läggning förbjuds. I artikel 21.2 förbjuds dessutom diskriminering på grund av nationalitet.

Det ska vara frivilligt att ta i bruk sådan e-legitimation, e-tjänstverktyg för utlänningar och identifieringsverktyg för fysiska personer som avses i propositionen. Ibruktagandet av de föreslagna tjänsterna ska inte påverka en persons rätt att använda samhällets digitala tjänster. Sålunda har produktionen av dessa tjänster inte konsekvenser för jämlikheten till denna del.

Propositionen är förenad med frågor om likabehandling som är av betydelse med tanke på 6 § i grundlagen samt Europakonventionen och Europeiska unionens stadga om de grundläggande rättigheterna och som gäller tillhandahållande av e-legitimation, e-tjänstverktyg för utlänningar och identifieringsverktyg för fysiska personer till specialgrupper samt dessa gruppers faktiska möjlighet att nyttja de föreslagna nya verktygen för e-tjänster i samhällets digitala tjänster.

*E-legitimation och identifieringsverktyg för fysiska personer*

I lagförslag nr 2 i regeringens proposition ingår bestämmelser om e-legitimation som tillhandahålls av polisen och som kan tas i bruk av en person som har ett giltigt finskt pass eller identitetskort. Med identitetskort avses i detta sammanhang också identitetskort för utlänningar och identitetskort för minderåriga över 15 år. För att ta i bruk e-legitimation förutsätts dessutom att man äger en smarttelefon, eftersom den är en förutsättning för registrering av beviset för kärnidentitet och installation av den mobila applikation som Myndigheten för digitalisering och befolkningsdata producerar. Dessutom lagras de bestyrkta uppgifter som lämnas till en persons eget förfogande i hans eller hennes smarttelefon.

Förutsättningarna för ibruktagande av e-legitimation, dvs. giltigt finskt pass eller identitetskort samt innehav av en smarttelefon, kan de facto hindra vissa grupper av personer från att ta i bruk e-legitimation.

Kravet på att man ska äga ett giltigt pass eller identitetskort är dock en nödvändig förutsättning för att skaffa en e-legitimation, eftersom e-legitimation är en elektronisk motsvarighet till dessa identitetshandlingar. Vid en helhetsbedömning är det dessutom av betydelse att det är möjligt

att få grundläggande utkomststöd från Folkpensionsanstalten för att skaffa pass eller ett fotografiförsett identitetskort, när det är nödvändigt för en person eller hans eller hennes familjemedlem att skaffa identitetshandlingen för att till exempel kunna sköta bankärenden. Sålunda bedöms inte kravet på ett giltigt pass eller identitetskort vara problematiskt med avseende på den allmänna klausulen om likabehandling eller diskrimineringsförbudet.

Också kravet på att man ska äga en mobil terminal (smarttelefon) måste bedömas med avseende på likabehandling. I princip använder medborgarna mobila enheter i stor utsträckning, men en del av befolkningen använder ändå inte sådana enheter av olika orsaker. Det kan handla om till exempel barn under skolåldern eller mycket gamla personer. Omständigheterna är emellertid mycket varierande och det är också möjligt att det finns personer som inte vill använda smarttelefon. E-legitimation möjliggör stark autentisering oberoende av kundrelationer i såväl den offentliga som den privata sektorns digitala tjänster som förutsätter stark autentisering. Personer som inte använder smarttelefon kan som ett alternativ till e-legitimation ta i bruk identifieringsverktyget för fysiska personer i anslutning till e-tjänster, med vars hjälp det är möjligt att identifiera sig i den offentliga sektorns digitala tjänster. Identifieringsverktyg för fysiska personer är ett fysiskt verktyg som kan användas utan mobil terminal eller chipskort. När det gäller användning av den offentliga sektorns digitala tjänster tillhandahålls en lösning också för de personer som inte har en smarttelefon, och till denna del är bestämmelserna motiverade med avseende på 6 § i grundlagen.

Identifieringsverktyget för fysiska personer ska ändå inte möjliggöra elektronisk identifiering i den privata sektorns e-tjänster som förutsätter stark autentisering. Till denna del kan lösningen motiveras med avseende på den konkurrens- och statsstödsrättsliga konsekvensbedömningen. Konsekvenserna för konkurrensen behandlas mer ingående ovan. I tillämpliga delar kan man även i dessa fall använda privata tjänsteleverantörers identifieringslösningar samt det medborgarcertifikat som ingår i identitetskort. På marknadsvillkor tillhandahålls motsvarande alternativa identifieringsverktyg, med vars hjälp det är möjligt att identifiera sig i den privata sektorns elektroniska tjänster. Identifieringsverktyget för fysiska personer ökar de jämlika möjligheterna att identifiera sig i den offentliga sektorns elektroniska tjänster och ger i sista hand alla möjlighet att uträtta ärenden hos myndigheterna på elektronisk väg.

Gällande uträttande av ärenden på plats fungerar det nuvarande passet och identitetskortet som alternativ till e-legitimation. De fungerar redan nu som ett tillförlitligt sätt att styrka identiteten då ärenden uträttas på plats. De befintliga identitetshandlingarna möjliggör ändå inte uppgiftsminimering i anslutning till uträttande av ärenden på plats så att den som styrker sin identitet på ett tillförlitligt sätt kan styrka till exempel endast sin ansiktsbild eller ålder i e-tjänsten. Tills vidare finns det emellertid ingen sådan färdig teknik för att visa selektiva bestyrkta uppgifter med vars hjälp personuppgifter som myndigheterna verifierat elektroniskt skulle kunna förmedlas till förlitande parter på ett tillförlitligt sätt utan smarttelefon.

På de grunder som anförs ovan kan den helhet som e-legitimation och identifieringsverktyg för fysiska personer bildar anses vara förenlig med 6 § i grundlagen.

*E-tjänstverktyg för utlänningar*

Ett syfte med propositionen är att förbättra åtkomsten till samhällets digitala tjänster för utlänningar som vistas i Finland. I lagförslag nr 1 i regeringens proposition föreslås att Myndigheten för digitalisering och befolkningsdata ska producera ett nytt e-tjänstverktyg för utlänningar.

Ansökan om ett e-tjänstverktyg för utlänningar ska kunna göras av en utländsk medborgare som inte har möjlighet att få finskt pass eller identitetskort, men som har behov av att uträtta ärenden i finländska e-tjänster. Myndigheten för digitalisering och befolkningsdata kan bevilja e-tjänstverktyget för en utländsk medborgare som är registrerad i befolkningsdatasystemet och som har fått finsk personbeteckning. E-tjänstverktyget för utlänningar är ändå inte en med pass eller identitetskort jämförbar identitetshandling. Den kan inte nyttjas i anslutning till uträttande av ärenden på plats, utan e-tjänstverktyget är avsett endast för e-tjänster.

Man kan få ett e-tjänstverktyg för utlänningar antingen genom att besöka Myndigheten för digitalisering och befolkningsdata personligen eller genom förfarandet för distansregistrering enligt 9 a § i BDS-lagen. Ett e-tjänstverktyg som skaffats genom förfarandet för distansregistrering är ändå inte lika tillförlitligt vad tillitsnivån beträffar som sådan identifiering av en person som grundar sig på ett identifieringsverktyg för stark autentisering. Sålunda ska det vara möjligt för en utländsk medborgare att använda e-tjänstverktyget i anslutning till e-tjänster, men de förlitande parterna bestämmer hur ett e-tjänstverktyg som skaffats genom förfarandet för distansregistrering kan nyttjas i praktiken på grund av dess lägre tillitsnivå.

Orsakerna till skillnaderna mellan e-tjänstverktyg för utlänningar och e-legitimation har framför allt att göra med informationssäkerheten: förfarandet för distransregistrering är inte en lika tillförlitlig metod för att kontrollera identiteten som ett personligt besök hos myndigheten och en utländsk identitetshandlings ansiktsbild uppfyller inte nödvändigtvis kraven på finländska ansiktsbilder som lagras i identitetskortsregistret och passregistret. Av dessa orsaker ska det inte vara möjligt att nyttja e-tjänstverktyget för utlänningar som ett egentligt verktyg för stark autentisering och inte heller i anslutning till uträttande av ärenden på plats. När identiteten styrks är det mycket viktigt att säkerställa informationssäkerhet och tillförlitlighet, och sålunda är et nödvändigt att begränsa nyttjandet av e-tjänstverktyg för utlänningar på de sätt som nämns ovan. Sålunda anses bestämmelserna till denna del uppfylla förutsättningarna i 6 § i grundlagen.

*Minderåriga*

Regeringens proposition har konsekvenser för minderårigas ställning som användare av digitala tjänster. Enligt 6 § 3 mom. i grundlagen ska barn bemötas som jämlika individer och de ska ha rätt till medinflytande enligt sin utvecklingsnivå i frågor som gäller dem själva. Enligt förarbetena till grundlagen (RP 309/1993 rd, s. 45/I) är det viktigt dels att barnen behandlas lika sinsemellan, dels att de ses som jämbördiga människor som i princip har samma grundläggande fri- och rättigheter som den vuxna befolkningen. Ett barn ska bemötas som en individ, inte bara som ett passivt föremål för åtgärder. Å andra sidan utgör bestämmelsen ett argument för särskilt skydd och särskild omsorg för barn eftersom de utgör en omyndig och svagare grupp än de vuxna (GrUU 64/2018 rd, s. 2).

Av betydelse är också konventionen om barnets rättigheter, enligt vars artikel 1 med barn avses varje människa under 18 års ålder, om inte barnet blir myndigt tidigare enligt den lag som gäller för barnet.

Enligt propositionen kan de som har fyllt 15 år ta i bruk e-legitimation utan vårdnadshavarens samtycke. I enlighet med den nya 1 a § om e-legitimation som föreslås i lagen om identitetskort ger ett identitetskort rätt till en i lagen om e-legitimation avsedd e-legitimation som utfärdas av en myndighet som utfärdat identitetskortet. Ett temporärt identitetskort eller ett sådant identitetskort för minderårig som har utfärdats för en person under 15 år ger dock inte rätt till en e-legitimation. Sålunda kan propositionen anses förbättra likabehandlingen av minderåriga på det sätt som avses i 6 § 3 mom. i grundlagen på så vis att 15—18-åringar i samband med ansökan

om identitetskort för minderårig enligt lagen om identitetskort enligt propositionen i fortsättningen utan vårdnadshavarens samtycke kan få en e-legitimation tillhandahållen av staten som möjliggör stark autentisering och visande bestyrkta uppgifter. Personer över 15 år kan i regel antas vara så mogna att de självständigt kan sköta sina egna ärenden i digitala tjänster, så till denna del främjar de föreslagna bestämmelserna likabehandlingen av minderåriga när det gäller samhällets elektroniska tjänster.

Enligt propositionen har de som är under 15 år ändå inte faktisk möjlighet att ta i bruk e-legitimation utan vårdnadshavarens samtycke. I anslutning till e-tjänster är det i princip inte möjligt att på samma sätt som i anslutning till uträttande av ärenden på plats från fall till fall bedöma barnets utvecklingsnivå och förmåga att fatta beslut som gäller hans eller hennes ärende. Detta talar för att det sätts en åldersgräns så att innehavaren av en identitetshandling som används i anslutning till e-tjänster nästan utan undantag kan antas vara förmögen att fatta beslut som gäller hans eller hennes egna ärenden. Den som är under 15 år har möjlighet att få handlingen med föräldrarnas samtycke, och på detta sätt säkerställs det att barnets utvecklingsnivå har beaktats. Trots att regleringen försätter dem som över och dem som är under 15 år i olika ställning med avseende på likabehandling, kan regleringen anses vara motiverad.

### 12.4 Överföring av lagstiftningsmakt till en myndighet

I förslaget till lag om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata bestäms det om nya befogenheter för Myndigheten för digitalisering och befolkningsdata att utfärda föreskrifter om kraven på informationssäkerhet hos tjänster för digital identitet. Myndigheten för digitalisering och befolkningsdata ska meddela närmare föreskrifter om de krav som ska ställas på de kontrollapplikationer som produceras av andra aktörer. Det ska krävas informationssäkerhet på motsvarande nivå som i fråga om Myndigheten för digitalisering och befolkningsdatas eget avläsargränssnitt.

