RP 272/2014 rd

Regeringens proposition till riksdagen med förslag till lag om ändring av lagen om stark autentisering och elektroniska signaturer

PROPOSITIONENS HUVUDSAKLIGA INNEHÅL

I denna proposition föreslås det att lagen om stark autentisering och elektroniska signaturer ändras.

Enligt propositionen ska leverantörer av identifieringstjänster och aktörer som tillhandahåller elektroniska signaturer i fortsättningen kräva personbeteckning vid identifieringen av en person.

Leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller elektroniska signaturer ska inhämta uppgifterna de behöver för tillhandahållandet av identifieringstjänster ur befolkningsdatasystemet. Leverantörer av identifieringstjänster ska dessutom säkerställa att personuppgifterna som behövs för tillhandahållandet av identifieringstjänster är uppdaterade.

Bestämmelsen om inledande identifiering av den som ansöker om ett identifieringsverktyg ska ändras så att en identitet som har verifierats elektroniskt alltid ska basera sig på en fysisk inledande identifiering som gjorts med hjälp av en identitetshandling som en myndighet har beviljat eller på en elektronisk identifiering av sökanden som har gjorts med hjälp av en befintlig identitet som verifierats elektroniskt.

Det föreslås dessutom att det till lagen fogas en bestämmelse om nätverket för leverantörer av identifieringstjänster som utgör ett öppet i lag fastställt förtroendenät mellan identifieringstjänsterna.

De föreslagna bestämmelserna gäller endast verksamhet som bedrivs av de leverantörer av tjänster för stark autentisering som har gjort en anmälan till Kommunikationsverket. Lagen avses träda i kraft den 1 maj 2015.

297460

SISÄLLYSLUETTELO

ALLMÄN MOTIVERING

1 Inledning

De elektroniska tjänsterna har ökat kraftigt under de senaste åren och utvecklingen förväntas fortsätta. De elektroniska tjänsternas affärsekonomiska och medborgarrättsliga betydelse ökar och för detta krävs det i allt fler tjänster en stark och tillförlitlig identifiering av och kännedom om användarna.

Ett huvudtema i programmet för statsminister Alexander Stubbs regering är främjandet av digitaliseringen. Det finns stor potential att effektivisera verksamheten inom de elektroniska tjänsterna, särskilt när det gäller de mest omfattande tjänsterna inom både den offentliga och privata sektorn. Inom den offentliga förvaltningen pågår nationella projekt för att utveckla den elektroniska serviceverksamheten, och inom dessa satsas det mycket på en prioritering av en elektronisk servicekanal. Exempelvis FPA, Skatteförvaltningen och social- och hälsovårdssektorn har i stor utsträckning övergått till att använda elektroniska tjänster.

För närvarande omfattar marknaden för stark elektronisk autentisering huvudsakligen banktjänster och betalningar via webben. Antalet identifieringar som sker på annat sätt än i en nätbank bedöms öka med cirka 30 procent under de närmaste åren. Den offentliga förvaltningen är en av de sektorer där elektronisk identifiering utnyttjas i stor utsträckning.

För serviceproduktionen inom den offentliga förvaltningen är det viktigt att den starka elektroniska autentiseringen är allmänt tillgänglig och kostnadseffektiv samt att användningsmöjligheterna är stora. De kundtjänster som produceras av den offentliga förvaltningen ska för det första vara tillgängliga för medborgarna, och för det andra förmånliga. Inom den traditionella kundbetjäningen har medborgaren bekostat rese- eller postutgifterna. Vid den elektroniska betjäningen bekostar medborgaren de utgifter som föranleds av anskaffningen och användningen av identifieringsverktyget.

Det finns också potential att effektivisera de nuvarande administrativa resurser som används för arrangemangen för elektronisk identifiering. Av de organisationer inom den offentliga förvaltningen som är leverantörer av stark elektronisk autentisering kräver nuvarande praxis att det ingås avtal med alla de leverantörer av stark elektronisk autentisering som har elektroniska identifieringsverktyg som kan användas i en elektronisk tjänst.

2 Nuläge

Den marknad för tjänster som utnyttjar verktyg för stark autentisering är i nuläget uppdelad främst i tre servicesektorer: bank- och försäkringstjänster, offentliga förvaltningens tjänster samt övriga privata tjänster. Bank- och försäkringssektorn samt de elektroniska tjänsterna inom den offentliga förvaltningen står för de största volymerna. I framtiden förväntas användningen av elektronisk identifiering öka inom den offentliga förvaltningen och i handeln på webben.

Tjänster för stark elektronisk autentisering produceras för närvarande av banker, teleoperatörer och Befolkningsregistercentralen. Tillsynen över aktörernas verksamhet inom stark elektronisk autentisering sköts av Kommunikationsverket som även ansvarar för registreringen av de aktörer som är leverantörer av stark elektronisk autentisering.

Bankkoderna innehar den största marknadsandelen i fråga om antalet användare och transaktioner. Teleoperatörernas mobilcertifikat samt de medborgarcertifikat som anknyts till de identitetskort som Befolkningsregistercentralen ger ut har inte uppnått en betydande ställning på marknaden för elektronisk identifiering. Med mobilcertifikatet är det möjligt att använda största delen av de elektroniska tjänster som tillhandahålls, med undantag av banktjänsterna.

I förarbetena till lagen om stark autentisering och elektroniska signaturer (617/2009) betonades det att marknaden för elektronisk identifiering behöver öppnas. Vid beredning-

en av lagen bedömde man att de ramar som fastställs i lagen är tillräckliga för att stärka marknaden och göra den lättillgängligare för nya aktörer. Detta har dock inte skett. Stark elektronisk autentisering skulle kunna användas i större utsträckning i olika tjänster både inom den privata och offentliga sektorn.

Inom projektet för den nationella servicearkitekturen under ledning av finansministeriet samt inom programmet för påskyndande av elektronisk ärendehantering och demokrati (SADe-programmet) produceras ett flertal tjänster och servicehelheter för genomförande av elektronisk handläggning inom olika förvaltningsområden. En stark elektronisk autentisering av användaren är viktigt för att uppnå målen för de båda programmen.

Under de närmaste åren kommer det många nya elektroniska tjänster inom social- och hälsovården, och för dem behövs det stark elektronisk autentisering. Inom social- och hälsovårdssektorn behandlar man ofta sådana uppgifter om personers hälsa eller försörjning som är sekretessbelagda, vilket kräver stark elektronisk autentisering av användarna och de personer som hanterar uppgifterna. Detta förutsätter att de olika aktörerna har en förenlig modell för att identifiera användaren i olika tjänster.

Elektronisk identifiering utnyttjas i betydande grad i samband med elektroniska tjänster som t.ex. i näthandeln, olika diskussionsforum samt andra sociala medier. I dem används i allmänhet svag elektronisk autentisering, där identifieringen av användaren baserar sig t.ex. på användarnamn och lösenord samt de personuppgifter användaren ger.

I de flesta elektroniska kundtjänster som produceras av den offentliga sektorn är det möjligt att låta identifiera sig med alla de identifieringsverktyg som används av de leverantörer av stark elektronisk autentisering som har lämnat en anmälan till Kommunikationsverket. En del av den offentliga förvaltningens tjänster godkänner dock inte alla identifieringsverktyg t.ex. på grund av de kostnader eller besvärliga avtal som hänför sig till användningen av dem.

Inom den offentliga sektorn används för närvarande två styrningstjänster för identifiering (Vetuma och tunnistus.fi), där de offentliga tjänsterna har tillgång till alla leverantörer av identifieringstjänster via ett och samma tekniska gränssnitt. Som ett led i programmet för den nationella servicearkitekturen ska man 2015 börja utarbeta en gemensam styrningstjänst för identifiering för den offentliga förvaltningen, som under övergångsperioden kommer att ersätta tunnistus.fi-tjänsten (ersätts först) och Vetuma-tjänsten (ersätts inom en längre övergångsperiod). Den nya styrningstjänsten för identifiering ska sammanföras med den nationella roll- och fullmaktstjänst som ska utvecklas under åren 2015-2017.

Genom dessa gemensamma arrangemang har den offentliga förvaltningen bidragit till ibruktagandet av stark elektronisk autentisering. Vid finansministeriet uppskattas det att det har ingåtts cirka 1500 avtal mellan statsförvaltningen och leverantörer av identifieringstjänster, och de flesta med olika bankgrupper. En sådan mängd avtal medför orimliga kostnader för små aktörer. Inom den privata sektorn har det dock bildats sådana tjänster som tillhandahåller många olika identifieringstjänster genom ett enda avtal och gränssnitt.

2.1 Lagstiftning och praxis

I samband med delegationen för vardagens informationssamhälle utarbetades ett principbeslut av statsrådet samt nationella riktlinjer för elektronisk autentisering. Propositionen baserar sig på dessa riktlinjer. Lagen om stark autentisering och elektroniska signaturer trädde i kraft den 1 september 2009. I lagen anges de krav som ställs i Finland på den starka elektroniska autentisering som ska tillhandahållas för allmänheten. Syftet med lagen är att bestämmelserna ska främja en marknadsbaserad utveckling av den elektroniska identifieringen samt att genom elektronisk identifiering som baserar sig på fri konkurrens garantera en lägre kostnadsnivå. Befolkningsregistercentralens identifieringstjänster omfattas utöver lagen om stark autentisering och elektroniska signaturer även av lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009).

De privata aktörernas roll vid beviljandet av en officiell elektronisk identitet baserar

sig på att de affärsekonomiska tjänsterna på identifieringsmarknaden har ansetts vara i den grad distanserade från den offentliga förvaltningsuppgiftens särdrag att verksamheten inte kan anses vara en betydande offentlig förvaltningsuppgift, även om verktygen för stark elektronisk autentisering samt certifikaten som sådana är av betydelse vid olika rättshandlingar.

Ansvaret för lagstiftningen om stark elektronisk autentisering är fördelat mellan kommunikationsministeriet och finansministeriet. Kommunikationsministeriet ansvarar för den allmänna lagstiftningen om elektronisk identifiering och finansministeriet för den lagstiftning som gäller Befolkningsregistercentralen samt för den offentliga förvaltningens styrning av användningen av elektronisk identifiering. Tillsynen över aktörernas verksamhet inom stark autentisering sköts av Kommunikationsverket som ansvarar för registreringen av de aktörer som är leverantörer av stark elektronisk autentisering.

Utöver lagen om stark autentisering och elektroniska signaturer inverkar även övriga lagar på den starka elektroniska autentiseringen och på de elektroniska signaturerna. Detta gäller särskilt lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003), lagstiftningen om de certifikattjänster som Befolkningsregistercentralen tillhandahåller (661/2009) och personuppgiftslagen (523/1999).

Vid beredningen av propositionen har man tagit i beaktande att de nuvarande leverantörerna av stark elektronisk autentisering förpliktas av föreskrifter inom många olika verksamhetsområden. Exempelvis vid beviljandet av nätbankkoder ska bl.a. lagen om kreditinstitutsverksamhet (121/2007), lagstiftningen om penningtvätt och bestämmelserna om grundavgiftskonton beaktas.

Vid beredningen av propositionen har man även beaktat Europaparlamentets och rådets förordning om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden, som behandlas närmare i avsnittet om den internationella utvecklingen. I förordningen hänvisas till de tillitsnivåer för elektronisk autentisering för vilka kommissionen för närvarande bereder definitioner. Den högsta tillitsnivån i förordningen är hög.

Det är ändamålsenligt att på nationell nivå bereda resurser för en hög tillitsnivå och stegvis försöka nå detta mål under 2016-2018 med beaktande av olika sektorers behov. Detta förutsätter eventuellt att lagstiftningen ändras samt att praxis utvecklas. Säkerheten vid elektronisk identifiering och de behövliga tillitsnivåerna ska ses över årligen och jämföras med den höga tillitsnivå som har fastställts i Europaparlamentets och rådets förordning. Tillräckligt säkra lösningar ska alltid eftersträvas vid den identifiering som sker på nationell nivå.

2.2 Den internationella utvecklingen samt lagstiftningen i utlandet och i EU

Inledning

I Finland avses med stark elektronisk autentisering sådana identifieringstjänster som det bestäms om i Europaparlamentets och rådets förordning om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (910/2014).

Europaparlamentets och rådets förordning om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden ska tillämpas på de system för elektronisk identifiering som anmälts av medlemsstaterna samt på de leverantörer av betrodda tjänster som är lokaliserade inom unionen. I förordningen avses med betrodda tjänster t.ex. de elektroniska tjänster som omfattar elektroniska signaturer eller elektroniska stämplar. Förordningen ska tillämpas på gränsöverskridande och ömsesidig elektronisk identifiering. Den omfattar inte de identifieringslösningar som används inom den privata sektorn, med undantag av de tillitsnivåer som ska fastställas för metoderna för elektronisk identifiering.