Enligt 80 § 2 mom. i grundlagen kan en myndighet genom lag bemyndigas att utfärda rättsnormer i bestämda frågor, om det med hänsyn till föremålet för regleringen finns särskilda skäl och regleringens betydelse i sak inte kräver att den sker genom lag eller förordning. Enligt grundlagen ska dessutom tillämpningsområdet för ett sådant bemyndigande vara exakt avgränsat. Särskilda skäl att bemyndiga en myndighet att utfärda föreskrifter är bland annat en teknisk reglering av smärre detaljer (GrUU 52/2001 rd, GrUU 46/2001 rd) som inte inbegriper prövningsrätt i någon större utsträckning (GrUU 43/2000 rd). De ärenden som bemyndigandet omfattar ska vara noggrant definierade i lagen och de ska vara exakt avgränsade till sitt tillämpningsområde (RP 1/1998 rd).

Bemyndigandet att meddela föreskrifter ska basera sig på tekniska kravspecifikationer och vara förenligt med kraven på informationssäkerhet. Med stöd av den föreslagna lagen ska Myndigheten för digitalisering och befolkningsdata besluta om närmare tekniska krav på informationssystemet för digital identitet samt om informationssäkerhetskrav. Kraven ska grunda sig på allmänt kända nationella eller internationella standarder. De närmare tekniska informationssäkerhetskraven på kontrollapplikationen preciseras i och med Myndigheten för digitalisering och befolkningsdatas egen implementering. Med beaktande av föreskrifternas tekniska natur och att standarderna och de allmänna informationssäkerhetskraven som ligger som grund för kraven håller på att förnyas är det motiverat att föreskriva om bemyndigande för Myndigheten för digitalisering och befolkningsdata att meddela föreskrifter. Bemyndigandet att meddela föreskrifter gör det möjligt för Myndigheten för digitalisering och befolkningsdata att uppdatera kravspecifikationerna med jämna mellanrum.

Det bemyndigande att meddela föreskrifter som beskrivs ovan uppfyller förutsättningarna enligt 80 § 2 mom. i grundlagen. Bestämmelsens betydelse i sak förutsätter inte att det bestäms om saken genom lag eller förordning. Det föreslagna bemyndigandet är noggrant avgränsat och detaljerat och dess tillämpningsområde är exakt avgränsat.

Med stöd av vad som anförts ovan kan lagförslagen behandlas i vanlig lagstiftningsordning. Regeringen anser det dock önskvärt att grundlagsutskottet ger ett utlåtande i frågan.

*Kläm*

Med stöd av vad som anförts ovan föreläggs riksdagen följande lagförslag:

*Lagförslag*

**1.**

# Lag

**om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata**

I enlighet med riksdagens beslut föreskrivs:

1 kap.

## Allmänna bestämmelser

1 §

*Tillämpningsområde*

Denna lag innehåller bestämmelser om de tjänster för digital identitet som produceras av Myndigheten för digitalisering och befolkningsdata och om nyttjande av sådana tjänster.

2 §

*Definitioner*

I denna lag avses med
*1) tjänster för digital identitet* ett informationssystem för digital identitet, bevis för kärnidentitet, e-tjänstverktyg för utlänningar, en tjänst för hantering av digital identitet, ett avläsargränssnitt och kontrollapplikationer,
*2) kärnidentitet* en sådan helhet av personuppgifter registrerade i befolkningsdatasystemet med vars hjälp identiteten allmänt kan specificeras och som består av de uppgifter som avses i 13 § 1 mom. 1 och 2 punkten i lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata (661/2009),
*3) bestyrkta uppgifter* personuppgifter som verifierats av en myndighet på elektronisk väg,
*4) e-legitimation* en identitetshandling som avses i 3 § 1 mom. i lagen om e-legitimation ( / ),
*5) teknisk plattform* en mobil terminal som innehavaren av en e-legitimation eller av ett e-tjänstverktyg för utlänningar förfogar över,
*6) applikation för digital identitet* en applikation som innehavaren av en identitetshandling har på sin mobila terminal och som gör det möjligt att använda en e-legitimation eller ett e-tjänstverktyg för utlänningar,
*7) förlitande part* en fysisk eller juridisk person för vilken innehavaren av en e-legitimation eller av ett e-tjänstverktyg för utlänningar styrker sin identitet eller visar bestyrkta uppgifter,
*8) uträttande av ärenden på plats* uträttande av ärenden på så sätt att innehavaren av en e-legitimation och den förlitande parten är samtidigt närvarande på samma plats och innehavaren av e-legitimationen styrker sin identitet eller visar andra bestyrkta uppgifter som gäller honom eller henne till den förlitande parten.

3 §

*Personuppgiftsansvarig för tjänster för digital identitet*

Myndigheten för digitalisering och befolkningsdata är personuppgiftsansvarig för tjänster för digital identitet. Myndigheten för digitalisering och befolkningsdata har dock inte rätt att till en förlitande part lämna ut personuppgifter som behandlas i samband med produktionen av tjänster för digital identitet.

2 kap.

**Väsentliga krav på informationssystemet för digital identitet och bedömning av kraven**

4 §

*Informationssystemet för digital identitet*

Myndigheten för digitalisering och befolkningsdata ska producera en applikation för digital identitet samt ett sådant informationssystem för digital identitet som består av ett bakomliggande system för applikationen. I informationssystemet ingår ett identifieringssystem med hjälp av vilket bestyrkta uppgifter kan visas i anslutning till e-tjänster och vid uträttande av ärenden på plats.

Avsikten med informationssystemet är att göra det möjligt att producera och nyttja e-legitimationer och e-tjänstverktyg för utlänningar.

5 §

*Kvalitets- och informationssäkerhetskrav*

Informationssystemet för digital identitet ska alltid vara tillgängligt, och det ska ha de reservsystem som behövs med tanke på störningar.

Myndigheten för digitalisering och befolkningsdata ska genom administrativa och tekniska åtgärder sörja för informationssystemets informationssäkerhet så att

1) informationssystemet och den information som behandlats där är tillgängliga endast för dem som har rätt att använda systemet och informationen,

2) informationen och informationssystemet inte kan ändras av andra än dem som har rätt till detta,

3) informationen och informationssystemet kan nyttjas av dem som har rätt att använda informationen och systemet,

4) informationssystemet tål sådana avancerade hot mot informationssäkerheten som kan förväntas, och

5) sådana betydande kränkningar av och hot mot informationssäkerheten som riktas mot informationssystemet kan upptäckas.

Myndigheten för digitalisering och befolkningsdata beslutar om närmare tekniska krav på informationssystemet och om krav på informationssäkerhet. Kraven ska grunda sig på allmänt kända nationella eller internationella standarder. Myndigheten för digitalisering och befolkningsdata ska höra Transport- och kommunikationsverket och Polisstyrelsen innan den meddelar ett beslut om krav på informationssäkerhet.

6 §

*Krav på identifieringssystemet*

Det identifieringssystem som ingår i informationssystemet för digital identitet ska åtminstone uppfylla kraven för tillitsnivån väsentlig enligt artikel 8.2 b i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.

Identifieringssystemet behöver vid produktion av e-tjänstverktyg för utlänningar inte uppfylla registreringskraven för tillitsnivån väsentlig enligt 1 mom.

7 §

*Information som ska offentliggöras före ibruktagandet av informationssystemet*

Innan Myndigheten för digitalisering och befolkningsdata gör det möjligt att nyttja informationssystemet för digital identitet ska den offentliggöra följande information:

1) datum från och med vilket det är möjligt för en förlitande part att nyttja informationssystemet,

2) informationssystemets egenskaper och en beskrivning av de tekniska gränssnitt och metoder för testning som tillhandahålls dem som nyttjar systemet,

3) uppgift om utförd bedömning av överensstämmelse med kraven,

4) eventuella andra än i 1–3 punkten avsedda villkor som är nödvändiga med tanke på nyttjandet av informationssystemet.

Myndigheten för digitalisering och befolkningsdata ska göra det möjligt att nyttja informationssystemet för digital identitet i enlighet med den information som offentliggjorts. Myndigheten för digitalisering och befolkningsdata ska utan dröjsmål offentliggöra ändringar i den information som avses i 1 mom.

8 §

*Autentisering av en förlitande part*

Genom applikationen för digital identitet ska en förlitande part som avses i 26 § autentiseras med hjälp av certifikat eller på ett annat informationssäkert sätt när en innehavare av applikationen visar sina bestyrkta personuppgifter med en e-legitimation eller ett e-tjänstverktyg för utlänningar.

Myndigheten för digitalisering och befolkningsdata bestämmer vilka certifikat eller andra autentiseringsmekanismer som ska godkännas i ett beslut som avses i 5 §, som en del av övriga närmare tekniska krav på informationssystemet för digital identitet och krav på informationssäkerhet.

Myndigheten för digitalisering och befolkningsdata ska föra och offentliggöra en förteckning över godkända autentiseringsmekanismer och en förteckning över icke-godkända certifikat och andra autentiseringsmekanismer som är tillgängliga för förlitande parter.

9 §

*Underrättelse om hot och störningar*

Myndigheten för digitalisering och befolkningsdata ska utan obefogat dröjsmål underrätta förlitande parter, dem som nyttjar e-legitimationer och e-tjänstverktyg för utlänningar samt innehavare av applikationen för digital identitet om upptäckta betydande hot och störningar som riktas mot tjänsternas funktion, informationssäkerheten eller användningen av tjänsterna och om avbrott i dem. I underrättelsen ska det redogöras för de åtgärder som olika aktörer har tillgång till för att avvärja hot och störningar samt de beräknade kostnaderna för åtgärderna. I underrättelsen ska det uppges hur länge störningen eller hotet beräknas pågå. När störningen eller hotet har upphört ska Myndigheten för digitalisering och befolkningsdata dessutom underrätta om detta.

10 §

*Bedömning av överensstämmelse med kraven*

Det att informationssystemet för digital identitet överensstämmer med kraven ska visas med ett intyg som utfärdas av ett sådant bedömningsorgan för informationssäkerhet som avses i 2 § i lagen om bedömningsorgan för informationssäkerhet (1405/2011).

Bedömningsorganet för informationssäkerhet bedömer i enlighet med denna lag och lagen om bedömningsorgan för informationssäkerhet efter ansökan av Myndigheten för digitalisering och befolkningsdata om informationssystemet uppfyller de krav som ställs på det. Som bedömningsgrunder ska kraven i denna lag och de krav som ställs av Myndigheten för digitalisering och befolkningsdata användas.

Bedömningsorganet för informationssäkerhet ska utfärda ett intyg över sin bedömning och ge en tillhörande kontrollrapport. Myndigheten för digitalisering och befolkningsdata ska begära ett utlåtande om bedömningen av Transport- och kommunikationsverket.

Ett intyg från bedömningsorganet för informationssäkerhet är i kraft högst två år. Bedömningsorganet för informationssäkerhet har rätt att trots sekretessbestämmelserna av Myndigheten för digitalisering och befolkningsdata kräva alla de uppgifter som förutsätts för bedömningen och för upprättandet och upprätthållandet av intyget. På utfärdande av intyget tillämpas i övrigt 9 § 3 mom. i lagen om bedömningsorgan för informationssäkerhet.

3 kap.

**Bevis för kärnidentitet**

11 §

*Bevis för kärnidentitet*

Ett bevis för kärnidentitet är ett tekniskt tillförlitligt sätt att visa att den som förfogar över beviset har fått den identitet som kärnidentiteten omfattar registrerad i befolkningsdatasystemet.

Ett bevis för kärnidentitet ska innehålla följande uppgifter:

1) en identifikationskod som avses i 11 a § i lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata,
2) serienummer,
3) det land som utfärdat beviset,
4) bevisets giltighetstid,
5) en öppen nyckel för innehavaren av beviset, och
6) uppgifter om undertecknaren av beviset.

Ett bevis för kärnidentitet ska åtminstone uppfylla kraven för tillitsnivån väsentlig enligt artikel 8.2 b i den förordning som nämns i 6 § 1 mom.

12 §

*Utfärdande av bevis för kärnidentitet*

Myndigheten för digitalisering och befolkningsdata utfärdar ett bevis för kärnidentitet när en person tar i bruk ett e-tjänstverktyg för utlänningar eller en e-legitimation.

Myndigheten för digitalisering och befolkningsdata har rätt att, trots sekretessbestämmelserna, för bestämmande av giltighetstiden för ett bevis för kärnidentitet som ska fogas till en e-legitimation få uppgifter om giltigheten för en persons pass eller identitetskort ur det identitetskortsregister som avses i 31 § i lagen om identitetskort (663/2016) eller det passregister som avses i 29 § i passlagen (671/2006).

En förutsättning för registrering av ett bevis för kärnidentitet är att personen finns registrerad i befolkningsdatasystemet.

13 §

*Register i anslutning till bevis för kärnidentitet*

I registret över bevis för kärnidentitet ska den identifikationskod som avses i 11 a § i lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata samt andra nödvändiga tekniska uppgifter som behövs vid användningen av beviset föras in.

I registret över tekniska plattformar med koppling till personer ska det föras in identifieringsuppgifter som specificerar en person, tekniska uppgifter om en teknisk plattform med koppling till personen, uppgifter om utrustningen och andra nödvändiga uppgifter som behövs för att producera bevis för kärnidentitet.

4 kap.

**E-tjänstverktyg för utlänningar**

14 §

*E-tjänstverktyg för utlänningar*

Myndigheten för digitalisering och befolkningsdata ska producera och tillhandahålla e-tjänstverktyg för utlänningar. E-tjänstverktyget för utlänningar är ett verktyg som är avsett för att visa uppgifter om identitet och andra styrkta uppgifter i anslutning till e-tjänster, och det tillhandahålls med hjälp av applikationen för digital identitet.

15 §

*Utfärdande av e-tjänstverktyg för utlänningar*

Myndigheten för digitalisering och befolkningsdata utfärdar ett e-tjänstverktyg för utlänningar antingen i samband med att personen personligen besöker myndigheten eller i samband med det förfarande för distansregistrering som anges i 9 a § i lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata.

Myndigheten för digitalisering och befolkningsdata ska identifiera en person med hjälp av ett resedokument som avses i den bestämmelse som nämns i 1 mom. och försäkra sig om att upp-

gifter om personen har registrerats i befolkningsdatasystemet och om att personen har en personbeteckning, när ett e-tjänstverktyg för utlänningar utfärdas för personen i samband med att personen uträttar ärenden personligen.

Om ett e-tjänstverktyg för utlänningar utfärdas, får sökanden inte något separat förvaltningsbeslut eller någon besvärsanvisning.

16 §

*Uppgifter som ingår i e-tjänstverktyg för utlänningar*

I samband med att ett e-tjänstverktyg för utlänningar utfärdas ska Myndigheten för digitalisering och befolkningsdata lämna innehavaren av verktyget en kopia av de uppgifter i befolkningsdatasystemet som gäller personen i fråga till hans eller hennes eget förfogande. Följande personuppgifter ska lämnas till innehavaren av verktyget:

1) förnamn,
2) efternamn,
3) födelsetid,
4) personbeteckning,
5) åldersbevis som grundar sig på födelsetiden.

Innan uppgifterna lämnas till personens eget förfogande är Myndigheten för digitalisering och befolkningsdata skyldig att bestyrka dem på ett sådant sätt att den förlitande parten kan försäkra sig om att uppgifterna är riktiga och aktuella genom att kontrollera giltigheten för beviset för kärnidentitet. Myndigheten för digitalisering och befolkningsdata har inte rätt att behandla de bestyrkta uppgifter som har lämnats till innehavaren av ett e-tjänstverktyg för utlänningar efter det att uppgifterna har lämnats till personen i fråga.

17§

*Nyttjande av e-tjänstverktyg för utlänningar*

Om ett e-tjänstverktyg för utlänningar har utfärdats i samband med det förfarande för distansregistrering som anges i 9 a § i lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata, får en förlitande part nyttja verktyget i sina elektroniska tjänster i de fall då det inte i lag förutsätts stark autentisering som avses i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009).

Om Myndigheten för digitalisering och befolkningsdata har identifierat innehavaren av ett e-tjänstverktyg för utlänningar i enlighet med 17 § i den lag som nämns i 1 mom., får den förlitande parten nyttja detta verktyg för stark autentisering med iakttagande av bestämmelserna i den lagen.

18 §

*Visande av bestyrkta uppgifter i anslutning till e-tjänster*

I anslutning till e-tjänster väljer innehavaren av ett e-tjänstverktyg för utlänningar själv vilka bestyrkta uppgifter som han eller hon vill visa den förlitande parten, om inte något annat föreskrivs i någon annan lag. I anslutning till e-tjänsterna ges emellertid alltid information om verktygets tillitsnivå.

19 §

*Registret över e-tjänstverktyg för utlänningar*

Myndigheten för digitalisering och befolkningsdata ska för tillhandahållande och produktion av e-tjänstverktyg för utlänningar föra ett register över sådana verktyg och över verktygens innehavare och giltighet.

20 §

*Giltigheten för e-tjänstverktyg för utlänningar*

Ett e-tjänstverktyg för utlänningar är i kraft högst fem år från utfärdandet.

21 §

*Förnyande av e-tjänstverktyg för utlänningar*

Myndigheten för digitalisering och befolkningsdata kan förlänga giltigheten för ett e-tjänstverktyg för utlänningar på begäran av innehavaren av verktyget. När verktygen förnyas ska kraven i avsnitt 2.2.4 i bilagan till kommissionens genomförandeförordning (EU) 2015/1502 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 uppfyllas.

22 §

*Indragning av e-tjänstverktyg för utlänningar*

Myndigheten för digitalisering och befolkningsdata ska utan dröjsmål dra in ett e-tjänstverktyg för utlänningar på begäran av dess innehavare.

Myndigheten för digitalisering och befolkningsdata kan utan begäran dra in e-tjänstverktyget för utlänningar eller förhindra användningen av det, om myndigheten har skäl att misstänka att verktyget används av någon annan än den det har utfärdats för eller att säkerheten vid användningen av verktyget annars har äventyrats. Myndigheten för digitalisering och befolkningsdata ska utan obefogat dröjsmål underrätta innehavaren av verktyget om att det har dragits in eller användningen av det förhindrats samt om tidpunkten för och orsakerna till detta.

23 §

*Skötsel av uppgifter som gäller utfärdande och indragning av e-tjänstverktyg för utlänningar inom ramen för samservice*

Utöver vad som i 6 § i lagen om samservice inom den offentliga förvaltningen (223/2007) föreskrivs om uppgifter som sköts inom ramen för samservice, får Myndigheten för digitalisering och befolkningsdata överföra biträdande uppgifter som gäller utfärdande och indragning av e-tjänstverktyg för utlänningar och uppdatering av registeruppgifter om sådana verktyg till att skötas inom ramen för samservice. I dessa uppgifter kan det ingå att

1) ta i bruk e-tjänstverktyg,
2) koppla e-tjänstverktyg till en teknisk plattform,
3) dra in e-tjänstverktyg på begäran av innehavaren.

Om samservicens uppdragstagare inte ens efter ytterligare utredning kan aktivera e-tjänstverktyget, koppla innehavarens identitet till verktyget eller på begäran av innehavaren dra in verktyget, ska uppdragstagaren överföra ärendet till Myndigheten för digitalisering och befolkningsdata för behandling.

5 kap.

## Nyttjande av tjänster för digital identitet

24 §

*Tjänsten för hantering av digital identitet*

Myndigheten för digitalisering och befolkningsdata ska producera en tjänst för hantering av digital identitet med hjälp av vilken bevis för kärnidentitet, e-legitimationer och e-tjänstverktyg för utlänningar hanteras.

25 §

*Avläsargränssnitt och kontrollapplikation*

Myndigheten för digitalisering och befolkningsdata producerar och tillhandahåller ett avläsargränssnitt och en kontrollapplikation med vilka identitet och bestyrkta uppgifter kan kontrolleras i e-legitimation vid uträttande av ärenden på plats.

Myndigheten för digitalisering och befolkningsdata kan också godkänna att en kontrollapplikation som produceras av någon annan aktör används för kontroll av identitet och bestyrkta uppgifter vid uträttande av ärenden på plats.

Myndigheten för digitalisering och befolkningsdata meddelar närmare föreskrifter om de krav som ska ställas på de kontrollapplikationer som produceras av andra aktörer. Det ska krävas informationssäkerhet på motsvarande nivå som i fråga om Myndigheten för digitalisering och befolkningsdatas eget avläsargränssnitt.

26 §

*Förlitande parters anmälningsplikt*

En förlitande part som nyttjar i lagen om e-legitimation avsedda e-legitimationer eller e-tjänstverktyg för utlänningar med hjälp av ett direkt tekniskt gränssnitt ska göra en anmälan till Myndigheten för digitalisering och befolkningsdata innan nyttjandet inleds.

I anmälan ska åtminstone följande uppgifter ingå:
1) tjänsteleverantörens namn,
2) tjänsteleverantörens fullständiga kontaktuppgifter,
3) uppgifter om de tillhandahållna tjänster där e-legitimationer eller e-tjänstverktyg för utlänningar kommer att nyttjas.

Den förlitande parten ska utan dröjsmål göra en anmälan om ändringar i de uppgifter som avses i 2 mom.

Myndigheten för digitalisering och befolkningsdata är personuppgiftsansvarig i fråga om de uppgifter som avses i 2 mom., och myndigheten ska föra och offentliggöra en förteckning över de förlitande parter som avses i 1 mom.

27 §

*Skyldigheter för innehavare av applikationen för digital identitet*

En innehavare av applikationen för digital identitet ska använda applikationen omsorgsfullt och får inte överlåta den för att användas av någon annan. Innehavaren är skyldig att ansvara för applikationen efter att ha tagit den i bruk.

Innehavaren av applikationen ska göra en anmälan till Myndigheten för digitalisering och befolkningsdata, om den tekniska plattformen har förkommit eller obehörigen har kommit i någon annans besittning, eller om applikationen obehörigen har använts. Anmälan ska göras utan obefogat dröjsmål efter det att saken har upptäckts. Myndigheten för digitalisering och befolkningsdata ska se till att det är möjligt att när som helst göra en anmälan.

28 §

*Begränsningar av ansvaret vid obehörig användning av applikationen för digital identitet*

En innehavare av applikationen för digital identitet ansvarar för obehörig användning av applikationen endast om

1) innehavaren har överlåtit applikationen till någon obehörig,

2) den tekniska plattformen har förkommit eller obehörigen har kommit i någon annans besittning eller applikationen obehörigen har använts på grund av innehavarens vårdslöshet, som inte är lindrig, eller

3) innehavaren har försummat att utan obefogat dröjsmål efter det att saken har upptäckts göra en anmälan till Myndigheten för digitalisering och befolkningsdata om att den tekniska plattformen har förkommit eller obehörigen har kommit i någon annans besittning eller att applikationen obehörigen har använts.

Innehavaren av applikationen ansvarar dock inte för obehörig användning av applikationen

1) till den del applikationen har använts efter det att innehavaren har gjort en anmälan till Myndigheten för digitalisering och befolkningsdata om att den tekniska plattformen har förkommit eller obehörigen har kommit i någon annans besittning eller att applikationen obehörigen har använts,

2) om innehavaren av applikationen inte utan obefogat dröjsmål efter det att saken har upptäckts har kunnat göra en anmälan om att den tekniska plattformen har förkommit eller obehörigen har kommit i någon annans besittning eller att applikationen obehörigen har använts, på grund av att Myndigheten för digitalisering och befolkningsdata har försummat sin skyldighet enligt 27 § 2 mom. att se till att innehavaren av applikationen har möjlighet att när som helst göra en sådan anmälan.

6 kap.