Europaparlamentets och rådets förordning om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden är direkt tillämplig rätt i medlemsstaterna. Detta innebär att medlemsstaternas förvaltningsmyndigheter och dom-

stolar är förpliktade att tillämpa förordningen direkt utan att en nationell lagberedare först omformar dem till nationella normer. Förordningen trädde i kraft den 17 september 2014, men den ska tillämpas först från och med den 1 juli 2016, med undantag av flera bestämmelser som ska tillämpas enligt särskilda övergångsbestämmelser, som t.ex. bestämmelserna om tillitsnivåerna. Kommissionen har inlett arbetet med mer detaljerade förordningar om genomförandet, och arbetet fortsätter till sommaren 2015. Målet är att genomförandebestämmelserna ska vara i kraft hösten 2015. På grund av att beredningen av genomförandet fortfarande pågår kan ändringar i enlighet med förordningen inte föreslås i detta utkast till regeringspropositionen, t.ex. när det gäller de tillitsnivåer eller definitioner som gäller identifieringstjänster. De ändringar av den nationella lagstiftningen som förordningen föranleder ska kartläggas och genomföras före den 1 juli 2016. Förordningen träder i kraft i sin helhet år 2018.

De ändringar som nu föreslås har beretts så att de inte strider mot förordningen. Genomförandebestämmelserna ska inte tillämpas på de delområden som föreslås i denna proposition. Genom denna regeringsproposition strävar man efter att skapa en verksamhetsmiljö där Finland har lätt att ansluta sig till det EU-omfattande förtroendenätet. Finlands anslutning till förtroendenätet kommer enligt de nuvarande planerna att skötas via en anslutningspunkt som upprätthålls av staten. Vid den elektroniska identifiering som sker mellan medlemsländerna ska inga avgifter betalas eller tas ut. Senast i det skede då verksamheten inleds införs dessa kostnader sannolikt i utgifterna för statsförvaltningens förmedlingstjänst. Identifieringarna bedöms bli få i början.

I följande avsnitt behandlas den elektroniska identifieringen i fem europeiska länder. Föremålen för granskningen är de nordiska länderna Sverige, Norge och Danmark. Dessutom granskas den elektroniska identifieringen i Estland och Holland. Estland valdes speciellt därför att staten i Estland har gjort ett betydande utvecklingsarbete inom de elektroniska tjänsterna under de senaste åren. Under ledning av finansministeriet pågår det även en beredning av en nationell servicekanal som baserar sig på den servicekanallösning som används i Estland. Holland valdes för att ta del av en synvinkel utanför våra grannländer och Norden.

I avsnittet om de olika länderna granskas främst hurdana lösningar som förekommer i länderna när det gäller inledande identifiering, användningen av nationella befolkningsdatasystem samt eventuella förtroendenät mellan aktörer inom elektroniska identifieringstjänster.

Estland

I Estland måste varje medborgare som fyllt 15 år ha ett identitetskort som även möjliggör elektronisk identifiering. Kortet är avgiftsbelagt och beviljas av medborgar- och immigrationsmyndigheten. Utöver identitetskortet kan man även skaffa ett separat frivilligt elektroniskt kodkort som kan användas endast för elektronisk identifiering. De certifikat som är anknutna till kodkorten produceras av ett privat företag som väljs på basis av konkurrensutsättning. De leverantörer av elektroniska tjänster som utnyttjar kort med certifikat betalar en avgift till certifikatproducenten för att få använda certifikaten.

Statens elektroniska kodkort är tydligt den lösning som används mest på marknaden. Elektronisk identifiering med det nationella kodkortet kräver en kortläsare, som de flesta användare även har hemma. Förutom kodkortet finns det även bankkoder och mobilkoder på marknaden, men de används dock inte i lika stor utsträckning som kodkorten.

Inrikesministeriet i Estland uppehåller ett nationellt befolkningsregister där alla medborgares basuppgifter registreras. Medborgarna har möjlighet att uppdatera sina egna uppgifter elektroniskt i registret. Befolkningsregistersystemets uppgifter är främst avsedda för att användas av statens aktörer, men även privata aktörer har inom ramen för lagen möjlighet att med den berörda personens samtycke begära personuppgifter ur befolkningsregistersystemet genom en separat ansökan.

Det nationella elektroniska identitetskortet och kodkortet används i stor utsträckning i olika tjänster inom den privata och offentliga sektorn. En gemensam servicekanal med

namnet X-Road sammanför de olika aktörerna och tjänsterna. För de tjänster som levereras via servicekanalen kan man låta identifiera sig med bankkoder, och detta anses ge en lika stark autentisering som det elektroniska kodkortet.

Över 300 nättjänster använder certifikattjänsten för att identifiera sina användare.

Sverige

I Sverige har man fattat ett beslut om att staten inte ska erbjuda tjänster för elektronisk identifiering alls, utan att identifieringstjänsterna ska tillhandahållas på den fria marknaden. I denna modell kräver elektronisk identifiering samt tillhandahållandet av tjänsterna att villkoren i lagen uppfylls. Samtliga nuvarande identifieringslösningar fungerar både inom den offentliga och privata sektorns tjänster. Alla tjänsteleverantörer har dock rätt att välja vilka identifieringslösningar de vill använda i sin tjänst.

För närvarande finns det tre olika identifieringstjänster på marknaden. Den klart största marknadsandelen omfattas av identifiering med bankkoder (BankID, 5 miljoner användare), som är en produkt av samarbetet mellan de största bankerna.

Hur den inledande identifieringen sköts beror på leverantören av identifieringstjänsten. När det gäller BankID och Nordeas koder sker den inledande identifieringen på bankens kontor i samband med att kundrelationen ingås eller separat vid undertecknandet av ett BankID-avtal. Telia Sonera erbjuder en möjlighet att ingå avtal via internet, varvid identifieringen sker på basis av givna personuppgifter och de egentliga identifieringsverktygen skickas till den adress som anges i befolkningsdatasystemet. Största delen av de elektroniska identifieringsverktygen förutsätter ett svenskt personnummer.

Förmedlandet och utnyttjandet av befolkningsdata regleras strikt i Sverige. Överträdelser av lagstiftningen kan leda till stränga sanktioner. Uppgifter ur befolkningsdatasystemet kan fås på basis av personnumret, om sökanden har ett skäl till det. Bankerna kontrollerar t.ex. adressuppgifterna i det nationella systemet vid behov.

I Sverige finns det inte en sådan nationell centraliserad lösning som motsvarar det förtroendenät som planeras för Finland. På marknaden finns det dock en tjänsteleverantör som tillhandahåller dirigering av olika koder till tjänsterna. En aktör inom näthandeln kan t.ex. få alla identifieringstjänster som finns på marknaden till dess sidor från en enda leverantör av dirigering. När det gäller bankidentifiering fungerar största delen av bankerna via en och samma dirigeringstjänst (BankID), och då behövs det inte separata avtal med varje bank. Utöver detta har vissa branscher (t.ex. skolor) bildat sammanslutningar, som gemensamt utarbetat en inloggning som godkänner olika elektroniska identifieringsmetoder.

Danmark

I Danmark utgör den elektroniska identifieringen en del av den nationella infrastrukturen. Den lösning som är i bruk kan användas för att identifiera användare både i offentliga och privata tjänster. Ägaren av denna lösning är finansministeriet. För utvecklandet och upprätthållandet av tjänsten ansvarar en privat aktör (Nets), som finansministeriet har valt på basis av konkurrensutsättning. Utöver utvecklingstjänsten tillhandahåller företaget också infrastruktur för betalningar. I praktiken förutsätter den elektroniska identifieringstjänsten ett användarnamn, ett lösenord och en utbytbar pin-kod.

I Danmark rekommenderas det att man ansöker om ett elektroniskt identifieringsverktyg via webben, varvid koderna skickas till den adress som anges i befolkningsregistret. Inledande identifieringar görs också på banker eller i kommunala servicepunkter. För att få en elektronisk kod krävs det en dansk personbeteckning. I samband med sådan inledande identifiering som sker personligen ska sökandens identitet bekräftas med pass, körkort eller annat motsvarande identitetsbevis.

Hanteringen av uppgifterna i befolkningsdatasystemet i Danmark regleras genom en personuppgiftslag och en lag om elektronisk identifiering. Personuppgiftslagen behandlar ämnet i stora drag och innehåller inte exakta bestämmelser om vem och för vilka ändamål någon kan få tillgång till personuppgifter el-

ler förmedla dem vidare. I praktiken har aktörer inom den offentliga sektorn en bättre tillgång till personuppgifterna än aktörer inom den privata sektorn. En aktör inom den privata sektorn (t.ex. en bank) behöver ett separat tillstånd av den berörda personen för att kunna få tillgång till personuppgifterna.

I praktiken finns det endast en elektronisk identifieringslösning som finansieras med offentliga medel, och den används även av bankerna. Ur en affärsekonomisk synvinkel utgör den elektroniska identifieringen affärsverksamhet endast för det företag som utvecklar och producerar denna produkt.

Norge

I Norge är det staten, bankerna och två privata företag som tillhandahåller elektroniska identifieringstjänster. Statens MinID-autentisering kan användas endast inom den offentliga sektorns tjänster. Med bankkoder och i övriga privata identifieringstjänster kan man dock låta identifiera sig både för offentliga och privata tjänster. Man har god kännedom om lösningarna för elektronisk identifiering och de används i stor utsträckning. Elektronisk identifiering utnyttjas vid skötseln av beskattningsärenden och pensionsärenden via elektroniska kanaler i de offentliga tjänsterna. Över tre miljoner norrmän använder elektronisk identifiering i de offentliga tjänsterna.

Elektronisk identifiering i offentliga tjänster kräver en identifieringstjänst som är kompatibel med inloggningssystemet ID-porten. För närvarande är alla identifieringstjänster på marknaden kompatibla med ID-porten. Marknaden för identifieringstjänster omfattas i princip av fri konkurrens, men av en ny aktör krävs det behörighet och registrering i enlighet med lagen. Tillstånd beviljas av Norges post- och kommunikationsverk. Norges post- och kommunikationsverk ansvarar för att alla registrerade producenter av identifieringstjänster uppfyller de krav som gäller elektroniska signaturer, och upprätthåller en förteckning över de aktörer som ger ut sådana identifieringsverktyg som uppfyller kvalitetskraven. De identifieringstjänster som tydligt används mest idag är det nationella MinID som fungerar endast i de offentliga tjänsterna samt bankernas BankID som fungerar både i de privata och offentliga tjänsterna.

För att få en nationell MinID-kod krävs det en norsk personbeteckning, en mobiltelefon eller en e-postadress och en separat PIN-kod som beställs med den egna personbeteckningen av en aktör inom den offentliga förvaltningen. Tjänsten förutsätter minst 13 års ålder. Privata aktörer bestämmer själva sina egna kravnivåer angående den inledande identifiering som krävs för att få ett elektroniskt identifieringsverktyg.

I Norge används ett nationellt befolkningsdatasystem som innehåller medborgarnas uppdaterade basuppgifter. För systemets upprätthållande ansvarar skatteförvaltningen. I princip kan man inte få tillgång till eller förmedla personuppgifter utan en laglig grund.

Holland

I Holland används två separata lösningar för elektronisk identifiering: en för medborgarna (DigiD) och en annan för företag (eHerkenning/eRecognition). DigiD är ett system för den offentliga sektorn. Det system som är avsett för företag är ett resultat av samarbete mellan den offentliga sektorn och företag. Detta system grundar sig på avtal mellan företag och staten och har som mål att skapa ett gemensamt identifieringssystem även för företagens ömsesidiga verksamhet. Staten utövar tillsyn över systemet för att alla de krav som ställs på det ska uppfyllas.

Båda lösningarna stöds med offentliga medel och kan ses som en del av den nationella infrastrukturen. Det system för elektronisk identifiering som är avsett för medborgarna fungerar endast i offentliga sektorns tjänster och i de tjänster som gäller försäkringsbolagens livsförsäkringar. Företagens identifieringstjänst fungerar utöver i de offentliga tjänsterna även vid kommunikationen mellan företagen.

Lösningen för elektronisk identifiering har tagits i bruk av medborgarna i stor utsträckning. Lagstiftningen möjliggör en fri marknad för de elektroniska identifieringstjänsterna, men för närvarande är aktörerna få. På marknaden finns några företag som tillhandahåller mobilautentisering, men i praktiken används mobilautentisering mycket lite och

få tjänster stöder detta. Mobilautentisering kan för närvarande inte användas i den offentliga sektorns tjänster. På marknaden används även bankkoder, men dessa kan endast utnyttjas i banktjänsterna.

Det elektroniska identifieringsverktyg som är avsett för medborgarna ges ut av inrikesministeriet på ansökan. Ansökan görs elektroniskt på webben. Aktiveringen av den elektroniska koden kräver en aktiveringskod som skickas till sökanden per post till den adress som har registrerats i det kommunala systemet. Efter detta ska personen logga in i systemet, aktivera koden och ändra lösenordet. DigiD-koder kan ansökas av en person som är registrerad i det kommunala registret och som har fått ett personnummer.

I Holland finns inte ett enda nationellt befolkningsdatasystem, utan uppgifterna registreras på kommunal nivå i kommunernas egna databaser. Dessa separata databaser är anknutna till varandra via en centraliserad organisation, men uppgifterna är inte alltid uppdaterade, vilket utgör en utmaning.