**Särskilda bestämmelser**

29 §

*Sökande av ändring*

Omprövning får begäras i fråga om beslut av Myndigheten för digitalisering och befolkningsdata som gäller sådant utfärdande av e-tjänstverktyg för utlänningar som avses i 15 § eller sådan indragning av e-tjänstverktyg för utlänningar som avses i 22 § 2 mom. Bestämmelser om begäran om omprövning finns i förvaltningslagen (434/2003).

Bestämmelser om sökande av ändring i förvaltningsdomstol finns i lagen om rättegång i förvaltningsärenden (808/2019).

30 §

*Ikraftträdande*

Denna lag träder i kraft den xx xxxx 20 .

Myndigheten för digitalisering och befolkningsdata ska meddela de föreskrifter som avses i 25 § 3 mom. inom 4 månader från ikraftträdandet av denna lag.

———

**2.**

# Lag

**om e-legitimation**

I enlighet med riksdagens beslut föreskrivs:

1 kap.

**Allmänna bestämmelser**

1 §

*Lagens syfte*

Denna lag innehåller bestämmelser om e-legitimationer som tillhandahålls finska medborgare samt utlänningar som vistas i Finland.

2 §

*Definitioner*

I denna lag avses med
1) *bestyrkta uppgifter* personuppgifter som verifierats av en myndighet på elektronisk väg,
2) *förlitande part* en fysisk eller juridisk person för vilken innehavaren av en e-legitimation styrker sin identitet eller visar bestyrkta uppgifter,
3) *innehavare av en e-legitimation* en person som har tagit i bruk en e-legitimation,
4) *teknisk plattform* en mobil terminal som innehavaren av en e-legitimation förfogar över,
5) *uträttande av ärenden på plats* uträttande av ärenden på så sätt att innehavaren av en e-legitimation och den förlitande parten är närvarande samtidigt och på samma plats och innehavaren av e-legitimationen visar upp sin i identitetshandlingen bestyrkta identitet eller andra bestyrkta uppgifter gällande honom eller henne till den förlitande parten,
6) *bevis för kärnidentitet* ett bevis som avses i 11 § i lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata ( / ).

3 §

*E-legitimation*

En e-legitimation är en identitetshandling som är avsedd för att styrka identiteten och visa bestyrkta uppgifter i anslutning till e-tjänster och vid uträttande av ärenden på plats. Bestämmelser om rätten till en e-legitimation finns i lagen om identitetskort (663/2016) och passlagen (671/2006). E-legitimationer produceras av polisen.

E-legitimationer tillhandahålls med hjälp av en sådan applikation för digital identitet som avses i 2 § 6 punkten i lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata ( / ).

Med avvikelse från vad som i 34 § i passlagen och i 34 § i lagen om identitetskort föreskrivs om avgifter för pass och identitetskort kan det bestämmas att avgiften för e-legitimation underskrider självkostnadsvärdet.

2 kap.

## Uppgifter som ingår i e-legitimationer samt e-legitimationernas giltighet

4 §

*Uppgifter som ingår i e-legitimationer*

Polisen ska lämna innehavaren av en e-legitimation en kopia av de uppgifter i identitetskortsregistret enligt 31 § i lagen om identitetskort eller i passregistret enligt 29 § i passlagen som gäller personen i fråga till hans eller hennes eget förfogande. Följande personuppgifter ska lämnas till innehavaren av en e-legitimation:

1) förnamn,
2) efternamn,
3) födelsetid,
4) uppgift om personens könstillhörighet,
5) uppgift om finskt medborgarskap,
6) personbeteckning eller någon annan identifikationskod på nationell nivå,
7) ansiktsbild som har sparats i pass- eller identitetskortsregistret,
8) giltighetstid för ett giltigt finskt pass eller identitetskort, och
9) e-legitimationens identifieringskod.

Innan uppgifterna lämnas till personens eget förfogande i e-legitimationen är polisen skyldig att verifiera dem på ett sådant sätt att den förlitande parten kan försäkra sig om att uppgifterna är riktiga och aktuella genom att kontrollera certifikatets giltighet. Polisen har inte rätt att behandla de bestyrkta uppgifter som har lämnats till innehavaren av en e-legitimation efter det att uppgifterna har lämnats till personen i fråga.

Certifikat som hänför sig till säkerställandet av äktheten och integriteten hos uppgifterna utfärdas av Myndigheten för digitalisering och befolkningsdata. Dessutom lämnar Myndigheten för digitalisering och befolkningsdata innehavaren av en e-legitimation åldersbevis som grundar sig på födelsetiden.

Uppgifterna i en e-legitimation uppdateras på innehavarens uttryckliga begäran. En förutsättning för användningen av en e-legitimation är emellertid att de uppgifter som ingår i den är aktuella och motsvarar de uppgifter som finns i de register som nämns i 1 mom.

5 §

*Registret över e-legitimationer*

Polisen för ett register över e-legitimationer. I registret får de uppgifter som avses i 4 § 1 mom. 1–9 punkten föras in till den del det är fråga om en person som har rätt att ta i bruk en e-legitimation. I registret förs det dessutom in uppgifter om e-legitimationerna och om deras innehavare och giltighet.

Uppgifterna i registret ska raderas senast tio år efter det att en persons rätt till en e-legitimation har upphört.

6 §

*Ibruktagande av e-legitimationer*

En person kan ta i bruk en e-legitimation i samband med uträttande av ärenden hos en annan behörig passmyndighet eller behörig myndighet som utfärdar identitetskort än utrikesministeriet eller genom användning av stark autentisering enligt 2 § 1 punkten i lagen om stark autentisering

och betrodda elektroniska tjänster (617/2009). Användning av stark autentisering förutsätter att uppgifterna i den tekniska delen på personens giltiga pass eller identitetskort har blivit fjärravlästa och motsvarar uppgifterna enligt den starka autentiseringen.

I samband med ibruktagandet av en e-legitimation kopplar polisen det bevis för kärnidentitet som har utfärdats av Myndigheten för digitalisering och befolkningsdata till den fysiska personen.

7 §

*Ibruktagande av e-legitimationer för minderåriga*

En minderårig kan ta i bruk e-legitimation, om dennes vårdnadshavare ger sitt samtycke.

Bestämmelsen i 1 mom. gäller inte minderåriga som har fyllt 15 år.

8 §

*Giltigheten för e-legitimationer*

En e-legitimation upphör att gälla ett år efter det att den identitetshandling som e-legitimationen grundar sig på har upphört att gälla.

Med identitetshandling avses den handling som har utfärdats i enlighet med passlagen eller lagen om identitetskort och med stöd av vilken en person har rätt till en e-legitimation.

9 §

*Indragning av e-legitimationer*

Polisen drar in en e-legitimation om innehavaren begär det. Om innehavaren av e-legitimationen anmäler att den tekniska plattformen har förkommit eller obehörigen har kommit i någon annans besittning, kan också Myndigheten för digitalisering och befolkningsdata dra in e-legitimationen.

Polisen kan dra in en e-legitimation om den innehåller ett uppenbart fel, om den identitetshandling som e-legitimationen grundar sig på dragits in, om e-legitimationen används av någon annan än innehavaren eller om säkerheten vid användningen av e-legitimationen annars har äventyrats.

3 kap.

**Användning av e-legitimationer**

10 §

*Visande av bestyrkta uppgifter i anslutning till e-tjänster*

I anslutning till e-tjänster väljer innehavaren av en e-legitimation själv vilka bestyrkta uppgifter som han eller hon vill visa den förlitande parten, om inte något annat föreskrivs i någon annan lag.

I anslutning till e-tjänster lämnas emellertid alltid information om den koppling som polisen gjort till personens kärnidentitet.

11 §

*Visande av bestyrkta uppgifter vid uträttande av ärenden på plats*

Vid uträttande av ärenden på plats väljer innehavaren av en e-legitimation själv de bestyrkta uppgifter som han eller hon vill visa den förlitande parten. Vid uträttande av ärenden på plats ska en ansiktsbild emellertid alltid visas.

Den förlitande part som tar emot uppgifterna har rätt att kontrollera giltigheten för det bevis för kärnidentitet som gäller innehavaren av e-legitimationen i det register över bevis för kärnidentitet som avses i 13 § 1 mom. i lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata.

4 kap.

**Särskilda bestämmelser**

12 §

*Sökande av ändring*

Omprövning får begäras i fråga om beslut av polisen som gäller sådan indragning av e-legitimationer som avses i 9 § 2 mom. Bestämmelser om begäran om omprövning finns i förvaltningslagen (434/2003).

Bestämmelser om sökande av ändring i förvaltningsdomstol finns i lagen om rättegång i förvaltningsärenden (808/2019).

13 §

*Ikraftträdande*

Denna lag träder i kraft den xx xxxx 20 .

**3.**

# Lag

**om ändring av lagen om stark autentisering och betrodda elektroniska tjänster**

I enlighet med riksdagens beslut

*ändras* i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) 2 § 1 mom. 1 och 11 punkten, 7 b §, 17 § 2 och 4 mom. och 42 a § 3 mom. 2 punkten,

sådana de lyder, 2 § 1 mom. 1 och 11 punkten, 7 b § och 17 § 2 mom. i lag 1009/2018, 17 § 4 mom. i lag 412/2019 och 42 a § 3 mom. 2 punkten i lag 230/2021, och

*fogas* till 2 § 1 mom., sådant det lyder i lag 1009/2018, nya 12 och 13 punkter, till lagen en ny 12 e §, till 16 §, sådan den lyder i lag 412/2019, ett nytt 3 mom., varvid det nuvarande 3 mom. blir 4 mom., och till lagen nya 16 a och 17 b §

som följer:

2 §

*Definitioner*

I denna lag avses med

1) *stark autentisering* identifiering av en person, av en juridisk person eller av en fysisk person som företräder en juridisk person och verifiering av identifikatorns autenticitet och riktighet genom tillämpning av ett verktyg för digital identitet eller en annan elektronisk metod som motsvarar tillitsnivån väsentlig enligt artikel 8.2 b i EU:s förordning om elektronisk identifiering eller tillitsnivån hög enligt artikel 8.2 c i den förordningen,

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

11) *organ för bedömning av överensstämmelse* ett av Transport- och kommunikationsverket godkänt organ enligt artikel 2.13 i Europaparlamentets och rådets förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93, som är ackrediterat i enlighet med den förordningen,

12) *leverantör av tjänster för digital identitet* den aktör som producerar i lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata ( / ), nedan *lagen om tjänster för digital identitet*, avsedda tjänster för digital identitet och som inte är en sådan leverantör av identifieringstjänster som avses i 3 punkten,

13) *verktyg för digital identitet* en sådan e-legitimation enligt 3 § i lagen om e-legitimation och ett sådant e-tjänstverktyg för utlänningar enligt 14 § i lagen om tjänster för digital identitet vars innehavare har identifierats i enlighet med 17 § i denna lag.

7 b §

*Information om giltighet för pass och identitetskort och för bevis för kärnidentitet i e-legitimation*

Leverantörer av identifieringstjänster har trots sekretessbestämmelserna rätt att via ett gränssnitt eller på något annat sätt i elektronisk form få information ur polisens informationssystem om giltighet för pass och identitetskort som används vid inledande identifiering. Information om giltighet för bevis för kärnidentitet i e-legitimationer som används vid inledande identifiering kan kontrolleras via en kontrollapplikation som avses i 25 § i lagen om tjänster för digital identitet och i det register över bevis för kärnidentitet som avses i 13 § i den lagen.

Leverantörer av identifieringsverktyg är skyldiga att säkerställa den i 1 mom. avsedda informationen om giltigheten för de handlingar som används vid inledande identifiering. Leverantörerna ska säkerställa att ett identifieringsverktyg inte är tillgängligt förrän handlingens giltighet har säkerställts.

12 e §

*Skyldigheter som leverantören av tjänster för digital identitet har i förtroendenätet*

Leverantören av tjänster för digital identitet ska avgiftsfritt erbjuda leverantörer av tjänster för identifieringsförmedling tillträdesrätt till det informationssystem för digital identitet som avses i 4 § i lagen om tjänster för digital identitet, så att leverantörerna kan förmedla de identifieringstransaktioner som grundar sig på ett verktyg för digital identitet till en part som förlitar sig på en elektronisk identifiering. Bestämmelser om den information som ska offentliggöras innan informationssystemet för digital identitet tas i bruk finns i 7 § i den lagen.

Leverantören av tjänster för digital identitet ska bestämma vilka tekniska gränssnitt och standarder som ska användas vid tillhandahållandet av informationssystemet för digital identitet.

16 §

*Anmälningar av leverantörer av identifieringstjänster om hot och störningar som riktas mot verksamheten eller skyddet av uppgifter*

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

Leverantören av identifieringstjänster ska trots sekretessbestämmelserna utan obefogat dröjsmål lämna den information som avses i 1 mom. också till leverantören av tjänster för digital identitet. Dessutom får leverantören av identifieringstjänster trots sekretessbestämmelserna lämna leverantören av tjänster för digital identitet information som avses i 2 mom. och information som hänför sig till utredning av hot och störningar.

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

16 a §

*Anmälningar av leverantören av tjänster för digital identitet om hot och störningar som riktas mot verksamheten eller skyddet av uppgifter*

Leverantören av tjänster för digital identitet ska trots sekretessbestämmelserna utan obefogat dröjsmål till de leverantörer av identifieringstjänster som är medlemmar i förtroendenätet och till Transport- och kommunikationsverket anmäla betydande hot och störningar som riktas mot funktionen hos verktyg för digital identitet, informationssäkerheten, dataskyddet eller användningen av en digital identitet och anmäla avbrott i tjänsterna samt lämna information som hänför sig till utredning av hot och störningar. I anmälan ska det redogöras för de åtgärder som olika aktörer har tillgång till för att avvärja hot och störningar samt de beräknade kostnaderna för åtgärderna.

En leverantör av identifieringstjänster och leverantören av tjänster för digital identitet får använda sådana uppgifter om varandra som de fått med stöd av 1 mom. och 16 § 3 mom. endast för det ändamål för vilket uppgifterna har lämnats. Uppgifterna får behandlas endast av den som arbetar hos eller för en leverantör av identifieringstjänster och som nödvändigt behöver uppgifterna i sitt arbete.

17 §

*Identifiering av en fysisk person som ansöker om ett identifieringsverktyg*

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

Dokument som godkänns vid inledande identifiering, när identifieringen endast sker utifrån en identitetshandling som utfärdats av en myndighet, är ett giltigt pass eller identitetskort som har utfärdats av en myndighet i en medlemsstat inom Europeiska ekonomiska samarbetsområdet, i Schweiz eller i San Marino. En leverantör av identifieringsverktyg som så önskar kan också vid kontrollen av identiteten använda ett giltigt pass som har utfärdats av en myndighet i någon annan stat eller en e-legitimation som avses i 3 § i lagen om e-legitimation.

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

En leverantör av identifieringsverktyg ska göra det möjligt för en annan leverantör av identifieringsverktyg eller för leverantören av tjänster för digital identitet att använda ett identifieringsverktyg för stark autentisering som beviljats av den förstnämnda för inledande identifiering vid ansökan om ett identifieringsverktyg för stark autentisering eller ett verktyg för digital identitet på motsvarande eller lägre tillitsnivå. Vad som i 12 a och 12 b § föreskrivs om överlåtelse av tillträdesrätt till identifieringstjänsten och offentliggörande av leveransvillkoren tillämpas också på i detta moment avsedd användning av identifieringsverktyg vid inledande identifiering.

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

17 b §

*E-legitimation vid inledande identifiering*

Leverantören av tjänster för digital identitet ska göra det möjligt för en leverantör av identifieringsverktyg att avgiftsfritt använda en e-legitimation enligt 3 § i lagen om e-legitimation för inledande identifiering vid ansökan om ett identifieringsverktyg för stark autentisering på motsvarande eller lägre tillitsnivå. Vad som i 7 § i lagen om tjänster för digital identitet föreskrivs om den information som ska offentliggöras innan informationssystemet för digital identitet tas i bruk tillämpas också på användning av e-legitimation vid inledande identifiering.

42 a §

*Transport- och kommunikationsverkets uppgifter*

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

Transport- och kommunikationsverket ska i enlighet med EU:s förordning om elektronisk identifiering

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

2) anmäla de system för elektronisk identifiering som anmälts i enlighet med 10 § till Europeiska kommissionen i enlighet med artiklarna 7–10 i förordningen,

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

———

Denna lag träder i kraft den xx xxxx 20 . Bestämmelserna i 7 b § 2 mom. tillämpas dock först från och med den 1 december 2023.

———

**4.**

# Lag

**om ändring av 16 och 22 § i lagen om behandling av personuppgifter i polisens verksamhet**

I enlighet med riksdagens beslut

*ändras* i lagen om behandling av personuppgifter i polisens verksamhet (616/2019) 16 § 1 mom. 15 punkten och 22 § 1 mom. 17 punkten samt

*fogas* till 16 § 1 mom., sådant det lyder delvis ändrat i lagarna 1162/2019, 632/2020 och 1308/2021, en ny 16 punkt och till 22 § 1 mom., sådant det lyder delvis ändrat i lag 632/2020, en ny 18 punkt som följer:

16 §

*Polisens rätt att få uppgifter ur vissa register och informationssystem*

Utöver vad som föreskrivs annanstans i lag har polisen trots sekretessbestämmelserna rätt att ur vissa register genom en teknisk anslutning eller som en datamängd få information för att utföra sina uppgifter och föra sina personregister, på det sätt det avtalas om tillvägagångssättet med den personuppgiftsansvarige, enligt följande:

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

15) av samfund och sammanslutningar uppgifter ur register som gäller passagerare och fordons personal, för förhindrande, avslöjande och utredning av brott och förande av brott till åtalsprövning samt för att nå efterlysta personer; bestämmelser om rätten att få uppgifter ur flygtrafikens PNR-uppgifter finns i lagen om användning av flygpassageraruppgifter för bekämpning av terroristbrott och grov brottslighet (657/2019),

16) ur register som avses i lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata ( / ) sådana uppgifter som är nödvändiga för produktion av e-legitimationer samt uppgifter för utredning av misstänkt missbruk av personuppgifter, identitetsstölder eller andra motsvarande brott och för förebyggande av sådana brott.

22 §

*Övrigt utlämnande av personuppgifter till myndigheter*

Polisen får trots sekretessbestämmelserna genom en teknisk anslutning eller som en datamängd lämna ut sådana personuppgifter som avses i 5–8, 11 och 12 § för en uppgift som myndigheten har enligt lag, enligt följande:

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

17) till Försvarsmakten, Tullen, Gränsbevakningsväsendet och Brottspåföljdsmyndigheten för bedömning av om en hos dessa anställd med rätt att bära skjutvapen i sina tjänste-, arbets- eller tjänstgöringsuppdrag är lämplig att bära skjutvapen,

18) till Myndigheten för digitalisering och befolkningsdata sådana personuppgifter som avses i 11 och 12 § för produktion och administration av det informationssystem för digital identitet och de bevis för kärnidentitet som avses i lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata.

———

Denna lag träder i kraft den xx xxxx 20 .

_____

**5.**

# Lag

**om ändring av lagen om identitetskort**

I enlighet med riksdagens beslut
*fogas* till lagen om identitetskort (663/2016) en ny 1 a § som följer:

1 a §

*E-legitimation*

Ett identitetskort ger rätt att ta i bruk en e-legitimation som avses i lagen om e-legitimation ( / ).
Vad som föreskrivs i 1 mom. gäller inte ett temporärt identitetskort eller ett sådant identitetskort för minderårig som har utfärdats för en person som är under 15 år.

_____

Denna lag träder i kraft den xx xxxx 20 .

Rätten att ta i bruk en e-legitimation i enlighet med 1 a § i denna lag tillämpas även på giltiga identitetskort som har utfärdats före ikraftträdandet av denna lag.

_____

**6.**

# Lag

**om ändring av passlagen**

I enlighet med riksdagens beslut
*fogas* till passlagen (671/2006) en ny 3 d § som följer:

3 d §

*E-legitimation*

Ett pass ger rätt att ta i bruk en e-legitimation som avses i lagen om e-legitimation ( / ).
Vad som föreskrivs i 1 mom. gäller inte ett tillfälligt pass eller ett nödpass.

———

Denna lag träder i kraft den xx xxxx 20 .

Rätten att ta i bruk en e-legitimation i enlighet med 3 d § i denna lag tillämpas även på giltiga pass som har utfärdats före ikraftträdandet av denna lag.

———

**7.**

# Lag

**om ändring av lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata**

I enlighet med riksdagens beslut

*fogas* till lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata (661/2009) ett nytt 6 b kap. som följer:

6 b kap.

**Identifieringsverktyg för fysiska personer**

*69 e §*

*Identifieringsverktyg för fysiska personer*

Myndigheten för digitalisering och befolkningsdata ska bevilja sådana identifieringsverktyg för elektronisk identifiering av fysiska personer som motsvarar tillitsnivån väsentlig enligt artikel 8.2 b i EU:s förordning om elektronisk identifiering eller tillitsnivån hög enligt artikel 8.2 c i den förordningen.

Ett identifieringsverktyg för fysiska personer är ett fysiskt verktyg som kan användas utan mobil terminal och chipkort.

Myndigheten för digitalisering och befolkningsdata tillhandahåller identifieringsverktygen för fysiska personer i form av identifieringsverktyg i enlighet med EU:s förordning om elektronisk identifiering, för att användas via den stödtjänst som avses i 3 § 1 mom. 4 punkten i lagen om stödtjänster.

*69 f §*

*Registret över identifieringsverktyg för fysiska personer*

Myndigheten för digitalisering och befolkningsdata ska för tillhandahållande och produktion av identifieringsverktyg för fysiska personer föra ett register över identifieringsverktygen och över verktygens innehavare. I registret får följande uppgifter om innehavare av identifieringsverktyg registreras:

1) de personuppgifter som ingår i den av en myndighet utfärdade identitetshandling som använts för kontroll av identiteten samt uppgifter som specificerar identitetshandlingen,

2) de personuppgifter som förmedlas i samband med den elektroniska identifieringsmetod som använts för kontroll av identiteten samt uppgifter om den elektroniska identifieringsmetoden,

3) en identifikationskod som avses i 11 a §,

4) en identifieringskod för identifieringsverktyget,

5) kontaktuppgifter,

6) andra än i 1–5 punkten avsedda uppgifter som behövs för tillhandahållandet av identifieringsverktyget.

Bestämmelser om behandling av personuppgifter inom tjänsteproduktionen i fråga om identifieringsverktyg för fysiska personer, om krav som gäller identifieringsverktyget och användningen av det och om styrningen av tjänsteproduktionen finns i 3–5 kap. i lagen om stödtjänster.

69 g §

*Styrkande av sökandens identitet*

Myndigheten för digitalisering och befolkningsdata beviljar på ansökan ett identifieringsverktyg till en fysisk person.

Vid inledande identifiering ska identifieringen av en fysisk person göras personligen eller elektroniskt på ett sådant sätt att de krav uppfylls som gäller för tillitsnivån väsentlig eller hög enligt avsnitt 2.1.2 i bilagan till kommissionens genomförandeförordning (EU) 2015/1502 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. Kontrollen av en persons identitet kan grunda sig på en identitetshandling som utfärdats av en myndighet eller på stark autentisering enligt 2 § 1 punkten i lagen om stark autentisering och betrodda elektroniska tjänster.

*69 h §*

*Skötsel av uppgifter som gäller beviljande av identifieringsverktyg inom ramen för samservice*

Utöver vad som i 6 § i samservicelagen föreskrivs om uppgifter som sköts inom ramen för samservice får Myndigheten för digitalisering och befolkningsdata överföra biträdande uppgifter som gäller beviljande av identifieringsverktyg till att skötas inom ramen för samservice. Dessa uppgifter kan omfatta verifiering av identiteten hos dem som ansöker om identifieringsverktyg och hos innehavare av identifieringsverktyg samt rådgivnings- och stödtjänster i samband med ansökan om identifieringsverktyg.