Holland har inte ett förtroendenät till vilket alla identifieringstjänster skulle kunna anslutas. Vid utbytet av information mellan aktörer inom den offentliga förvaltningen fungerar medborgarnas DigiD-lösning bra, och har inga märkbara brister. Bankerna har utvecklat en egen lösning vid namn iDeal för sin ömsesidiga verksamhet, som utnyttjas för elektroniska betalningar.

Flera privata aktörer är intresserade av en öppen gemensam identifieringslösning, men för närvarande har de alla egna lösningar som tidvis upplevs som otillräckliga.

2.3 Bedömning av nuläget

Under de nuvarande förhållandena är det svårt för nya leverantörer av identifieringstjänster samt för nya identifieringslösningar att få tillträde till marknaden. Syftet med förslaget är att effektivisera verksamheten på marknaden bl.a. genom att skapa förutsättningar för utveckling och användning av nya lösningar på marknaden för identifieringsverktyg och identifieringslösningar. I och med detta ges även användarna valmöjligheter.

Den sammanlagda kostnaden för de identifieringstjänster som används i den offentliga förvaltningens elektroniska tjänster samt för utnyttjandet av dem har under de senaste åren uppgått till cirka 4-6 miljoner euro per år beroende på antalet identifieringar. Antalet identifieringar inom den offentliga förvaltningens tjänster uppgick 2013 till sammanlagt cirka 20,7 miljoner. Antalet förväntas öka med cirka 15-30 procent under de följande åren.

Antalet nätbankkoder uppgår till cirka 5,5 miljoner, och 2013 användes dessa för 47,1 miljoner identifieringstransaktioner. Antalet beviljade mobilcertifikat uppgår till flera tiotusen och certifikattransaktionerna till flera tiotusen eller hundratusen per år. Användningen av mobilcertifikat har inte ännu gett någon betydande avkastning. Antalet HST-kort och de medborgarcertifikat som är anknutna till dem uppgår till cirka 450 000. För närvarande statistikförs inte Befolkningsregistercentralens certifikattransaktioner per certifikat.

De nuvarande nätbankkoderna är främst avsedda för bankernas egna kunder som verktyg vid användningen av konton. Delvis på grund av detta godkänner för närvarande de banker som tillhandahåller identifieringstjänster inte andra identifieringstjänsters identifieringsverktyg. Som en följd av detta behöver användaren flera olika identifieringsverktyg t.ex. om användaren är kund hos flera än en bank. Detta har även lett till att leverantörerna av elektroniska tjänster är tvungna att ingå separata avtal med alla de olika leverantörerna av identifieringstjänster för att möjliggöra elektronisk handläggning för alla som är kund hos en leverantör av identifieringstjänster.

Ett tydligt problem i nuläget är att leverantörerna av elektroniska tjänster inte kan öppna de elektroniska identifieringstjänsterna för verklig konkurrens och således inte heller aktivt kontrollera de kostnader som utnyttjandet av identifieringstjänsterna medför. Syftet med förslaget är att skapa förutsättningar för en marknad för nya identifieringsverktyg och nya slags affärsmöjligheter för identifiering, men samtidigt även att säkerställa att de nuvarande identifieringsverktygen kan användas störningsfritt i fortsättningen. Genom

förslaget strävar man efter att leverantörerna av elektroniska tjänster ska ha bättre möjligheter att påverka och kontrollera kostnaderna för identifiering.

Den tekniska utvecklingen på marknaden för identifieringstjänster ligger efter den övriga teknologiutvecklingen. Genom att i enlighet med förslaget skapa förutsättningar för nya aktörer inom branschen skapas det på identifieringsmarknaden förutsättningar och incitament för utveckling av ny teknik och nya slags tjänster för elektronisk identifiering.

Befolkningsregistercentralens roll inom elektronisk identifiering är förutom att upprätthålla befolkningsdataregistret att producera tjänster för elektronisk identifiering för den offentliga och privata sektorn. I befolkningsdatasystemet antecknas basuppgifter om finska medborgare och om utlänningar som bor permanent i Finland.

I de elektroniska tjänster som Befolkningsdatacentralen tillhandahåller ingår t.ex. medborgarcertifikaten, som anknyts till de identitetskort som beviljas av polisen, certifikattjänsterna för aktörer inom hälso- och sjukvården och organisationscertifikaten för organisationer. Priserna på de tjänster som Befolkningsdatacentralen tillhandahåller fastställs i enlighet med lagen om grunderna för avgifter till staten (150/1992) och den förordning av Befolkningsdatacentralen som utfärdats med stöd av den.

Befolkningsdatacentralens roll såsom leverantör av ett myndighetsregister som innehåller officiella personuppgifter har bromsat utvecklingen av en jämlik marknad för identifieringstjänster. Därför finns det även skäl att utreda olika myndigheters roller och uppgifter när den elektroniska identifieringen utvecklas nationellt i fortsättningen.

För närvarande kontrollerar leverantörerna av identifieringstjänster ur sina egna kundregister att identiteten på den identifierade personen stämmer. Detta har inte medfört problem, eftersom praxis har varit att uppgifterna i fråga baserar sig på befolkningsdatasystemet, som också används för att kontrollera uppgifterna. Förfarandet har inte utvecklats som en följd av den lagstiftning som gäller stark elektronisk identifiering. Den verksamhet som bedrivs av leverantörer av identifieringstjänster regleras utöver lagstiftningen om elektronisk identifiering även genom andra bestämmelser och föreskrifter, t.ex. genom lagstiftningen om penningtvätt. I den lagstiftning som inte gäller elektronisk identifiering anvisas leverantörerna av identifieringstjänster att använda myndigheternas register. Det är möjligt att nya aktörer som inte omfattas av andra föreskrifter än den lagstiftning som gäller elektronisk identifiering kommer att tillträda marknaden. Med tanke på ett fungerande samhälle är det viktigt att t.ex. basuppgifterna om en persons identitet alltid baserar sig på en myndighets register.

I nuläget och särskilt i framtiden bör man lägga vikt vid informationssäkerheten i fråga om den tekniska utrustning som används för stark elektronisk autentisering. I och med att teknologin utvecklas kan bl.a. identitetsstölderna utgöra ett problem ifall den starka elektroniska autentiseringen sker med sådan utrustning som inte är säker och från vilken t.ex. PIN-koden är lätt att stjäla. Kraven på säkerheten ska beaktas när genomförandet av Europaparlamentets och rådets förordning om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden samt förordningarna och föreskrifterna utfärdade av Europeiska bankmyndigheten bereds. I Finland ska den utrustning som används för stark elektronisk autentisering motsvara de krav som ställs på unionnivå och vara tillräckligt säker, men samtidigt får inte användbarheten ur användarens eller tjänsteleverantörens perspektiv försämras.

3 Målsättning och de viktigaste förslagen

3.1 Målsättning

Syftet med den gällande lagstiftningen är att möjliggöra samarbete mellan olika aktörer inom identifiering, vilket garanterar att marknaden utvecklas. Den starka elektroniska autentiseringen baserar sig för närvarande främst på de nätbankkoder som är avsedda för kontoanvändning, och i praktiken är därför den identifieringstjänst som ska levereras till allmänheten bunden till en kundrelation och tillhandahålls vid sidan av en annan

tjänst. Detta kan inte anses vara ändamålsenligt ur ett konkurrens- och konsumentperspektiv. Detta är en delorsak till att de olika aktörerna inte lyckats komma överens om ett omfattande ömsesidigt godkännande av elektroniska identifieringsverktyg och till att det inte skett någon marknadsbaserad utveckling av identifieringstjänsterna trots att den nuvarande lagstiftningen har möjliggjort detta.

Målet är att medborgarens verktyg för stark elektronisk autentisering ska kunna användas i alla sådana tjänster inom privata sektorn där en stark autentisering av användaren är nödvändig samt i alla de tjänster inom den offentliga sektorn där en stark autentisering av användaren behövs. Leverantören av den elektroniska tjänsten kan dock besluta vilka identifieringsverktyg eller identifieringslösningar den godkänner.

För att få tillhandahålla elektroniska identifieringstjänster krävs det en anmälan om inledande av verksamhet till Kommunikationsverket. De leverantörer av identifieringstjänster som har lämnat en anmälan till Kommunikationsverket och som uppfyller kriterierna för verksamheten bildar ett förtroendenät inom elektronisk identifiering. Med hjälp av förtroendenätet skapas förutsättningar för ökad konkurrens på marknaden för identifieringstjänster, vilket förhindrar att en enda leverantör av identifieringstjänster får monopol på identifieringstjänsterna inom den offentliga förvaltningen.

Med förtroendenät avses en verksamhetsmodell där både användaren och leverantören av den elektroniska tjänsten har en stödjande s.k. "tredje part" som i servicesituationen förenar de två för varandra okända parterna (användaren och leverantören) på ett tillförlitligt sätt. Med hjälp av förmedlarna bildas på så sätt ett förtroende mellan de två för varandra okända parterna. Det är fråga om ett förtroendenät då det finns flera grupper av användare och leverantörer med sina tredje parter.

I enlighet med 2 § 1 mom. 4 punkten i lagen om stark autentisering och elektroniska signaturer kan leverantören av identifieringstjänster ha två olika roller i förtroendenätet: att ge ut identifieringsverktyg till slutanvändarna eller skicka vidare en annan leverantörs användaridentifieringar till leverantörer av elektroniska tjänster. Leverantören kan dock också ha båda rollerna.

I de elektroniska tjänster som kan antas kräva stark autentisering av och kännedom om användaren, kan leverantören av den elektroniska tjänsten besluta vilka identifieringsverktyg som ska godkännas. En leverantör av identifieringstjänster ska erbjuda leverantörerna av elektroniska tjänster en teknisk och administrativ möjlighet att godkänna alla de identifieringstjänster som används.

Den som levererar en identifieringstjänst och den leverantör av elektroniska tjänster som utnyttjar en identifieringstjänst ansvarar i förtroendenätet för de kostnader som identifieringarna orsakar dess egen leverantör av identifieringstjänster. När den leverantör av elektroniska tjänster som utnyttjar identifieringstjänsten begär att en användare ska identifieras betalar denna således en ersättning endast till den leverantör av identifieringstjänster med vilken den har ett avtal.

I och med förtroendenätet minskar mängden avtalsgränssnitt avsevärt särskilt inom statsförvaltningen. Leverantörerna av identifieringstjänster avtalar om att parterna ska ha tillit till de identifieringsverktyg som den andra aktören inom identifieringstjänster tillhandahåller. Av detta följer att leverantören av elektroniska tjänster endast behöver ingå ett enda avtal med en utvald leverantör av identifieringstjänster, varefter alla de användare som innehar ett identifieringsverktyg utgör potentiella kunder för leverantören av den elektroniska tjänsten. Det föreslås dock inte att leverantören av en elektronisk tjänst måste godkänna de olika identifieringstjänsterna, utan leverantören kan välja vilka identifieringstjänster den godkänner. En marknadsbaserad utveckling av den elektroniska identifieringen och de elektroniska tjänsterna förutsätter en tillräckligt fri affärsmodell där de företag som bedriver verksamhet inom de olika sektorerna kan utveckla sin affärsverksamhet för elektronisk identifiering eller de tjänster som denna möjliggör. Målet för de föreslagna ändringarna är en sådan verksamhetsmiljö som skapar förutsättningar för marknaden att erbjuda sådana elektroniska identifieringstjänster som lämpar sig för olika ändamål.

De tjänster som baserar sig på elektronisk identifiering samt de ekonomiska och rättsliga åtgärder som vidtas i samband med dem är alla mycket olika. Detta kräver att alla de leverantörer av identifieringstjänster som omfattas av lagstiftningen har en gemensam reglerad grundnivå för tillförlitligheten. De bestämmelser som föreslås i propositionen behandlar förhållandet mellan leverantörerna av identifieringstjänster. På grund av skillnaderna i tjänsternas ekonomiska eller rättsliga verkningar behöver leverantörerna av identifieringstjänster och de leverantörer av elektroniska tjänster som utnyttjar identifieringstjänster kunna avtala om de ömsesidiga ansvarsbegränsningarna i de avtal om tjänster som ingås. Därför tas det i de föreslagna ändringarna inte ställning till hur ansvaret mellan de olika tjänsteleverantörerna ska fördelas, utan detta ska bestämmas i de privaträttsliga avtalen.

Leverantörerna av tjänster för stark elektronisk autentisering kan fortsätta tillhandahålla sina egna elektroniska identifieringsverktyg till användarna även efter att den föreslagna lagen har trätt i kraft, om leverantören av elektroniska identifieringstjänster har lämnat en anmälan till Kommunikationsverket om att de levererar tjänster för stark autentisering. När Europaparlamentets och rådets förordning om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden börjar tillämpas den 1 juli 2016 ska tillitsnivåerna för de nuvarande identifieringsverktygen ses över för att motsvara kraven i förordningen. Den gällande lagstiftningen och de föreslagna ändringarna gäller endast sådan stark elektronisk autentisering som är avsedd för allmänheten.