Om samservicens uppdragstagare inte ens efter ytterligare utredning kan verifiera sökandens identitet, ska uppdragstagaren överföra ärendet till Myndigheten för digitalisering och befolkningsdata för behandling.

69 i §

*Information om giltighet för pass och identitetskort*

Myndigheten för digitalisering och befolkningsdata har trots sekretessbestämmelserna rätt att via ett tekniskt gränssnitt eller på något annat sätt i elektronisk form få information ur polisens informationssystem om giltighet för pass och identitetskort som används vid inledande identifiering.

69 j §

*Skyldighet för Myndigheten för digitalisering och befolkningsdata att lämna uppgifter*

Myndigheten för digitalisering och befolkningsdata ska innan ett identifieringsverktyg beviljas informera sökanden om

1) användningen av identifieringsverktyget,
2) parternas rättigheter och skyldigheter,
3) eventuella ansvarsbegränsningar, och
4) eventuella andra än i 1–3 punkten avsedda villkor för användning av identifieringsverktyget.

De uppgifter som avses i 1 mom. ska lämnas skriftligen eller elektroniskt så att den som ansöker om ett identifieringsverktyg kan spara och återge dem i oförändrad form.

69 k §

*Rätten för Myndigheten för digitalisering och befolkningsdata att återkalla eller förhindra användning av identifieringsverktyg*

Myndigheten för digitalisering och befolkningsdata kan återkalla eller förhindra användningen av ett identifieringsverktyg, om

1) det finns skäl att misstänka att identifieringsverktyget används av någon annan än den det har beviljats till,

2) identifieringsverktyget innehåller ett uppenbart fel,

3) det finns skäl att misstänka att säkerheten vid användningen av identifieringsverktyget har äventyrats,

4) innehavaren av identifieringsverktyget använder det på ett sätt som väsentligt strider mot villkoren för användningen,

5) innehavaren av identifieringsverktyget har avlidit.

Myndigheten för digitalisering och befolkningsdata ska så snart som möjligt underrätta innehavaren av identifieringsverktyget om att verktyget har återkallats eller användningen av det förhindrats samt om tidpunkten för och orsakerna till detta.

Myndigheten för digitalisering och befolkningsdata ska erbjuda en ny möjlighet att använda identifieringsverktyget eller tillhandahålla innehavaren ett nytt verktyg omedelbart efter det att en sådan orsak som avses 1 mom. 2 eller 3 punkten inte längre föreligger.

69 l §

*Skyldigheter för innehavare av identifieringsverktyg för fysiska personer*

Innehavaren av ett identifieringsverktyg för fysiska personer ska använda verktyget i enlighet med villkoren för användningen. Innehavaren ska förvara identifieringsverktyget omsorgsfullt. Innehavaren är skyldig att ansvara för verktyget efter att ha tagit emot det.

Innehavaren av ett identifieringsverktyg får inte överlåta verktyget för att användas av någon annan.

Innehavaren av ett identifieringsverktyg ska göra en anmälan till Myndigheten för digitalisering och befolkningsdata, om verktyget obehörigen har kommit i någon annans besittning eller obehörigen har använts. Anmälan ska göras utan obefogat dröjsmål efter det att saken har upptäckts.

Myndigheten för digitalisering och befolkningsdata ska se till att det är möjligt att när som helst göra en anmälan enligt 3 mom. Myndigheten ska återkalla identifieringsverktyget eller förhindra användningen av det utan dröjsmål efter det att anmälan har mottagits. Innehavaren av ett identifieringsverktyg ansvarar inte för obehörig användning av verktyget efter att ha gjort anmälan till Myndigheten för digitalisering och befolkningsdata.

69 m §

*Sökande av ändring*

Omprövning får begäras i fråga om sådana beslut av Myndigheten för digitalisering och befolkningsdata som gäller beviljande av identifieringsverktyg för fysiska personer i enlighet med 69 e § eller återkallelse av identifieringsverktyg för fysiska personer i enlighet med 69 k §. Bestämmelser om begäran om omprövning finns i förvaltningslagen.

Bestämmelser om sökande av ändring i förvaltningsdomstol finns i lagen om rättegång i förvaltningsärenden (808/2019).

---

Denna lag träder i kraft den xx xxxx 20 .

---

**8.**

# Lag

**om ändring av 3 och 9 § i lagen om förvaltningens gemensamma stödtjänster för e-tjänster**

I enlighet med riksdagens beslut

*ändras* i lagen om förvaltningens gemensamma stödtjänster för e-tjänster (571/2016) 3 § 1 mom. 4 punkten och 9 § 1 punkten, av dem 9 § 1 punkten sådan den lyder i lag 1174/2019, som följer:

3 §

*Stödtjänster*

De gemensamma stödtjänsterna för e-tjänster omfattar

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

4) en sådan tjänst för identifiering av fysiska personer som identifierar en fysisk person som använder den offentliga förvaltningens e-tjänster med hjälp av en tjänst som tillhandahålls av en sådan leverantör av identifieringstjänster som avses i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) eller med hjälp av en tjänst som avses i 6 b kap. i lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata (661/2009), administrerar identifieringstransaktionen och till användarorganisationen lämnar ut identifieringsuppgifter om en person ur befolkningsdatasystemet,

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

9 §

*Informationskällor som regelbundet utnyttjas inom tjänsteproduktionen*

För att fullgöra sina uppgifter enligt denna lag har Myndigheten för digitalisering och befolkningsdata, med iakttagande av detta kapitel, rätt att behandla i denna paragraf avsedda uppgifter som införts i följande informationssystem:

1) i fråga om befolkningsdatasystemet enligt lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata, uppgifter om personers namn, personbeteckning, elektroniska kommunikationskod, medborgarskap, kontaktspråk, modersmål, dödsdag, intressebevakning, begränsning av handlingsbehörigheten, intressebevakningsfullmakt och vårdnad om barn samt kontaktuppgifter och uppgifter om spärrmarkering,

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

———

Denna lag träder i kraft den xx xxxx 20 .

———

Helsingfors den 15 september 2022

**Statsminister**

**Sanna Marin**

kommunminister Sirpa Paatero

**3.**

# Lag

**om ändring av lagen om stark autentisering och betrodda elektroniska tjänster**

I enlighet med riksdagens beslut

*ändras* i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) 2 § 1 mom. 1 och 11 punkten, 7 b §, 17 § 2 och 4 mom. och 42 a § 3 mom. 2 punkten,

sådana de lyder, 2 § 1 mom. 1 och 11 punkten, 7 b § och 17 § 2 mom. i lag 1009/2018, 17 § 4 mom. i lag 412/2019 och 42 a § 3 mom. 2 punkten i lag 230/2021, och

*fogas* till 2 § 1 mom., sådant det lyder i lag 1009/2018, nya 12 och 13 punkter, till lagen en ny 12 e §, till 16 §, sådan den lyder i lag 412/2019, ett nytt 3 mom., varvid det nuvarande 3 mom. blir 4 mom., och till lagen nya 16 a och 17 b §

som följer:

| *Gällande lydelse* | *Föreslagen lydelse* |
|---|---|
| 2 § | 2 § |
| *Definitioner* | *Definitioner* |
| I denna lag avses med | I denna lag avses med |
| 1) *stark autentisering* identifiering av en person, av en juridisk person eller av en fysisk person som företräder en juridisk person och verifiering av identifikatorns autenticitet och riktighet genom tillämpning av en elektronisk metod som motsvarar tillitsnivån väsentlig enligt artikel 8.2 b i EU:s förordning om elektronisk identifiering eller tillitsnivån hög enligt artikel 8.2 c i den förordningen, | 1) *stark autentisering* identifiering av en person, av en juridisk person eller av en fysisk person som företräder en juridisk person och verifiering av identifikatorns autenticitet och riktighet genom tillämpning *av ett verktyg för digital identitet eller en annan* elektronisk metod som motsvarar tillitsnivån väsentlig enligt artikel 8.2 b i EU:s förordning om elektronisk identifiering eller tillitsnivån hög enligt artikel 8.2 c i den förordningen, |
| — — — — — — — — — — — — — — | — — — — — — — — — — — — — — |
| 11) *organ för bedömning av överensstämmelse* ett av Transport- och kommunikationsverket godkänt organ enligt artikel 2.13 i Europaparlamentets och rådets förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93, som är ackrediterat i enlighet med den förordningen. | 11) *organ för bedömning av överensstämmelse* ett av Transport- och kommunikationsverket godkänt organ enligt artikel 2.13 i Europaparlamentets och rådets förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93, som är ackrediterat i enlighet med den förordningen, |
| | *12)* ***leverantör av tjänster för digital identitet*** *den aktör som producerar i lagen om de tjänster för digital identitet som tillhandahålls* |

| *Gällande lydelse* | *Föreslagen lydelse* |
| --- | --- |
| | *av Myndigheten för digitalisering och befolkningsdata ( / ), nedan **lagen om tjänster för digital identitet**, avsedda tjänster för digital identitet och som inte är en sådan leverantör av identifieringstjänster som avses i 3 punkten,* |
| | *13) **verktyg för digital identitet** en sådan e-legitimation enligt 3 § i lagen om e-legitimation och ett sådant e-tjänstverktyg för utlänningar enligt 14 § i lagen om tjänster för digital identitet vars innehavare har identifierats i enlighet med 17 § i denna lag.* |
| 7 b § | 7 b § |
| *Information om giltighet för pass eller identitetskort* | *Information om giltighet för pass och identitetskort **och för bevis för kärnidentitet i e-legitimation*** |
| Leverantörer av identifieringstjänster har trots sekretessbestämmelserna rätt att via ett gränssnitt eller annars i elektronisk form få information ur polisens informationssystem om giltighet för pass eller identitetskort som används vid inledande identifiering. | Leverantörer av identifieringstjänster har trots sekretessbestämmelserna rätt att via ett gränssnitt eller på något annat sätt i elektronisk form få information ur polisens informationssystem om giltighet för pass och identitetskort som används vid inledande identifiering. *Information om giltighet för bevis för kärnidentitet i e-legitimationer som används vid inledande identifiering kan kontrolleras via en kontrollapplikation som avses i 25 § i lagen om tjänster för digital identitet och i det register över bevis för kärnidentitet som avses i 13 § i den lagen.* |
| | *Leverantörer av identifieringsverktyg är skyldiga att säkerställa den i 1 mom. avsedda informationen om giltigheten för de handlingar som används vid inledande identifiering. Leverantörerna ska säkerställa att ett identifieringsverktyg inte är tillgängligt förrän handlingens giltighet har säkerställts.* |
| | *12 e §* |
| | *Skyldigheter som leverantören av tjänster för digital identitet har i förtroendenätet* |
| | *Leverantören av tjänster för digital identitet ska avgiftsfritt erbjuda leverantörer av tjänster för identifieringsförmedling tillträdesrätt till det informationssystem för digital identitet som avses i 4 § i lagen om tjänster för digital* |

| Gällande lydelse | Föreslagen lydelse |
| --- | --- |
| | *identitet, så att leverantörerna kan förmedla de identifieringstransaktioner som grundar sig på ett verktyg för digital identitet till en part som förlitar sig på en elektronisk identifiering. Bestämmelser om den information som ska offentliggöras innan informationssystemet för digital identitet tas i bruk finns i 7 § i den lagen.*<br>Leverantören av tjänster för digital identitet ska bestämma vilka tekniska gränssnitt och standarder som ska användas vid tillhandahållandet av informationssystemet för digital identitet. |
| 16 § | 16 § |
| *Anmälningar av leverantörer av identifieringstjänster om hot och störningar som riktas mot verksamheten eller skyddet av uppgifter* | *Anmälningar av leverantörer av identifieringstjänster om hot och störningar som riktas mot verksamheten eller skyddet av uppgifter* |
| — — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — — |
| Leverantören av identifieringstjänster får trots sekretessbestämmelserna underrätta alla medlemmar i förtroendenätet om hot och störningar som avses i 1 mom. samt om tjänsteleverantörer som skäligen kan misstänkas för att eftersträva orättmätig ekonomisk vinning, lämna betydelsefull osann eller vilseledande information eller behandla personuppgifter på ett olagligt sätt. | *Leverantören av identifieringstjänster ska trots sekretessbestämmelserna utan obefogat dröjsmål lämna den information som avses i 1 mom. också till leverantören av tjänster för digital identitet. Dessutom får leverantören av identifieringstjänster trots sekretessbestämmelserna lämna leverantören av tjänster för digital identitet information som avses i 2 mom. och information som hänför sig till utredning av hot och störningar.* |
| — — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — — |
| | *16 a §* |
| | *Anmälningar av leverantören av tjänster för digital identitet om hot och störningar som riktas mot verksamheten eller skyddet av uppgifter* |
| | *Leverantören av tjänster för digital identitet ska trots sekretessbestämmelserna utan obefogat dröjsmål till de leverantörer av identifieringstjänster som är medlemmar i förtroendenätet och till Transport- och kommunikationsverket anmäla betydande hot och störningar som riktas mot funktionen hos verktyg för digital identitet, informationssäkerheten, dataskyddet eller användningen av en digital* |