I propositionen föreslås det att en identitet som verifieras elektroniskt alltid ska basera sig på en fysisk inledande identifiering genom en identitetshandling som en myndighet har beviljat eller på en inledande identifiering som skett genom att en befintlig identitet verifierats elektroniskt. De uppgifter som gäller en identitet som har verifierats elektroniskt kontrolleras alltid i det befolkningsdatasystem som upprätthålls av Befolkningsregistercentralen i samband med en inledande identifiering eller när ett nytt identifieringsverktyg skapas genom ett befintligt identifieringsverktyg. För att få ett verktyg för stark autentisering ska det enligt förslaget krävas den finska personbeteckning som anges i befolkningsdatasystemet och ett giltigt pass eller identitetskort som har utfärdats av en myndighet i en medlemsstat inom Europeiska ekonomiska samarbetsområdet, i Schweiz eller i San Marino, eller, om leverantören så önskar, ett giltigt körkort som har utfärdats efter den 1 oktober 1990 av en myndighet i en medlemsstat i Europeiska ekonomiska samarbetsområdet eller ett giltigt pass eller giltigt verktyg för stark elektronisk autentisering som har utfärdats av en myndighet i någon annan stat.

Vid en ansökan om ett elektroniskt identifieringsverktyg utförs det en verifiering av användarens identitet, och den utgör grunden för att få det identifieringsverktyg som kopplas ihop med de uppgifter som identifierar personen och som används för att verifiera användarens identitet elektroniskt. Ett identifieringsverktyg måste kunna sammankopplas på detta sätt för att kunna skapa nya elektroniska identifieringsverktyg.

I fråga om användningen av det elektroniska identifieringsverktyget föreslås det i propositionen att leverantören av identifieringstjänsten ska sörja för att de personuppgifter om användaren som används i de lektroniska identifieringstjänsterna uppdateras och överensstämmer med uppgifterna i Befolkningsregistercentralens befolkningsdatasystem.

Avsikten med propositionen är att öka möjligheterna för ett ökat utbud av elektroniska tjänster, t.ex. genom att de aktörer som levererar elektroniska identifieringstjänster ska kunna utnyttja den elektroniska identifieringen även vid fysisk kundbetjäning.

Avsikten med en verksamhet där aktörerna är starkt marknadsbaserade är också att utveckla teknologineutrala identifieringstjänster.

Europaparlamentets och rådets förordning om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden kommer att medföra ändringar av den nationella lagen om stark autentisering och elektroniska signaturer. Förordningen överlappar delvis den nationella lagstiftningen, men förordningen innehåller

också helt nya avsnitt som ska genomföras före den 1 juli 2016. Dessa ändringar ingår inte i denna proposition, eftersom kommissionens arbete med genomförandebestämmelserna ännu pågår. Ändringen av lagen om stark autentisering och elektroniska signaturer är således en process i två delar, vars första del genomförs genom denna proposition.

Propositionen har avgränsats så att den endast behandlar sådan elektronisk identifiering som gäller de privatpersoner vars uppgifter finns i befolkningsdatasystemet. Hur identifieringen av företag ska utvecklas kommer att beredas senare i en särskild arbetsgrupp. Utgångspunkten vid utvecklandet av identifieringen av företag är att den ska bygga på de identifieringslösningar som föreslås i denna proposition. Bestämmelserna om den handläggning och de uppgifter om roller och bemyndiganden som gäller privatpersoner ska beredas särkilt, på samma sätt som identifieringen av företag. Dessa projekt ska ha sin grund i de lösningar som föreslås i denna proposition samt i de bemyndiganden som ska anknytas till elektroniska identifieringsverktyg. Bemyndigandena kan t.ex. gälla förmynderskap eller bevakning av intressen.

3.2 Alternativ för genomförandet

I denna proposition föreslås det en sådan modell för stark elektronisk identifiering som baserar sig på ett förtroendenät. Det föreslås att bestämmelser om förtroendenätets administrativa praxis, tekniska gränssnitt och ansvar ska utfärdas genom förordning av statsrådet.

De aktörer som levererar tjänster för stark elektronisk autentisering omfattas av många olika bestämmelser. Avtalen mellan aktörerna samt de olika samreglerings- och självregleringsåtgärderna kan utgöra ett alternativ till de separata anvisningarna om förtroendenätet. Även om anvisningarna ges endast för särskilda aktörer eller genom förordning av statsrådet, ökar detta nämligen i vilket fall som helst regleringsbördan för de aktörer som levererar identifieringstjänster. I stället för föreskrifter eller övriga styrnings- eller tillsynsåtgärder kan samreglerings- och självregleringsåtgärder vidtas, förutsatt att det på basis av ärendets natur är möjligt att genom samreglerings- och självregleringsåtgärderna trygga uppfyllandet av kraven i lagen på ett sådant sätt att konkurrensen inte äventyras samt på ett öppet, jämlikt och effektivt sätt med tanke på de som levererar och använder tjänsterna.

3.3 De viktigaste förslagen

I propositionen föreslås det att lagen om stark autentisering och elektroniska signaturer ändras så att en definition av förtroendenätet fogas till lagen.

I propositionen föreslås det att behandlingen av personuppgifter ska ändras så att leverantörer av identifieringstjänster samt leverantörer av elektroniska signaturer i framtiden ska kräva personbeteckning i samband med sådan identifiering som hänför sig till en persons ansökan om ett identifieringsverktyg.

I propositionen föreslås det att användningen av uppgifterna i befolkningsdatasystemet ska ändras så att leverantören av identifieringstjänsten samt den certifikatutfärdare som tillhandahåller elektroniska signaturer ska kontrollera att de uppgifter som behövs för leveransen av identifieringstjänsten är uppdaterade i enlighet med uppgifterna i befolkningsdatasystemet.

I propositionen föreslås det att bestämmelsen om inledande identifiering av den som ansöker om ett identifieringsverktyg ska ändras så att en identitet som har verifierats elektroniskt alltid ska basera sig på en fysisk inledande identifiering genom en identitetshandling som en myndighet har beviljat, eller på en elektronisk identifiering som har skett genom att en befintlig identitet verifierats elektroniskt.

I lagen föreslås dessutom en bestämmelse om ett nätverk för leverantörer av identifieringstjänster som ska utgöra ett öppet förtroendenät mellan identifieringstjänsterna.

De föreslagna bestämmelserna gäller endast den verksamhet som bedrivs av de leverantörer av tjänster för stark autentisering som har lämnat en anmälan till Kommunikationsverket.

4 Propositionens konsekvenser

4.1 Inledning

I propositionen föreslås ett förtroendenät för leverantörerna av identifieringstjänster. Nätet får många positiva konsekvenser för användarna, leverantörerna av identifieringstjänster, leverantörerna av elektroniska tjänster och för övriga som producerar tilläggstjänster. I och med förtroendenätet skapas ett verktyg för stark elektronisk autentisering som ger användarna tillgång till flera olika elektroniska tjänster. Användaren kan fritt välja det lämpligaste identifieringsverktyget, eller att eventuellt använda flera identifieringsverktyg parallellt. Genom propositionen strävar man efter att minska kostnaderna för elektronisk identifiering för alla aktörer, men eftersom utbudet av identifieringstjänster är marknadsbaserat, är det möjligt att de avgifter som användarna betalar för de elektroniska identifieringstjänsterna stiger. För leverantörerna av elektroniska tjänster innebär förtroendenätet att praktiskt taget alla de användare som innehar ett elektroniskt identifieringsverktyg kan bli kunder utan att det för identifiering tas ut avtalsavgifter mellan olika leverantörer av identifieringstjänster. På så sätt skapas det förutsättningar för en utveckling av nya elektroniska tjänster som baserar sig på stark elektronisk autentisering.

Propositionen inverkar på identifieringen av den som ansöker om ett identifieringsverktyg i och med att man tidigare har varit tvungen att ansöka om verktyget för stark elektronisk autentisering personligen. Som en följd av de föreslagna ändringarna behövs det ingen fysisk inledande identifiering, om användaren redan har ett verktyg för stark elektronisk autentisering. Ansökan om ett nytt identifieringsverktyg kan även göras elektroniskt. Den leverantör av identifieringstjänster som ska utföra den inledande identifieringen får för att kunna göra den på ett tillförlitligt sätt utnyttja den inledande identifiering som har gjorts av en annan leverantör av identifieringstjänster, men ansvarar dock för eventuella fel i den elektroniska inledande identifieringen. De nuvarande bankkoderna kan i fortsättningen användas som förut, med beaktande av att det kan krävas eventuella ändringar när samtliga bestämmelser i Europaparlamentets och rådets förordning om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden träder i kraft 2018.

I propositionen föreslås det att de uppgifter som ska anknytas till identifieringsverktyget ska kontrolleras i befolkningsdatasystemet, vilket säkerställer den inledande identifieringens tillförlitlighet. Vid uppfyllandet av kravet ska det dock beaktas att de uppgifter som ska kontrolleras hos Befolkningsregistercentralen endast ska användas för den inledande identifieringen.

4.2 Ekonomiska konsekvenser

De debiteringar av användare som gäller stark elektronisk autentisering omfattar för närvarande cirka 88 miljoner euro per år. Detta är en uppskattning av den nationella sammanlagda omsättningen av stark elektronisk autentisering. Kostnaderna för leverans av stark elektronisk autentisering gäller inledande identifiering, utdelning av identifieringsverktyg samt användning och upprätthållande av identifieringstjänsten. På grund av att de olika aktörernas verksamhetsmodeller är mycket olika, varierar också leveranskostnaderna för identifieringstjänsterna mycket. Dessutom medför ingåendet av avtal och administreringen av dem kostnader, liksom de stödtjänster och clearingtjänster som hänför sig till identifieringstjänsterna.

Största delen av debiteringarna hänför sig till användningen av de elektroniska identifieringsverktygen. Den största andelen utgörs av de månadsavgifter som tas ut hos konsumenterna för användningen av nätbankkoderna, nämligen cirka 72 miljoner euro. Avgiften för användningen av en nätbankkod är vanligen 0–2,5 euro, och den ingår ofta i avgifterna för de övriga tjänster som banken tillhandahåller. Hittills har teleoperatörerna inte tagit ut användningsavgifter, men i teleoperatörernas prislistor har det angetts månadsavgifter på cirka 1 euro och 7 euro per transaktion. Den näst största andelen av debiteringarna utgörs av de avgifter per transaktion och månad som tas ut av leverantörer av elektroniska tjänster, sammanlagt cirka 16 miljoner euro.

De olika aktörernas priser varierar i hög grad, eftersom leverantörerna av identifieringstjänster orsakas kostnader för behövlig

it-infrastruktur, administrativa tjänster och stödtjänster samt leverans och utdelning av identifieringsverktyg. De olika aktörernas kostnader bedöms uppgå till cirka 8 miljoner euro endast för upprätthållandet av den it-infrastruktur som behövs för elektronisk identifiering. Kostnaderna för administrativa tjänster och stödtjänster kan anses innefatta t.ex. kostnader för inledande identifiering och för administrering och arkivering av avtal. Leveransen och utdelningen av identifieringsverktyg medför kostnader för cirka 6 miljoner euro för leverantörerna av identifieringstjänster. Dessa kostnader orsakas i huvudsak av att bankerna måste skicka nätbankkoderna till kunderna per post.

Efter att de ändringar som föreslås i propositionen har genomförts kommer det fortfarande att uppstå kostnader för nya identifieringsverktyg som skapas med befintliga identifieringsverktyg, för utdelningen och användningen av identifieringsverktyg samt för den infrastruktur som hänför sig till leveransen av dessa. Även i fortsättningen kommer den största delen av avkastningen att komma av användningen av identifieringsverktyg och identifieringstjänster, och användarna kommer fortsättningsvis att betala den största delen av kostnaderna. Nivån på de totala kostnaderna kommer att sjunka i och med förslaget, men eftersom förslaget inte innebär att aktörerna tvingas följa en viss verksamhetsmodell, är det svårt att förutse riktningen. Därför har man utarbetat tre olika scenarier för bedömningen av konsekvenserna: ett försiktigt scenario, ett scenario med stora förändringar samt ett scenario där bankerna inte har slutna identifieringstjänster. Enligt det scenario där bankerna inte har slutna identifieringstjänster sker övergången till förtroendenätet snabbt både när det gäller banktjänsterna och de övriga leverantörerna av identifieringstjänster.

Enligt det försiktiga scenariot minskar den nuvarande kostnaden per transaktion med cirka 20 procent, och enligt den största förändringen med minst 50 procent.

Enligt det försiktiga scenariot utgår man från att volymerna av banktjänsterna inte förändras, medan de enligt de två andra scenarierna förväntas öka med cirka 5 procent per år med den nuvarande takten. Antalet övriga identifieringstransaktioner ökar enligt alla de tre scenarierna med 20 procent per år. I det scenario där bankerna inte har slutna identifieringstjänster slopas bankkoderna småningom under de följande 10 åren då bankerna övergår till att använda andra identifieringstjänster som tillhandahålls på marknaden.

Enligt det försiktiga scenariot kommer övergången till förtroendenätet för banktjänsternas del att ske långsammare jämfört med den övriga elektroniska identifieringen. Dessutom får marknaden nya aktörer, vilket inte sker inom bankernas identifiering. Enligt det försiktiga scenariot ökar det totala antalet identifieringstransaktioner med 30 procent under de följande 10 åren. På kort sikt ökar de totala kostnaderna en aning enligt denna modell på grund av överlappande identifieringslösningar, men på lång sikt sjunker de totala kostnaderna med cirka 20 procent.

Enligt det scenario som innebär en stor förändring sker övergången till förtroendenätet för banktjänsternas del fortfarande långsammare jämfört med övriga elektronisk identifiering. Dessutom får marknaden nya aktörer, vilket inte sker inom bankernas identifieringsverksamhet. Enligt den stora förändringens scenario fördubblas antalet identifieringar under de följande 10 åren på grund av att antalet bankkoder ökar. Enligt detta scenario kommer cirka hälften av de stora bankerna att använda och utveckla sina egna slutna identifieringstjänster år 2018. På kort sikt minskar de totala kostnaderna enligt denna modell med cirka 10 procent och sjunker med cirka 35 procent på lång sikt.

Enligt det scenario där bankerna inte har slutna identifieringstjänster sker övergången till förtroendenätet för banktjänsternas del snabbt, liksom för den övriga elektroniska identifieringen. Nya aktörer tillträder marknaden snabbare, även inom bankernas identifiering. Antalet identifieringar fördubblas under de följande 10 åren på grund av att antalet bankkoder ökar. Enligt detta scenario övergår alla banker 2018 stegvis till att använda identifieringstjänster inom förtroendenätet. Enligt detta scenario fördubblas antalet identifieringar under de följande 10 åren och de nya identifieringstjänsterna får en betydande ställning även inom banktjänsterna. På kort sikt minskar de totala kostnaderna enligt

denna modell med cirka 10 procent och sjunker med cirka 50 procent på lång sikt.

4.3 Konsekvenser för myndigheternas verksamhet

De ändringar som föreslås i propositionen inverkar inte på fördelningen av behörigheten mellan myndigheterna eller på användarnas eller företagens ställning och rättigheter, eftersom det är frivilligt för leverantörerna av elektroniska identifieringstjänster att ansluta sig till förtroendenätet.

I och med de föreslagna ändringarna kan den offentliga förvaltningen även konkurrensutsätta den elektroniska identifieringstjänsten. I fråga om offentliga förvaltningens identifieringstjänster bedöms de föreslagna ändringarna minska de totala kostnaderna. Detta leder t.ex. till att antalet användare av identifieringstjänster ökar då det blir lättare för enskilda myndigheter (bl.a. kommuner) att ta i bruk nya elektroniska tjänster.

De föreslagna ändringarna får i viss mån konsekvenser för Kommunikationsverket, vars uppgift att utöva tillsyn över de elektroniska identifieringstjänsterna utvidgas från tillsyn i efterhand mot en kontinuerlig tillsyn över den verksamhet som bedrivs av leverantörer av identifieringstjänster i förtroendenätet. Kommunikationsverkets tillsynsuppgifter och de resurser som det kräver kommer att bedömas noggrannare vid beredningen av de genomförandebestämmelser som gäller Europaparlamentets och rådets förordning om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

Den föreslagna ändringen av skyldigheten hos leverantörerna av identifieringstjänster att kontrollera och uppdatera de personuppgifter som behövs för tillhandahållandet av identifieringstjänster och identifieringsverktyg får i viss mån konsekvenser för försäljningen av Befolkningsregistercentralens avgiftsbelagda prestationer och för antalet registreringar inom befolkningsregisterförvaltningen vid magistraterna, men konsekvenserna bedöms bli ringa.

Ändringarna får inga direkta konsekvenser för verksamheten vid de övriga myndigheterna, och ändringarna inverkar inte på uppgiftsfördelningen mellan staten och kommunerna.

4.4 Konsekvenser för miljön

Ett av syftena med propositionen är att öka de elektroniska tjänsterna och utnyttjandet av dem. Indirekt ökar detta människans trivsel och minskar resandet samt möjliggör bevarandet av den nuvarande samhällsstrukturen, särskilt när det gäller tillgången till tjänster på glesbygden. I och med propositionen kommer t.o.m. över 50 procent av den inledande identifiering av medborgare som sker personligen att kunna skötas elektroniskt, vilket minskar medborgarnas resande.

De föreslagna ändringarna får inga andra betydande miljökonsekvenser.

4.5 Samhälleliga konsekvenser

Den identifieringsmarknad som i enlighet med förslaget bygger på ett förtroendenät stöder ibruktagandet av gemensamma system samt sådana servicehelheter som är mera integrerade och mindre beroende av förvaltnings- och organisationsgränser. Dessa ger både medborgare och företag både fler och bättre elektroniska tjänster som är oberoende av tid och plats.

Ett av syftena med propositionen är att öka utbudet och användningen av elektroniska tjänster och tjänster för elektronisk handläggning. De föreslagna ändringarna gör övergången till elektroniska tjänster enklare, eftersom t.ex. leverantörer av elektroniska tjänster endast behöver ingå avtal med en enda leverantör av identifieringstjänster för att nå alla potentiella kunder.

Den elektroniska identifieringen är en viktig del av den nationella servicearkitektur som finansministeriet bygger upp i enlighet med regeringens beslut. Genom att elektronisk identifiering är lätt att ta i bruk är det lättare att skapa nya tjänster, och dessutom skapas en grund för en mera omfattande digitalisering. De föreslagna komponenterna och tjänsterna ska utarbetas inom programmet för servicearkitekturen.

Användningen av tjänsterna kommer sannolikt att öka snabbast inom förvaltningsområdet för social- och hälsovård.

5 Beredningen av propositionen

5.1 Beredningsskeden och beredningsmaterial

Beredningen av den nationella modellen för elektronisk autentisering inleddes i slutet av 2011 av SITRA. Det första förslaget utarbetades av ett andelslag bestående av olika aktörer.

Finansministeriet och kommunikationsministeriet beredde på begäran av aktörerna år 2013 ett förslag till en statsstyrd modell. Modellen avslogs på grund av konkurrensmässiga och affärsekonomiska skäl.

Den 16 maj 2014 tillsatte finansministeriet en tjänstemannagrupp för att bereda en nationell modell för stark elektronisk autentisering. Efter detta skrevs det sommaren 2014 in i programmet för statsminister Stubbs regering att man ska genomföra en fungerande nationell lösning för elektronisk identifiering.

Tjänstemannagruppens uppgift var att ansvara för beredningen av en nationell modell för stark elektronisk autentisering. Arbetsgruppen stöddes av en referensgrupp med representanter för aktörer som arbetar med elektronisk autentisering, t.ex. för banker, operatörer, IKT-företag och ämbetsverk. Referensgruppen informerades öppet om hur beredningen framskred, och utöver detta utnyttjades referensgruppen i den egentliga beredningen av lagstiftningen.

Propositionen har beretts vid kommunikationsministeriet i samarbete med finansministeriet och den arbetsgrupp som tillsattes för behandlingen av den elektroniska autentiseringen. För att undvika eventuella överlappningar samt motstridigheter med denna proposition och gällande bestämmelser har man vid beredningen av propositionen hört de nuvarande aktörerna inom stark elektronisk autentisering och deras tillsynsorganisationer. Utlåtande om propositionen har begärts av den referensgrupp som följde upp beredningen samt av övriga instanser som har velat yttra sig.

Under beredningen ordnades tillfällen för att höra referensgruppen, och under beredningen av lagstiftningen begärdes utlåtande dessutom skriftligen av aktörerna i branschen.

5.2 Utlåtanden och hur de har beaktats

Under remissförfarandet tog Kommunikationsministeriet emot sammanlagt 40 utlåtanden om utkastet till regeringens proposition samt utkastet till statsrådets förordning. Utlåtandena finns i statsrådets projektregister HARE, ärendenummer KM055:00/2014.

Utlåtandena avvek från varandra avsevärt i fråga om innehållet, eftersom vissa remissinstanser ansåg att projektet och den modell som baserar sig på förtroendenätet ska understödas, medan andra ansåg att det finns stora problem med både utkastet till propositionen och utkastet till förordningen. Leverantörerna av elektroniska tjänster förhöll sig i huvudsak positivt till propositionen. Även de nuvarande teleoperatörerna förhöll sig främst positivt till propositionen. Postsektorn förhöll sig mest kritiskt till propositionen.

Lagens konsekvensbedömningar har kompletterats till de delar de i utlåtandena ansågs vara bristfälliga.

Kravet om sammankopplad inledande identifiering, och särskilt prissättningen av den, ansågs i många utlåtanden som problematisk. På basis av kommentarerna i utlåtandena strök man i propositionen kravet i fråga om en rimlig prissättning för den inledande identifieringen.

Justitieministeriet fäste uppmärksamhet vid motiveringen till lagstiftningsordningen i fråga om avtalsförhållandenas beständighet och begärde en noggrannare specificering av hur lagförslaget inverkar på avtalsförhållandenas beständighet. På basis av denna begäran bedömde man avtalsförhållandenas beständighet och beslutade att stryka det avsnittet från motiveringen till lagstiftningsordningen, eftersom propositionen inte inverkar på beständigheten i fråga om de nuvarande aktörernas avtalsförhållanden.

I många utlåtanden behandlades den starka elektroniska autentisering som gäller utlänningar och övriga som hade lämnats utanför propositionen i fråga om den föreslagna modellen. Justitieministeriet begärde också att den persongrupp vars uppgifter med tanke på jämlikhetsbestämmelsen i 6 § i grundlagen

inte kan kontrolleras i befolkningsdatasystemet ska specificeras särskilt i motiveringen till lagstiftningsordningen. Den grupp av användare som enligt utlåtandena hade lämnats utanför den föreslagna modellen har specificerats samt bedömts i enlighet med 6 § i grundlagen.

I många utlåtanden tog man ställning till den ersättning som ska betalas för de identifieringsuppgifter som skickas mellan leverantörerna av identifieringstjänster. På basis av utlåtandena strök man den bestämmelse som gäller ersättningen från utkastet till statsrådets förordning, och fogade den i stället till den nya bestämmelsen om förtroendenätet i utkastet till regeringspropositionen. Syftet med prisregleringen är att förebygga eventuella störningar på marknaden.

I enlighet med justitieministeriets begäran har propositionen preciserats även i fråga om bemyndigandena att utfärda förordning.

De kommentarer i utlåtandena som gällde utkastet till statsrådets förordning beaktas separat vid den fortsatta beredningen av förordningen.

DETALJMOTIVERING

1 Lagförslag

2 §. *Definitioner*. I propositionen föreslås det att till paragrafen fogas en ny definition som gäller förtroendenät. I propositionen föreslås det dessutom att 12 och 13 punkten i definitionerna ändras, eftersom bindeorden och skiljetecknen i dessa punkter måste ändras till följd av tillägget av den nya 14 punkten.

Enligt den nya 14 punkten i definitionerna avses med förtroendenät de leverantörer av identifieringstjänster som har gjort en anmälan till Kommunikationsverket.

Leverantörerna av elektroniska identifieringstjänster utgör i förtroendenätet ett kompatibelt tekniskt och administrativt nätverk. Användarna av identifieringstjänsterna kan utnyttja nätverket genom att ingå avtal med en eller flera leverantörer av identifieringstjänster och använda det erhållna verktyget för stark autentisering i alla de elektroniska tjänster där identifieringsverktyget godkänns. En leverantör av elektroniska tjänster kan utnyttja nätverket genom att med en leverantör av identifieringstjänster ingå avtal om förmedling av identifieringsuppgifter, och leverantören kan använda alla identifieringstjänster som omfattas av förtroendenätet och de identifieringsverktyg som de leverantörer av identifieringstjänster som hör till förtroendenätet har gett ut. Närmare bestämmelser om nätverket för leverantörer av identifieringstjänster föreslås i den föreslagna 12 a §.

6 §. *Behandling av personuppgifter*. I propositionen föreslås det att 6 § 3 mom. ändras så att när leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller elektroniska signaturer kontrollerar sökandens identitet ska de kräva att han eller hon uppger sin personbeteckning. Enligt 3 mom. i den gällande lagen får leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller elektroniska signaturer när de kontrollerar sökandens identitet kräva att han eller hon uppger sin personbeteckning.

Den föreslagna ändringen inverkar inte på leverantörerna av identifieringstjänsters praktiska processer, eftersom leverantörerna av identifieringstjänster enligt vedertagen praxis begär att sökanden ska uppge sin personbeteckning när de kontrollerar sökandens identitet. Den föreslagna ändringen syftar till att förtydliga gällande praxis vid kontrollen av en användares identitet.

7 §. *Användning av uppgifter i befolkningsdatasystemet.* I propositionen föreslås det att rubriken för 7 § ändras så att den är användning av uppgifter i befolkningsdatasystemet, eftersom det bättre motsvarar innehållet.

Enligt det föreslagna momentet ska leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller elektroniska signaturer inhämta och uppdatera uppgifterna

de behöver för tillhandahållandet av identifieringstjänster ur befolkningsdatasystemet. En leverantör av identifieringstjänster ska när den skickar en identifieringsuppgift som gäller ett identifieringsverktyg till en annan leverantör av identifieringstjänster alltid förmedla åtminstone uppgiften som identifierar en person. En uppgift som identifierar en person kan vara personbeteckningen eller en annan beteckning som är individuell och utifrån vilken personens personbeteckning på ett tillförlitligt sätt kan kontrolleras i befolkningsdatasystemet. Utöver detta föreslås det i momentet att leverantörer av identifieringstjänster ska säkerställa att uppgifterna som de behöver för tillhandahållandet av identifieringstjänster är uppdaterade i relation till uppgifterna i befolkningsdatasystemet.