| *Gällande lydelse* | *Föreslagen lydelse* |
| --- | --- |
| | *identitet och anmäla avbrott i tjänsterna samt lämna information som hänför sig till utredning av hot och störningar. I anmälan ska det redogöras för de åtgärder som olika aktörer har tillgång till för att avvärja hot och störningar samt de beräknade kostnaderna för åtgärderna.* |
| | *En leverantör av identifieringstjänster och leverantören av tjänster för digital identitet får använda sådana uppgifter om varandra som de fått med stöd av 1 mom. och 16 § 3 mom. endast för det ändamål för vilket uppgifterna har lämnats. Uppgifterna får behandlas endast av den som arbetar hos eller för en leverantör av identifieringstjänster och som nödvändigt behöver uppgifterna i sitt arbete.* |
| 17 § | 17 § |
| *Identifiering av en fysisk person som ansöker om ett identifieringsverktyg* | *Identifiering av en fysisk person som ansöker om ett identifieringsverktyg* |
| — — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — — |
| Dokument som godkänns vid inledande identifiering, när identifieringen endast sker utifrån en identitetshandling som utfärdats av en myndighet, är ett giltigt pass eller identitetskort som har utfärdats av en myndighet i en medlemsstat inom Europeiska ekonomiska samarbetsområdet, i Schweiz eller i San Marino. En leverantör av identifieringsverktyg som så önskar kan också vid kontrollen av identiteten använda ett giltigt pass som har utfärdats av en myndighet i någon annan stat. | Dokument som godkänns vid inledande identifiering, när identifieringen endast sker utifrån en identitetshandling som utfärdats av en myndighet, är ett giltigt pass eller identitetskort som har utfärdats av en myndighet i en medlemsstat inom Europeiska ekonomiska samarbetsområdet, i Schweiz eller i San Marino. En leverantör av identifieringsverktyg som så önskar kan också vid kontrollen av identiteten använda ett giltigt pass som har utfärdats av en myndighet i någon annan stat *eller en e-legitimation som avses i 3 § i lagen om e-legitimation*. |
| — — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — — |
| En leverantör av identifieringsverktyg ska göra det möjligt för en annan leverantör av identifieringsverktyg att använda ett identifieringsverktyg för stark autentisering som beviljats av den förstnämnda för inledande identifiering vid ansökan om ett identifieringsverktyg för stark autentisering på motsvarande eller lägre tillitsnivå. Vad som i 12 a och 12 b § föreskrivs om överlåtelse av tillträdesrätt till identifieringstjänsten och publicering av leveransvillkoren tillämpas också på i detta moment avsedd användning av identifieringsverktyg vid inledande identifiering. | En leverantör av identifieringsverktyg ska göra det möjligt för en annan leverantör av identifieringsverktyg *eller för leverantören av tjänster för digital identitet* att använda ett identifieringsverktyg för stark autentisering som beviljats av den förstnämnda för inledande identifiering vid ansökan om ett identifieringsverktyg för stark autentisering *eller ett verktyg för digital identitet* på motsvarande eller lägre tillitsnivå. Vad som i 12 a och 12 b § föreskrivs om överlåtelse av tillträdesrätt till identifieringstjänsten och offentliggörande av leveransvillkoren tillämpas också på i detta |

| *Gällande lydelse* | *Föreslagen lydelse* |
| --- | --- |
| — — — — — — — — — — — — — — | moment avsedd användning av identifieringsverktyg vid inledande identifiering. |
| | — — — — — — — — — — — — — — |
| | *17 b §* |
| | *E-legitimation vid inledande identifiering* |
| | *Leverantören av tjänster för digital identitet ska göra det möjligt för en leverantör av identifieringsverktyg att avgiftsfritt använda en e-legitimation enligt 3 § i lagen om e-legitimation för inledande identifiering vid ansökan om ett identifieringsverktyg för stark autentisering på motsvarande eller lägre tillitsnivå. Vad som i 7 § i lagen om tjänster för digital identitet föreskrivs om den information som ska offentliggöras innan informationssystemet för digital identitet tas i bruk tillämpas också på användning av e-legitimation vid inledande identifiering.* |
| 42 a § | 42 a § |
| *Transport- och kommunikationsverkets uppgifter* | *Transport- och kommunikationsverkets uppgifter* |
| — — — — — — — — — — — — — — | — — — — — — — — — — — — — — |
| Transport- och kommunikationsverket ska i enlighet med EU:s förordning om elektronisk identifiering | Transport- och kommunikationsverket ska i enlighet med EU:s förordning om elektronisk identifiering |
| — — — — — — — — — — — — — — | — — — — — — — — — — — — — — |
| 2) anmäla system för elektronisk identifiering till Europeiska kommissionen i enlighet med artiklarna 7–10 i förordningen, | 2) anmäla *de* system för elektronisk identifiering *som anmälts i enlighet med 10 §* till Europeiska kommissionen i enlighet med artiklarna 7–10 i förordningen, |
| — — — — — — — — — — — — — — | — — — — — — — — — — — — — — |
| | ———— |
| | *Denna lag träder i kraft den xx xxxx 20 . Bestämmelserna i 7 b § 2 mom. tillämpas dock först från och med den 1 december 2023.* |
| | ———— |

**4.**

# Lag

**om ändring av 16 och 22 § i lagen om behandling av personuppgifter i polisens verksamhet**

I enlighet med riksdagens beslut

*ändras* i lagen om behandling av personuppgifter i polisens verksamhet (616/2019) 16 § 1 mom. 15 punkten och 22 § 1 mom. 17 punkten samt

*fogas* till 16 § 1 mom., sådant det lyder delvis ändrat i lagarna 1162/2019, 632/2020 och 1308/2021, en ny 16 punkt och till 22 § 1 mom., sådant det lyder delvis ändrat i lag 632/2020, en ny 18 punkt som följer:

| *Gällande lydelse* | *Föreslagen lydelse* |
|---|---|
| 16 § | 16 § |
| *Polisens rätt att få uppgifter ur vissa register och informationssystem* | *Polisens rätt att få uppgifter ur vissa register och informationssystem* |
| Utöver vad som föreskrivs annanstans i lag har polisen trots sekretessbestämmelserna rätt att ur vissa register genom en teknisk anslutning eller som en datamängd få information för att utföra sina uppgifter och föra sina personregister, på det sätt det avtalas om tillvägagångssättet med den personuppgiftsansvarige, enligt följande: | Utöver vad som föreskrivs annanstans i lag har polisen trots sekretessbestämmelserna rätt att ur vissa register genom en teknisk anslutning eller som en datamängd få information för att utföra sina uppgifter och föra sina personregister, på det sätt det avtalas om tillvägagångssättet med den personuppgiftsansvarige, enligt följande: |
| — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — |
| 15) av samfund och sammanslutningar uppgifter ur register som gäller passagerare och fordons personal, för förhindrande, avslöjande och utredning av brott och förande av brott till åtalsprövning samt för att nå efterlysta personer; bestämmelser om rätten att få uppgifter ur flygtrafikens PNR-uppgifter finns i lagen om användning av flygpassageraruppgifter för bekämpning av terroristbrott och grov brottslighet. | 15) av samfund och sammanslutningar uppgifter ur register som gäller passagerare och fordons personal, för förhindrande, avslöjande och utredning av brott och förande av brott till åtalsprövning samt för att nå efterlysta personer; bestämmelser om rätten att få uppgifter ur flygtrafikens PNR-uppgifter finns i lagen om användning av flygpassageraruppgifter för bekämpning av terroristbrott och grov brottslighet (657/2019), |
| | *16) ur register som avses i lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata ( / ) sådana uppgifter som är nödvändiga för produktion av e-legitimationer samt uppgifter för utredning av misstänkt missbruk av personuppgifter, identitetsstölder eller andra motsvarande brott och för förebyggande av sådana brott.* |

| *Gällande lydelse* | *Föreslagen lydelse* |
| --- | --- |
| 22 § | 22 § |
| *Övrigt utlämnande av personuppgifter till myndigheter* | *Övrigt utlämnande av personuppgifter till myndigheter* |
| Polisen får trots sekretessbestämmelserna genom en teknisk anslutning eller som en datamängd lämna ut sådana personuppgifter som avses i 5–8, 11 och 12 § för en uppgift som myndigheten har enligt lag, enligt följande: | Polisen får trots sekretessbestämmelserna genom en teknisk anslutning eller som en datamängd lämna ut sådana personuppgifter som avses i 5–8, 11 och 12 § för en uppgift som myndigheten har enligt lag, enligt följande: |
| — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — |
| 17) till Försvarsmakten, Tullen, Gränsbevakningsväsendet och Brottspåföljdsmyndigheten för bedömning av om en hos dessa anställd med rätt att bära skjutvapen i sina tjänste- eller arbetsuppdrag är lämplig att bära skjutvapen. | 17) till Försvarsmakten, Tullen, Gränsbevakningsväsendet och Brottspåföljdsmyndigheten för bedömning av om en hos dessa anställd med rätt att bära skjutvapen i sina tjänste-, arbets- eller tjänstgöringsuppdrag är lämplig att bära skjutvapen, |
| | *18) till Myndigheten för digitalisering och befolkningsdata sådana personuppgifter som avses i 11 och 12 § för produktion och administration av det informationssystem för digital identitet och de bevis för kärnidentitet som avses i lagen om de tjänster för digital identitet som tillhandahålls av Myndigheten för digitalisering och befolkningsdata.* |
| | ———— |
| | *Denna lag träder i kraft den xx xxxx 20 .* |
| | ———— |

**5.**

# Lag

**om ändring av lagen om identitetskort**

I enlighet med riksdagens beslut
*fogas* till lagen om identitetskort (663/2016) en ny 1 a § som följer:

| *Gällande lydelse* | *Föreslagen lydelse* |
| --- | --- |
| | *1 a §* |
| | *E-legitimation* |
| | *Ett identitetskort ger rätt att ta i bruk en e-legitimation som avses i lagen om e-legitimation ( / ).* |
| | *Vad som föreskrivs i 1 mom. gäller inte ett temporärt identitetskort eller ett sådant identitetskort för minderårig som har utfärdats för en person som är under 15 år.* |
| | *Denna lag träder i kraft den xx xxxx 20 .* |
| | *Rätten att ta i bruk en e-legitimation i enlighet med 1 a § i denna lag tillämpas även på giltiga identitetskort som har utfärdats före ikraftträdandet av denna lag.* |

**6.**

# Lag

**om ändring av passlagen**

I enlighet med riksdagens beslut
*fogas* till passlagen (671/2006) en ny 3 d § som följer:

| *Gällande lydelse* | *Föreslagen lydelse* |
| --- | --- |
| | *3 d §* |
| | *E-legitimation* |
| | *Ett pass ger rätt att ta i bruk en e-legitimation som avses i lagen om e-legitimation ( / ).* |
| | *Vad som föreskrivs i 1 mom. gäller inte ett tillfälligt pass eller ett nödpass.* |
| | _____ |
| | *Denna lag träder i kraft den xx xxxx 20 .* |
| | *Rätten att ta i bruk en e-legitimation i enlighet med 3 d § i denna lag tillämpas även på giltiga pass som har utfärdats före ikraftträdandet av denna lag.* |
| | _____ |