I propositionen begränsas inte de uppgifter som en leverantör av identifieringstjänster som identifierat en slutanvändare ska förmedla utöver uppgiften som identifierar personen, eftersom man i propositionen vill skapa förutsättningar för leverantörerna av identifieringstjänster att utveckla och tillhandahålla olika tilläggstjänster. Om leverantörerna av identifieringstjänster utöver den uppgift som identifierar en person förmedlar även andra personuppgifter än de uppgifter som anges i 6 § i lagen om stark autentisering och elektroniska signaturer, tillämpas på dessa uppgifter annan lagstiftning om behandling av personuppgifter.

Genom den föreslagna ändringen strävar man efter att etablera befolkningsdatasystemets ställning som primärt datalager vid inhämtning och uppdatering av uppgifter som är avsedda för tillhandahållande av identifieringstjänster.

Den viktigaste orsaken till att grunderna för beviljande av identifieringsverktyg kopplas till att personuppgifterna inhämtas ur befolkningsdatasystemet är att säkerställa uppgiften som identifierar en person och som ska fogas till identifieringsverktyget. En uppgift som identifierar en person kan vara personbeteckningen som registrerats i befolkningsdatasystemet eller en elektronisk kommunikationskod, och för upprätthållandet av uppgifterna svarar en myndighet. Genom den föreslagna ändringen vill man säkerställa att det identifieringsverktyg som överlåtits till en person kopplas till uppgiften som identifierar en person och som finns i myndighetsregistret, och att detta alltid sker på samma sätt oberoende av leverantören av identifieringstjänster.

För att kunna beviljas ett verktyg för stark autentisering ska en persons personbeteckning vara registrerad i befolkningsdatasystemet. Personer vars uppgifter finns i befolkningsdatasystemet kan identifieras av en leverantör av identifieringstjänster. I 7 § i lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster föreskrivs det om föremål för registrering som ska registreras i befolkningsdatasystemet och i 9 § om förutsättningar för registrering av utländska medborgare.

Av den föreslagna ändringen följer att en del av personerna som använder elektroniska identifieringstjänster inte omfattas av systemet enligt den föreslagna modellen. Personer vars uppgifter inte kan kontrolleras i befolkningsdatasystemet ska av de nuvarande leverantörerna av identifieringstjänster erbjudas tjänster för elektronisk identifiering på samma sätt som de för närvarande erbjuds identifieringsverktyg och identifieringstjänster. Sådana identifieringsverktyg och identifieringstjänster används i de egna tjänster som den som gett ut identifieringsverktyget tillhandahåller eller i andra tjänster som godkänner identifieringsverktyget. I dessa fall kan identifieringsverktyget inte användas för att med hjälp av ett befintligt identifieringsverktyg skapa ett identifieringsverktyg som avses i lagen om stark autentisering och elektroniska signaturer. Det föreslås att leverantörer av elektroniska tjänster och leverantörer av identifieringstjänster i de fall som nämns ovan ska avtala om godkännande av identifieringsverktyg och därmed sammanhängande ansvarsfrågor från fall till fall.

Det beräknas finnas få personer vars uppgifter inte kan kontrolleras i befolkningsdatasystemet. Tidigare kunde vissa utlänningar som fått uppehållstillstånd inte registreras i befolkningsdatasystemet, eftersom de inte hade en identitetshandling. I och med den ändring av lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster som trädde i kraft den 1 mars 2014 kan man i undantagsfall kontrollera tillförlitligheten hos personuppgifter som ska

registreras även med hjälp av annat än en officiell handling i original. En utländsk medborgare kan således ges en personbeteckning och personens personuppgifter kan registreras i befolkningsdatasystemet, trots att personen inte kan uppvisa pass eller andra tillförlitliga identitetshandlingar.

12 a §. *Nätverk för leverantörer av identifieringstjänster.* Det föreslås att det till lagen fogas en ny paragraf om nätverk för leverantörer av identifieringstjänster.

I 1 mom. föreslås en bestämmelse om anslutning till förtroendenätet. När en leverantör av identifieringstjänster gör en anmälan till Kommunikationsverket enligt 10 § i lagen om stark autentisering och elektroniska signaturer ansluter sig leverantören av identifieringstjänster till förtroendenätet. För att godkännas som en leverantör av tjänster för stark autentisering ska leverantören av identifieringstjänster alltså göra en anmälan till Kommunikationsverket. Identifieringstjänster kan tillhandahållas också utan att det görs en anmälan till Kommunikationsverket, men i detta fall anses leverantören av identifieringstjänster inte vara en leverantör av tjänster för stark autentisering. En leverantör av identifieringstjänster som hör till förtroendenätet är skyldig att iaktta bestämmelserna i lagen om stark autentisering och elektroniska signaturer, såsom de allmänna skyldigheterna för leverantörer av identifieringstjänster. Syftet med den nationella elektroniska identifieringen ska alltid vara tillräckligt säkra lösningar med beaktande av den tekniska utvecklingen på identifieringsmarknaden och datasäkerhetskraven. I Finland ska datasäkerhetskraven granskas genom en jämförelse av de nationella kraven och kraven i de övriga EU-medlemsländerna i fråga om säkerhetsnivåer.

Kommunikationsverket utövar med stöd av 42 § i lagen om stark autentisering och elektroniska signaturer tillsyn över leverantörerna av tjänster för stark autentisering. Aktörer som inte uppfyller de i 9 § i denna lag avsedda kraven som gäller leverantörer av identifieringstjänster kan inte heller höra till förtroendenätet. Kommunikationsverket övervakar eventuella oegentligheter med stöd av 45 § och 12 § 2 mom. i lagen om stark autentisering och elektroniska signaturer. Om en leverantör av identifieringstjänster bryter mot denna lag eller mot föreskrifter som har utfärdats med stöd av den, kan Kommunikationsverket ålägga denne att avhjälpa felet eller försummelsen. Beslutet kan förenas med vite eller med hot om att verksamheten kommer att avbrytas helt eller delvis eller att den försummade åtgärden kommer att vidtas på den försumliges bekostnad.

I 2 mom. föreslås bestämmelser om administrativ praxis som säkerställer att de tjänster som tillhandahålls av leverantörer av identifieringstjänster och av tjänsteleverantörer som använder dessa identifieringstjänster är kompatibla. Det föreslås att det i samma moment föreskrivs om de tekniska gränssnitt som förtroendenätet förutsätter och som möjliggör den tekniska kompatibiliteten mellan aktörerna som tillhandahåller identifieringstjänster och aktörerna som utnyttjar dessa tjänster.

Propositionen syftar inte till att skapa nya gränssnitt som ska erbjudas klienterna eller att ålägga skyldighet att ta i bruk nya gränssnitt, utan avsikten är att leverantörerna av identifieringstjänster inom förtroendenätet använder ett gränssnitt, vilket innebär att leverantörerna av elektroniska tjänster inte föranleds kostnader för utvecklande av nya gränssnitt eller anslutning till dem. Leverantörerna av identifieringstjänster ska alltså komma överens om vilket gränssnitt som används, och därför anger inte myndigheten ett visst gränssnitt eller en beskrivning av det. I propositionen tas det inte ställning till genom vilka tekniska gränssnitt identifieringstjänster ska säljas till leverantörer av elektroniska tjänster, men det skulle vara kostnadseffektivt att iaktta de standarder som används allmänt i gränssnitten.

I 3 mom. föreslås bestämmelser om ersättningar mellan leverantörer av elektroniska identifieringstjänster när identifieringsuppgifter förmedlas mellan två olika leverantörer av identifieringstjänster. I fråga om identifieringsuppgifter som förmedlas och som alltid ska innehålla åtminstone uppgiften som identifierar en person får ersättningen vara högst 10 cent.

Ersättningen ska betalas till den som skickar uppgifterna, eftersom vägran att ta ut ersättning kan skapa ett fripassagerarproblem

på marknaden för stark autentisering. Vid denna störning på marknaden kan det uppstå en situation där en medlem i förtroendenätverket som är fripassagerare antingen mycket billigt eller kostnadsfritt kan tillhandahålla leverantörer av elektroniska tjänster sådana identifieringstjänster som de andra leverantörerna av identifieringstjänster i förtroendenätet bekostat, varvid möjligheterna för leverantörerna av identifieringstjänster att tjäna pengar kan begränsas till endast avgifterna som tas ut av användarna.

Leverantörerna av identifieringstjänster kan genom ömsesidiga avtal även komma överens om ett lägre pris eller en lägre prissättning som möjliggör en ersättning som är oberoende av antalet identifieringstransaktioner. Den genomsnittliga ersättningen för en identifieringsuppgift som förmedlas får dock inte överstiga maximiersättningen på 10 cent.

Om en leverantör av identifieringstjänster är både en aktör som beviljar identifieringsverktyg och en aktör som förmedlar identifieringsuppgifter behöver en intern ersättning för förmedlade identifieringsuppgifter inte tas ut.

Nivån på ersättningens maximibelopp kommer att bedömas årligen med beaktande av i synnerhet förändringarna på identifieringsmarknaden. Kommunikationsverket ska i egenskap av den myndighet som utövar tillsyn över leverantörerna av identifieringstjänster i förtroendenätet tillsammans med de behöriga myndigheterna och medlemmarna i förtroendenätet vid ett sammanträde som ordnas en gång per år bedöma förändringarna på identifieringsmarknaden i fråga om i synnerhet den tekniska utvecklingen och säkerhetsnivåerna.

I 4 mom. föreslås bestämmelser om skyldigheten för leverantörerna av identifieringstjänster och deras ansvar att samarbeta på så sätt att de tekniska gränssnitten och administrativa praxisen är kompatibla. I momentet föreskrivs en samarbetsskyldighet för leverantörerna av identifieringstjänster och syftet med den är att de tekniska gränssnitten och administrativa praxisen enligt 1 mom. ska kunna användas mellan leverantörerna av identifieringstjänster.

I 5 mom. föreslås det att närmare bestämmelser om förtroendenätets administrativa praxis, tekniska gränssnitt och ansvar ska utfärdas genom förordning av statsrådet.

17 §. *Identifiering av den som ansöker om ett identifieringsverktyg.* I propositionen föreslås det att rubriken för 17 § ändras så att den är identifiering av den som ansöker om ett identifieringsverktyg i stället för som tidigare inledande identifiering av den som ansöker om ett identifieringsverktyg, eftersom detta bättre motsvarar innehållet.

I 1 mom. föreskrivs det om två sätt på vilka identifiering kan göras. Ett; om sökanden inte har ett tidigare verktyg för stark autentisering enligt denna lag ska identifieringen göras personligen. Två; om sökanden redan har ett verktyg för stark autentisering får det identifieringsverktyg som avses i denna lag sökas elektroniskt.

I 2 mom. föreskrivs det om hur den personliga identifiering som avses i 1 mom. ska göras. Paragrafen motsvarar till innehållet det gällande 17 § 1 mom. I fråga om 2 mom. i paragrafen bör det betonas att ett identifieringsverktyg får beviljas även med stöd av en annan än en finsk identitetshandling, om personens uppgifter finns i befolkningsdatasystemet. På så sätt kan man försäkra sig om att myndigheten har kontrollerat en persons identitetshandlingar och att personens uppgifter har registrerats i befolkningsdatasystemet.

I 3 mom. föreslås det bestämmelser om undantag i det fall att identiteten hos den som ansöker om ett identifieringsverktyg inte kan verifieras på ett tillförlitligt sätt. Momentet motsvarar 17 § 4 mom. i den gällande lagen.

I 4 mom. föreslås bestämmelser om elektronisk ansökan om ett identifieringsverktyg. Ansökan om ett identifieringsverktyg kan göras både elektroniskt med hjälp av befintliga identifieringsverktyg som har getts ut av leverantörer av identifieringstjänster som gjort en anmälan till Kommunikationsverket och med hjälp av helt nya identifieringsverktyg som har getts ut av leverantörer av identifieringstjänster som i framtiden gör en anmälan till Kommunikationsverket. I praktiken innebär detta att en ansökan om ett identifieringsverktyg kan göras med hjälp av ett befintligt verktyg för stark autentisering och att leverantörerna av identifieringstjänster som hör till förtroendenätet ska säkerställa att

identifieringsverktygen som de har gett ut används när nya identifieringsverktyg skapas med hjälp av befintliga identifieringsverktyg. Ett befintligt identifieringsverktyg ska kunna användas för att ansöka om ett motsvarande identifieringsverktyg.

Stark autentisering enligt denna lag avser identifiering av en person och verifiering av identifikatorns autenticitet och riktighet genom tillämpning av en elektronisk metod. Identifieringen och verifieringen grundar sig på minst två av följande tre alternativ: a) ett lösenord eller någonting annat som en innehavare av ett identifieringsverktyg vet, b) ett smartkort eller någonting annat som en innehavare av ett identifieringsverktyg har i sin besittning, eller c) fingeravtryck eller någon annan egenskap som identifierar en innehavare av ett identifieringsverktyg. Svag autentisering är elektronisk identifiering som inte uppfyller den definition som anges ovan. Av metoderna som tillämpas vid svag autentisering är den mest använda användarnamn–lösenord. Svag autentisering regleras inte i lag.

I 4 mom. föreslås det dessutom bestämmelser om att den aktör som litar på den identifiering som en leverantör av identifieringstjänster gjort bär ansvaret om identifieringen är felaktig. Vid övervägandet av ansvarsfrågor ska det beaktas att när en leverantör av identifieringstjänster beviljar ett identifieringsverktyg som avses i 2 § 1 mom. 2 punkten i den gällande lagen har den ursprungliga inledande identifieringen gjorts i enlighet med 17 § i denna lag.

Vid beredningen av propositionen ansågs det inte ändamålsenligt att reglera priset på inledande identifiering eller priset på att det med hjälp av ett befintligt identifieringsverktyg skapas ett nytt identifieringsverktyg. De ovannämnda priserna fastställs således på marknadsvillkor. Målet är dock att prissättningen av den inledande identifieringen ska vara transparent och icke-diskriminerande. Leverantörerna av identifieringstjänster får med stöd av andra privaträttsliga bestämmelser sinsemellan avtala om eventuella ersättningar som tas ut i samband med inledande identifiering.

Propositionen säkerställer att leverantörerna av identifieringstjänster, om de så önskar, kan erbjuda leverantörer av elektroniska tjänster tilläggstjänster. En leverantör av identifieringstjänster kan, om den så önskar, tillhandahålla t.ex. en tjänst som möjliggör övervakning av kedjan av stark autentisering av en person. I detta fall kan den som skaffar tilläggstjänsten t.ex. kontrollera uppgifterna om vilken aktör som har beviljat det föregående identifieringsverktyget, men i propositionen förutsätts det dock inte att leverantörerna av identifieringstjänster ska föra ett sådant register.

2 Ikraftträdande

Lagen föreslås träda i kraft den 1 maj 2015. Lagens 12 a § ska dock tillämpas först från den 1 maj 2017.

En övergångsperiod på två år från lagens ikraftträdande föreslås för medlemmarna i förtroendenätet för utvecklande av förtroendenätets tekniska och administrativa beredskap. Två år efter lagens ikraftträdande, dvs. efter det att den tekniska och administrativa beredskapen har utvecklats kan aktörerna i förtroendenätet ta i bruk systemen de utvecklat och då blir även den föreslagna 12 a § tillämplig.

3 Förhållande till grundlagen samt lagstiftningsordning

3.1 Näringsfrihet

Betydelsefulla med tanke på näringsfriheten enligt grundlagen är bestämmelserna i 12 a § i förslaget, vilka gäller nätverket för leverantörer av identifieringstjänster.

Enligt 18 § i grundlagen har var och en i enlighet med lag rätt att skaffa sig sin försörjning genom arbete, yrke eller näring som han eller hon valt fritt. Grundlagsutskottet har behandlat förhållandet mellan anmälningsskyldighet och näringsfrihet t.ex. i utlåtandet GrUU 54/2002 rd (lagen om domännamn).

Enligt 10 § i lagen om stark autentisering och elektroniska signaturer är leverantörer av identifieringstjänster skyldiga att skriftligen anmäla att verksamheten inleds till Kommunikationsverket. Enligt det föreslagna 12 a § 1 mom. i denna proposition ansluter sig en

leverantör av identifieringstjänster till förtroendenätet när leverantören gör en anmälan till Kommunikationsverket enligt 10 § i lagen om stark autentisering och elektroniska signaturer. Anslutningen till förtroendenätet som sådan kräver inte att en separat anmälan görs till Kommunikationsverket. Identifiering av en person baserar sig på de handlingar som anges i 6 § i lagen om stark autentisering och elektroniska signaturer.

Identifieringstjänster kan tillhandahållas också utan att det görs en anmälan till Kommunikationsverket, men i detta fall anses leverantören av identifieringstjänster inte vara en leverantör av tjänster för stark autentisering i enlighet med denna lag. För att kunna godkännas som en tjänst för stark autentisering krävs det att en anmälan görs till Kommunikationsverket.

Grundlagsutskottet har konstaterat att bestämmelser om anmälningsskyldighet inte utgör ett problem ur näringsfrihetssynpunkt, i synnerhet inte då myndigheten inte förväntas fatta några beslut med anledning av anmälan. Kommunikationsverket behöver inte fatta beslut om anslutning till det förtroendenät som föreslås i propositionen. Dessutom har försummande av den föreslagna anmälningsskyldigheten inte belagts med sanktioner.

Leverantörer av identifieringstjänster ska behandla sina klienter på ett icke-diskriminerande och likvärdigt sätt. I praktiken innebär detta att en i lagen om stark autentisering och elektroniska signaturer avsedd leverantör av identifieringstjänster kan vägra att bevilja en person ett elektroniskt identifieringsverktyg endast i det fallet att personens uppgifter inte finns i befolkningsdatasystemet eller personen inte har en i 17 § i lagen om stark autentisering och elektroniska signaturer avsedd identitetshandling som utfärdats av en myndighet eller ett befintligt identifieringsverktyg med hjälp av vilket identiteten kan verifieras. Leverantörer av identifieringstjänster kan tillhandahålla elektroniska identifieringsverktyg som en del av den övriga servicen, men även i dessa fall ska identifieringsverktyget beviljas på ett icke-diskriminerande och likvärdigt sätt. En leverantör av identifieringstjänster har dock rätt att vägra bevilja ett identifieringsverktyg även med stöd av annan förpliktande lagstiftning, såsom skyldigheterna som gäller kundkontroll och identifiering i lagstiftningen om penningtvätt.

Personer vars uppgifter inte kan kontrolleras i befolkningsdatasystemet ska av de nuvarande leverantörerna av identifieringstjänster erbjudas tjänster för elektronisk identifiering på samma sätt som de i nuläget erbjuds elektroniska identifieringsverktyg och identifieringstjänster för användning i de egna tjänster som den som beviljat identifieringsverktyget upprätthåller eller i andra tjänster som godkänner det elektroniska identifieringsverktyget. I dessa fall kan det elektroniska identifieringsverktyget inte användas för att med hjälp av ett befintligt verktyg för stark autentisering skapa ett sådant verktyg för stark autentisering som anges i lagen om stark autentisering och elektroniska signaturer. Det föreslås att leverantörerna av elektroniska tjänster och leverantörerna av identifieringstjänster ska avtala om godkännande av identifieringsverktyg och därmed sammanhängande ansvarsfrågor från fall till fall.

Det beräknas inte finnas särskilt många personer vars uppgifter inte kan kontrolleras i befolkningsdatasystemet. Tidigare kunde vissa utlänningar som fått uppehållstillstånd inte registreras i befolkningsdatasystemet, eftersom de inte hade en identitetshandling. I och med den ändring av lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster som trädde i kraft den 1 mars 2014 kan man i undantagsfall kontrollera tillförlitligheten hos personuppgifter som ska registreras även med hjälp av annat än en officiell handling i original. En utländsk medborgare kan således ges en personbeteckning och personens personuppgifter kan registreras i befolkningsdatasystemet, trots att personen inte kan uppvisa pass eller andra tillförlitliga identitetshandlingar. Registreringen av utlänningar i befolkningsdatasystemet underlättas dessutom av en lagändring som träder i kraft den 1 december 2014. I fortsättningen får Migrationsverket och polisen registrera begränsade basuppgifter om en person i befolkningsdatasystemet i samband med beviljande av uppehållstillstånd och utfärdande av uppehållskort samt registrering av uppehållsrätt. Således borde det i Finland i princip inte finnas utlänningar som vistas här

med stöd av uppehållstillstånd, uppehållskort eller registrerad uppehållsrätt och som inte finns i befolkningsdatasystemet.

Alla utlänningar som vistas i Finland kan i praktiken inte få ett sådant identifieringsverktyg som avses i propositionen trots att de har registrerats i befolkningsdatasystemet. En del av utlänningarna har inga sådana identitetshandlingar, såsom pass eller identitetskort, som behövs för att få ett verktyg för stark autentisering. Man försöker för närvarande lösa problemet i ett av inrikesministeriet tillsatt inledande projekt som gäller behovet av att ändra lagen om identitetskort. Syftet är att utlänningar som har fått uppehållstillstånd och registrerats i befolkningsdatasystemet ska kunna beviljas ett identitetskort för utlänningar trots att de inte har en tillförlitlig identitetshandling.

Enligt 6 § i grundlagen får ingen utan godtagbart skäl 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. Propositionen syftar till att lösa problemet med stark autentisering för den stora allmänheten genom att koppla stark autentisering till uppgifterna som har registrerats i befolkningsdatasystemet. Av ovannämnda orsaker anses detta dock inte försätta någon människogrupp i en ojämlik ställning vid ansökan om identifieringsverktyg.

3.2 Behandling av personuppgifter

Enligt 10 § i grundlagen utfärdas närmare bestämmelser om skydd för personuppgifter genom lag. Enligt regeringens proposition som gäller revideringen av de grundläggande fri- och rättigheterna hänvisar bestämmelsen till behovet av att genom lagstiftning trygga individens rättsskydd och skydd för privatlivet i behandlingen, registreringen och användningen av personuppgifter (RP 309/1993 rd, s.57). Bestämmelsens laghänvisning om skydd för personuppgifter förutsätter enligt syftet med revideringen av de grundläggande fri- och rättigheterna (GrUB 25/1994 rd, s. 6/II) att lagstiftaren utfärdar bestämmelser om denna rättighet, men detaljerna i regleringen är beroende av lagstiftarens prövning.

Grundlagsutskottet har behandlat skydd för personuppgifter bl.a. i utlåtandena GrUU 47/1996 rd (telemarknadslagen), GrUU 26/1998 rd (lagen som gäller datasekretess vid telekommunikation), GrUU 27/1998 rd och GrUU 27a/1998 rd (lagen om integritetsskydd i arbetslivet) och GrUU 25/1998 rd (personuppgiftslagen).

Utskottet har i sina utlåtanden allmänt betonat betydelsen av att de detaljerade bestämmelserna i lagen är exakta. Enligt utskottets utlåtandepraxis omfattas även frågan om hur länge de i personregistren registrerade uppgifterna ska förvaras av det krav på reglering i lag som anges i den nämnda paragrafen i grundlagen. Det är viktigt att reglera åtminstone syftet med registreringen, de registrerade personuppgifternas innehåll, deras tillåtna användningsändamål inbegripet uppgifternas tillförlitlighet och uppgifternas förvaringstid i personregistren samt den registrerades rättssäkerhet. Detsamma gäller i vilken utsträckning dessa omständigheter ska regleras och i så fall hur ingående på lagnivå.

I denna proposition syftar den föreslagna ändringen av 6 § till att förtydliga gällande praxis så att leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller elektroniska signaturer när de kontrollerar sökandens identitet ska kräva att sökanden uppger sin personbeteckning. Den föreslagna ändringen gör tolkningen av bestämmelsen entydigare och motsvarar således grundlagsutskottets krav på att de detaljerade bestämmelserna i lagen ska vara exakta.

Det i denna proposition föreslagna kravet på att leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller elektroniska signaturer ska inhämta och uppdatera uppgifterna de behöver för tillhandahållandet av identifieringstjänster ur befolkningsdatasystemet ökar och preciserar ursprung och användningsändamål i fråga om uppgifterna i anslutning till stark autentisering.

3.3 Bedömning av lagstiftningsordningen

På ovan nämnda grunder kan lagförslagen behandlas i vanlig lagstiftningsordning.

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

Lagförslag

Lag

om ändring av lagen om stark autentisering och elektroniska signaturer

I enlighet med riksdagens beslut

ändras i lagen om stark autentisering och elektroniska signaturer (617/2009) 2 § 12 och 13 punkten, 6 § 3 mom. samt 7 och 17 § samt

fogas till 2 § 1 mom. en ny 14 punkt och till lagen en ny 12 a § som följer:

2 §

Definitioner

I denna lag avses med

— — — — — — — — — — — — — — —

12) *anordning för signaturframställning* programvara eller maskinvara för användning av signaturframställningsdata då en elektronisk signatur skapas,

13) *signaturverifieringsdata* data, såsom koder eller öppna nycklar, som används för att verifiera en elektronisk signatur,

14) *förtroendenät* de leverantörer av identifieringstjänster som har gjort en anmälan till Kommunikationsverket.

6 §

Behandling av personuppgifter

— — — — — — — — — — — — — — —

När leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller elektroniska signaturer kontrollerar sökandens identitet ska de kräva att han eller hon uppger sin personbeteckning. Leverantörerna av identifieringstjänster och certifikatutfärdarna som tillhandahåller elektroniska signaturer får behandla personbeteckningar i sina register i de syften som nämns i 1 mom. Identifieringsverktyg och certifikat får innehålla personbeteckning om verktygets eller certifikatets innehåll är tillgängligt endast för dem som nödvändigt behöver personbeteckningen för att tillhandahålla tjänsten. Personbeteckningen får inte vara tillgänglig i en offentlig katalog.