**7.**

# Lag

**om ändring av lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata**

I enlighet med riksdagens beslut

*fogas* till lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata (661/2009) ett nytt 6 b kap. som följer:

| *Gällande lydelse* | *Föreslagen lydelse* |
|---|---|
| | *6 b kap.* |
| | ***Identifieringsverktyg för fysiska personer*** |
| | *69 e §* |
| | *Identifieringsverktyg för fysiska personer* |
| | *Myndigheten för digitalisering och befolkningsdata ska bevilja sådana identifieringsverktyg för elektronisk identifiering av fysiska personer som motsvarar tillitsnivån väsentlig enligt artikel 8.2 b i EU:s förordning om elektronisk identifiering eller tillitsnivån hög enligt artikel 8.2 c i den förordningen.* |
| | *Ett identifieringsverktyg för fysiska personer är ett fysiskt verktyg som kan användas utan mobil terminal och chipkort.* |
| | *Myndigheten för digitalisering och befolkningsdata tillhandahåller identifieringsverktygen för fysiska personer i form av identifieringsverktyg i enlighet med EU:s förordning om elektronisk identifiering, för att användas via den stödtjänst som avses i 3 § 1 mom. 4 punkten i lagen om stödtjänster.* |
| | *69 f §* |
| | *Registret över identifieringsverktyg för fysiska personer* |
| | *Myndigheten för digitalisering och befolkningsdata ska för tillhandahållande och produktion av identifieringsverktyg för fysiska personer föra ett register över identifieringsverktygen och över verktygens innehavare. I registret får följande uppgifter om innehavare av identifieringsverktyg registreras:* |

| Gällande lydelse | Föreslagen lydelse |
| --- | --- |
| | *1) de personuppgifter som ingår i den av en myndighet utfärdade identitetshandling som använts för kontroll av identiteten samt uppgifter som specificerar identitetshandlingen,*<br>*2) de personuppgifter som förmedlas i samband med den elektroniska identifieringsmetod som använts för kontroll av identiteten samt uppgifter om den elektroniska identifieringsmetoden,*<br>*3) en identifikationskod som avses i 11 a §,*<br>*4) en identifieringskod för identifieringsverktyget,*<br>*5) kontaktuppgifter,*<br>*6) andra än i 1–5 punkten avsedda uppgifter som behövs för tillhandahållandet av identifieringsverktyget.*<br>*Bestämmelser om behandling av personuppgifter inom tjänsteproduktionen i fråga om identifieringsverktyg för fysiska personer, om krav som gäller identifieringsverktyget och användningen av det och om styrningen av tjänsteproduktionen finns i 3–5 kap. i lagen om stödtjänster.* |
| | *69 g §* |
| | *Styrkande av sökandens identitet* |
| | *Myndigheten för digitalisering och befolkningsdata beviljar på ansökan ett identifieringsverktyg till en fysisk person.*<br>*Vid inledande identifiering ska identifieringen av en fysisk person göras personligen eller elektroniskt på ett sådant sätt att de krav uppfylls som gäller för tillitsnivån väsentlig eller hög enligt avsnitt 2.1.2 i bilagan till kommissionens genomförandeförordning (EU) 2015/1502 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. Kontrollen av en persons identitet kan grunda sig på en identitetshandling som utfärdats av en myndighet eller på stark autentisering enligt 2 § 1 punkten i lagen om stark autentisering och betrodda elektroniska tjänster.* |

*Gällande lydelse*

*Föreslagen lydelse*

*69 h §*

*Skötsel av uppgifter som gäller beviljande av identifieringsverktyg inom ramen för samservice*

*Utöver vad som i 6 § i samservicelagen föreskrivs om uppgifter som sköts inom ramen för samservice får Myndigheten för digitalisering och befolkningsdata överföra biträdande uppgifter som gäller beviljande av identifieringsverktyg till att skötas inom ramen för samservice. Dessa uppgifter kan omfatta verifiering av identiteten hos dem som ansöker om identifieringsverktyg och hos innehavare av identifieringsverktyg samt rådgivnings- och stödtjänster i samband med ansökan om identifieringsverktyg.*

*Om samservicens uppdragstagare inte ens efter ytterligare utredning kan verifiera sökandens identitet, ska uppdragstagaren överföra ärendet till Myndigheten för digitalisering och befolkningsdata för behandling.*

*69 i §*

*Information om giltighet för pass och identitetskort*

*Myndigheten för digitalisering och befolkningsdata har trots sekretessbestämmelserna rätt att via ett tekniskt gränssnitt eller på något annat sätt i elektronisk form få information ur polisens informationssystem om giltighet för pass och identitetskort som används vid inledande identifiering.*

*69 j §*

*Skyldighet för Myndigheten för digitalisering och befolkningsdata att lämna uppgifter*

*Myndigheten för digitalisering och befolkningsdata ska innan ett identifieringsverktyg beviljas informera sökanden om*

*1) användningen av identifieringsverktyget,*

*Gällande lydelse*

*Föreslagen lydelse*

*2) parternas rättigheter och skyldigheter,*

*3) eventuella ansvarsbegränsningar, och*

*4) eventuella andra än i 1–3 punkten avsedda villkor för användning av identifieringsverktyget.*

*De uppgifter som avses i 1 mom. ska lämnas skriftligen eller elektroniskt så att den som ansöker om ett identifieringsverktyg kan spara och återge dem i oförändrad form.*

*69 k §*

*Rätten för Myndigheten för digitalisering och befolkningsdata att återkalla eller förhindra användning av identifieringsverktyg*

*Myndigheten för digitalisering och befolkningsdata kan återkalla eller förhindra användningen av ett identifieringsverktyg, om*

*1) det finns skäl att misstänka att identifieringsverktyget används av någon annan än den det har beviljats till,*

*2) identifieringsverktyget innehåller ett uppenbart fel,*

*3) det finns skäl att misstänka att säkerheten vid användningen av identifieringsverktyget har äventyrats,*

*4) innehavaren av identifieringsverktyget använder det på ett sätt som väsentligt strider mot villkoren för användningen,*

*5) innehavaren av identifieringsverktyget har avlidit.*

*Myndigheten för digitalisering och befolkningsdata ska så snart som möjligt underrätta innehavaren av identifieringsverktyget om att verktyget har återkallats eller användningen av det förhindrats samt om tidpunkten för och orsakerna till detta.*

*Myndigheten för digitalisering och befolkningsdata ska erbjuda en ny möjlighet att använda identifieringsverktyget eller tillhandahålla innehavaren ett nytt verktyg omedelbart efter det att en sådan orsak som avses 1 mom. 2 eller 3 punkten inte längre föreligger.*

*69 l §*

*Skyldigheter för innehavare av identifieringsverktyg för fysiska personer*

*Gällande lydelse*

*Föreslagen lydelse*

*Innehavaren av ett identifieringsverktyg för fysiska personer ska använda verktyget i enlighet med villkoren för användningen. Innehavaren ska förvara identifieringsverktyget omsorgsfullt. Innehavaren är skyldig att ansvara för verktyget efter att ha tagit emot det.*

*Innehavaren av ett identifieringsverktyg får inte överlåta verktyget för att användas av någon annan.*

*Innehavaren av ett identifieringsverktyg ska göra en anmälan till Myndigheten för digitalisering och befolkningsdata, om verktyget obehörigen har kommit i någon annans besittning eller obehörigen har använts. Anmälan ska göras utan obefogat dröjsmål efter det att saken har upptäckts.*

*Myndigheten för digitalisering och befolkningsdata ska se till att det är möjligt att när som helst göra en anmälan enligt 3 mom. Myndigheten ska återkalla identifieringsverktyget eller förhindra användningen av det utan dröjsmål efter det att anmälan har mottagits. Innehavaren av ett identifieringsverktyg ansvarar inte för obehörig användning av verktyget efter att ha gjort anmälan till Myndigheten för digitalisering och befolkningsdata.*

*69 m §*

*Sökande av ändring*

*Omprövning får begäras i fråga om sådana beslut av Myndigheten för digitalisering och befolkningsdata som gäller beviljande av identifieringsverktyg för fysiska personer i enlighet med 69 e § eller återkallelse av identifieringsverktyg för fysiska personer i enlighet med 69 k §. Bestämmelser om begäran om omprövning finns i förvaltningslagen.*

*Bestämmelser om sökande av ändring i förvaltningsdomstol finns i lagen om rättegång i förvaltningsärenden (808/2019).*

---

*Denna lag träder i kraft den xx xxxx 20 .*

---

**8.**

# Lag

**om ändring av 3 och 9 § i lagen om förvaltningens gemensamma stödtjänster för e-tjänster**

I enlighet med riksdagens beslut

*ändras* i lagen om förvaltningens gemensamma stödtjänster för e-tjänster (571/2016) 3 § 1 mom. 4 punkten och 9 § 1 punkten, av dem 9 § 1 punkten sådan den lyder i lag 1174/2019, som följer:

| *Gällande lydelse* | *Föreslagen lydelse* |
|---|---|
| 3 § | 3 § |
| *Stödtjänster* | *Stödtjänster* |
| De gemensamma stödtjänsterna för e-tjänster omfattar | De gemensamma stödtjänsterna för e-tjänster omfattar |
| — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — |
| 4) en sådan tjänst för identifiering av fysiska personer som identifierar en fysisk person som använder den offentliga förvaltningens e-tjänster med hjälp av en tjänst som tillhandahålls av en sådan leverantör av identifieringstjänster som avses i lagen om stark autentisering och betrodda elektroniska tjänster (533/2016), administrerar identifieringstransaktionen och till användarorganisationen lämnar ut identifieringsuppgifter om en person ur befolkningsdatasystemet, | 4) en sådan tjänst för identifiering av fysiska personer som identifierar en fysisk person som använder den offentliga förvaltningens e-tjänster med hjälp av en tjänst som tillhandahålls av en sådan leverantör av identifieringstjänster som avses i lagen om stark autentisering och betrodda elektroniska tjänster *(617/2009) eller med hjälp av en tjänst som avses i 6 b kap. i lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata (661/2009),* administrerar identifieringstransaktionen och till användarorganisationen lämnar ut identifieringsuppgifter om en person ur befolkningsdatasystemet, |
| — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — |
| 9 § | 9 § |
| *Informationskällor som regelbundet utnyttjas inom tjänsteproduktionen* | *Informationskällor som regelbundet utnyttjas inom tjänsteproduktionen* |
| För att fullgöra sina uppgifter enligt denna lag har Myndigheten för digitalisering och befolkningsdata, med iakttagande av detta kapitel, rätt att behandla i denna paragraf avsedda uppgifter som införts i följande informationssystem:<br>1) i fråga om befolkningsdatasystemet enligt lagen om befolkningsdatasystemet och de | För att fullgöra sina uppgifter enligt denna lag har Myndigheten för digitalisering och befolkningsdata, med iakttagande av detta kapitel, rätt att behandla i denna paragraf avsedda uppgifter som införts i följande informationssystem:<br>1) i fråga om befolkningsdatasystemet enligt lagen om befolkningsdatasystemet och de |

| *Gällande lydelse* | *Föreslagen lydelse* |
| --- | --- |
| certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata *(661/2009)*, uppgifter om personers namn, personbeteckning, elektroniska kommunikationskod, medborgarskap, kontaktspråk, modersmål, dödsdag, intressebevakning, begränsning av handlingsbehörigheten, intressebevakningsfullmakt och vårdnad om barn samt kontaktuppgifter och uppgifter om spärrmarkering, | certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata, uppgifter om personers namn, personbeteckning, elektroniska kommunikationskod, medborgarskap, kontaktspråk, modersmål, dödsdag, intressebevakning, begränsning av handlingsbehörigheten, intressebevakningsfullmakt och vårdnad om barn samt kontaktuppgifter och uppgifter om spärrmarkering, |
| — — — — — — — — — — — — — — — — | — — — — — — — — — — — — — — — — |

———

*Denna lag träder i kraft den xx xxxx 20 .*

———