— — — — — — — — — — — — — — —

7 §

Användning av uppgifter i befolkningsdatasystemet

Leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller elektroniska signaturer ska inhämta och uppdatera uppgifterna de behöver för tillhandahållandet av identifieringstjänster ur befolkningsdatasystemet. Leverantörer av identifieringstjänster ska dessutom säkerställa att uppgifterna som de behöver för tillhandahållandet av identifieringstjänster är uppdaterade i relation till uppgifterna i befolkningsdatasystemet.

En uppgift som lämnas ut ur befolkningsdatasystemet är en offentligrättslig prestation. Bestämmelser om avgiften för en prestation finns i lagen om grunderna för avgifter till staten (150/1992).

12 a §

Nätverk för leverantörer av identifieringstjänster

När en leverantör av identifieringstjänster gör en anmälan till Kommunikationsverket enligt 10 § ansluter sig leverantören av identifieringstjänster till förtroendenätet.

En leverantör av identifieringstjänster som hör till förtroendenätet ska iaktta administrativa praxis som säkerställer att de tjänster som tillhandahålls av leverantörer av identifieringstjänster och av leverantörer av elektroniska tjänster som använder dessa identifieringstjänster är kompatibla samt erbjuda tekniska gränssnitt som skapar förutsättningar för verksamheten mellan aktörerna som tillhandahåller identifieringstjänster och aktörerna som använder tjänsterna.

När en leverantör av elektroniska identifieringstjänster skickar en uppgift som gäller ett elektroniskt identifieringsverktyg till en annan leverantör av elektroniska identifieringstjänster för vidareförmedling, ska det för den förmedlade identifieringsuppgiften betalas en ersättning till den som skickat uppgiften. Ersättningen som tas ut för en förmedlad identifieringsuppgift får uppgå till högst 10 cent. Nivån på ersättningen ska bedömas årligen.

Leverantörerna av identifieringstjänster bär gemensamt ansvaret för att de tekniska gränssnitten och administrativa praxisen är kompatibla.

Närmare bestämmelser om förtroendenätets administrativa praxis, tekniska gränssnitt och ansvar utfärdas genom förordning av statsrådet.

17 §

Identifiering av den som ansöker om ett identifieringsverktyg

Om sökanden inte har ett tidigare verktyg för stark autentisering enligt denna lag ska den inledande identifieringen göras personligen. Om sökanden redan har ett verktyg för stark autentisering får det identifieringsverktyg som avses i denna lag sökas elektroniskt.

När den personliga inledande identifieringen görs ska leverantören av identifieringstjänster noggrant identifiera den som ansöker om ett identifieringsverktyg genom att fastställa identiteten med hjälp av ett giltigt pass eller identitetskort som har utfärdats av en myndighet i en medlemsstat inom Europeiska ekonomiska samarbetsområdet, i Schweiz eller i San Marino. Vid den inledande identifieringen får leverantören, om denne så önskar, även använda ett giltigt körkort som har utfärdats efter den 1 oktober 1990 av en myndighet i en medlemsstat i Europeiska ekonomiska samarbetsområdet eller ett giltigt pass som har utfärdats av en myndighet i någon annan stat.

Om identiteten hos den som ansöker om ett identifieringsverktyg inte kan verifieras på ett tillförlitligt sätt, ska polisen utföra den inledande identifiering som gäller ansökan. De kostnader som polisens inledande identifiering orsakar den som ansöker om ett identifieringsverktyg är en offentligrättslig prestation. Bestämmelser om avgiften för en sådan prestation finns i lagen om grunderna för avgifter till staten.

Med hjälp av ett befintligt verktyg för stark autentisering får det ansökas om ett motsvarande elektroniskt identifieringsverktyg. Den leverantör av tjänster för stark autentisering som litar på en tidigare identifiering bär ansvaret i förhållande till den skadelidande om identifieringen är felaktig.

Denna lag träder i kraft den 20 . Lagens 12 a § tillämpas dock först från den 1 maj 2017.

Helsingfors den 27 november 2014

Statsministerns ställföreträdare, finansminister

ANTTI RINNE

Trafik- och kommunminister *Paula Risikko*

Bilaga
Parallelltext

Lag

om ändring av lagen om stark autentisering och elektroniska signaturer

I enlighet med riksdagens beslut
ändras i lagen om stark autentisering och elektroniska signaturer (617/2009) 2 § 12 och 13 punkten, 6 § 3 mom. samt 7 och 17 §, samt
fogas till 2 § 1 mom. en ny 14 punkt och till lagen en ny 12 a §, som följer:

Gällande lydelse	*Föreslagen lydelse*
2 §	2 §
Definitioner	*Definitioner*
I denna lag avses med	I denna lag avses med
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
12) *anordning för signaturframställning* programvara eller maskinvara för användning av signaturframställningsdata då en elektronisk signatur skapas, och	12) *anordning för signaturframställning* programvara eller maskinvara för användning av signaturframställningsdata då en elektronisk signatur skapas,
13) *signaturverifieringsdata data*, såsom koder eller öppna nycklar, som används för att verifiera en elektronisk signatur.	13) *signaturverifieringsdata* data, såsom koder eller öppna nycklar, som används för att verifiera en elektronisk signatur,
	14) förtroendenät de leverantörer av identifieringstjänster som har gjort en anmälan till Kommunikationsverket.
6 §	6 §
Behandling av personuppgifter	*Behandling av personuppgifter*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
När leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller elektroniska signaturer kontrollerar sökandens identitet får de kräva att han eller hon uppger sin personbeteckning. Leverantörerna och certifikatutfärdarna får behandla personbeteckningar i sina register i de syften som nämns i 1 mom. Identifieringsverktyg och certifikat får innehålla personbeteckning om verktygets eller certifikatets innehåll är tillgängligt endast för dem som nödvändigt be-	När leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller elektroniska signaturer kontrollerar sökandens identitet *ska de kräva* att han eller hon uppger sin personbeteckning. Leverantörerna av identifieringstjänster och certifikatutfärdarna som tillhandahåller elektroniska signaturer får behandla personbeteckningar i sina register i de syften som nämns i 1 mom. Identifieringsverktyg och certifikat får innehålla personbeteckning om verktygets eller

Gällande lydelse	*Föreslagen lydelse*
höver den för att tillhandahålla tjänsten. Personbeteckningen får inte vara tillgänglig i en offentlig katalog.	certifikatets innehåll är tillgängligt endast för dem som nödvändigt behöver personbeteckningen för att tillhandahålla tjänsten. Personbeteckningen får inte vara tillgänglig i en offentlig katalog.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
7 §	7 §
Användning av uppgifter i befolkningsdatasystemet	*Användning av uppgifter i befolkningsdatasystemet*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller elektroniska signaturer får på de grunder som avses i 8 § 1 mom. 1 och 2 punkten i personuppgiftslagen och för de syften som nämns i 6 § 1 mom. i denna lag inhämta personuppgifter ur befolkningsdatasystemet och i systemet kontrollera de personuppgifter som en sökande eller innehavare har uppgett.	Leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller elektroniska signaturer *ska inhämta och uppdatera uppgifterna de behöver för tillhandahållandet av identifieringstjänster ur befolkningsdatasystemet. Leverantörer av identifieringstjänster ska dessutom säkerställa att uppgifterna som de behöver för tillhandahållandet av identifieringstjänster är uppdaterade i relation till uppgifterna i befolkningsdatasystemet.*
En uppgift som lämnas ut ur befolkningsdatasystemet är en offentligrättslig prestation. I fråga om avgiften för en prestation föreskrivs i lagen om grunderna för avgifter till staten (150/1992).	En uppgift som lämnas ut ur befolkningsdatasystemet är en offentligrättslig prestation. Bestämmelser om avgiften för en prestation finns i lagen om grunderna för avgifter till staten (150/1992).
	12 a §
	Nätverk för leverantörer av identifieringstjänster
	När en leverantör av identifieringstjänster gör en anmälan till Kommunikationsverket enligt 10 § ansluter sig leverantören av identifieringstjänster till förtroendenätet.
	En leverantör av identifieringstjänster som hör till förtroendenätet ska iaktta administrativa praxis som säkerställer att de tjänster som tillhandahålls av leverantörer av identifieringstjänster och av leverantörer av elektroniska tjänster som använder dessa identifieringstjänster är kompatibla samt erbjuda tekniska gränssnitt som skapar förutsättningar för verksamheten mellan aktörerna som tillhandahåller identifieringstjänster och ak-

Gällande lydelse	Föreslagen lydelse
	törerna som använder tjänsterna. *När en leverantör av elektroniska identifieringstjänster skickar en uppgift som gäller ett elektroniskt identifieringsverktyg till en annan leverantör av elektroniska identifieringstjänster för vidareförmedling, ska det för den förmedlade identifieringsuppgiften betalas en ersättning till den som skickat uppgiften. Ersättningen som tas ut för en förmedlad identifieringsuppgift får uppgå till högst 10 cent. Nivån på ersättningen ska bedömas årligen.* *Leverantörerna av identifieringstjänster bär gemensamt ansvaret för att de tekniska gränssnitten och administrativa praxisen är kompatibla.* *Närmare bestämmelser om förtroendenätets administrativa praxis, tekniska gränssnitt och ansvar utfärdas genom förordning av statsrådet.*
17 §	17 §
Inledande identifiering av den som ansöker om ett identifieringsverktyg	*Identifiering av den som ansöker om ett identifieringsverktyg*
Den inledande identifieringen ska göras personligen. Leverantören av identifieringstjänster ska noggrant identifiera den som ansöker om ett identifieringsverktyg genom att fastställa identiteten med hjälp av ett giltigt pass eller identitetskort som har utfärdats av en myndighet i en medlemsstat inom Europeiska ekonomiska samarbetsområdet, i Schweiz eller i San Marino. Vid den inledande identifieringen får leverantören, om denne så önskar, även använda ett giltigt körkort som har utfärdats efter den 1 oktober 1990 av en myndighet i en medlemsstat i Europeiska ekonomiska samarbetsområdet eller ett giltigt pass som har utfärdats av en myndighet i någon annan stat. Den inledande identifieringen behöver inte göras personligen, om leverantörer av identifieringstjänster sinsemellan har avtalat om möjligheten att lita på varandras inledande identifieringar. Då kan ansökan om identifieringsverktyg göras elektroniskt. I avtalet ska leverantörerna av identifieringstjänster fastställa hur ansvaret fördelas mellan dem, om den ursprungliga identifieringen är felaktig.	*Om sökanden inte har ett tidigare verktyg för stark autentisering enligt denna lag ska den inledande identifieringen göras personligen. Om sökanden redan har ett verktyg för stark autentisering får det identifieringsverktyg som avses i denna lag sökas elektroniskt.* *När den personliga inledande identifieringen görs ska leverantören av identifieringstjänster noggrant identifiera den som ansöker om ett identifieringsverktyg genom att fastställa identiteten med hjälp av ett giltigt pass eller identitetskort som har utfärdats av en myndighet i en medlemsstat inom Europeiska ekonomiska samarbetsområdet, i Schweiz eller i San Marino. Vid den inledande identifieringen får leverantören, om denne så önskar, även använda ett giltigt körkort som har utfärdats efter den 1 oktober 1990 av en myndighet i en medlemsstat i Europeiska ekonomiska samarbetsområdet eller ett giltigt pass som har utfärdats av en myndighet i någon annan stat.*

Gällande lydelse	*Föreslagen lydelse*
Den leverantör som litar på en inledande identifiering som gjorts av en annan leverantör bär ansvaret i förhållande till den skadelidande.	
Ansökan om identifieringsverktyg kan göras elektroniskt också när sökanden har ett gällande identifieringsverktyg som har getts ut av samma leverantör av identifieringstjänster. Då behöver den inledande identifieringen inte göras på nytt.	
Om identiteten hos den som ansöker om ett identifieringsverktyg inte kan verifieras på ett tillförlitligt sätt, ska polisen utföra den inledande identifiering som gäller ansökan. De kostnader som polisens identifiering orsakar den som ansöker om ett identifieringsverktyg är en offentligrättslig prestation. I fråga om avgiften för en sådan prestation föreskrivs i lagen om grunderna för avgifter till staten.	*Om identiteten hos den som ansöker om ett identifieringsverktyg inte kan verifieras på ett tillförlitligt sätt, ska polisen utföra den inledande identifiering som gäller ansökan. De kostnader som polisens inledande identifiering orsakar den som ansöker om ett identifieringsverktyg är en offentligrättslig prestation. Bestämmelser om avgiften för en sådan prestation finns i lagen om grunderna för avgifter till staten.*
	Med hjälp av ett befintligt verktyg för stark autentisering får det ansökas om ett motsvarande elektroniskt identifieringsverktyg. Den leverantör av tjänster för stark autentisering som litar på en tidigare identifiering bär ansvaret i förhållande till den skadelidande om identifieringen är felaktig.

Denna lag träder i kraft den 20 . Lagens 12 a § tillämpas dock först från den 1 maj 2017.
