Regeringens proposition till riksdagen med förslag till lagar om ändring av lagen om stark autentisering och elektroniska signaturer samt av vissa andra lagar som har samband med den

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

Syftet med denna proposition är att för sin del främja regeringens spetsprojekt för att skapa en tillväxtmiljö för digital affärsverksamhet och att göra lagstiftningen smidigare.

I denna proposition föreslås det att lagen om stark autentisering och elektroniska signaturer ändras. Ändringarna beror huvudsakligen på Europeiska unionens lagstiftning om elektronisk identifiering och betrodda tjänster, såsom elektronisk underskrift.

Enligt propositionen är det Kommunikationsverkets uppgift att övervaka att Europeiska unionens lagstiftning om elektronisk identifiering och betrodda tjänster iakttas.

Minst samma villkor för tillförlitlighet och informationssäkerhet ska krävas av de system för stark autentisering som används i Finland som det i Europeiska unionens lagstiftning med tillitsnivån väsentlig krävs av de system för elektronisk identifiering som överskrider unionens gränser. Ett nytt krav på leverantörer av elektroniska identifieringstjänster som införs enligt förslaget är skyldighet för dem att påvisa att tjänsterna uppfyller kraven.

Det är Kommunikationsverkets och Befolkningsregistercentralens uppgift att i Finland genomföra de åtgärder som Europeiska unionens system för interoperabilitet i elektronisk identifiering kräver.

Leverantörer av elektroniska identifieringsverktyg och leverantörer av tjänster för identifieringsförmedling som agerar i ett förtroendenätverk för elektronisk identifiering definieras och de olika aktörernas skyldigheter enligt den gällande lagen preciseras. Ett verktyg för stark autentisering ska inte längre kunna beviljas enbart på basis av körkort i Finland eller i någon annan stat inom Europeiska ekonomiska samarbetsområdet från ingången av 2019. Namnet på lagen ändras samtidigt så att det bättre motsvarar innehållet i lagen.

De hänvisningar som finns någon annanstans i lag till lagen om stark autentisering och elektroniska signaturer ändras till hänvisningar till lagen om stark autentisering och betrodda elektroniska tjänster eller till EU:s förordning om elektronisk identifiering och betrodda tjänster.

I propositionen föreslås det dessutom ändringar i lagen om elektronisk kommunikation i myndigheternas verksamhet, lagen om kommunikationsförvaltningen, jordabalken, lagen om förhindrande och utredning av penningtvätt och av finansiering av terrorism, lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster, lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården, lagen om beskattningsförfarande, lagen om överlåtelseskatt, lagen om förskottsuppbörd, blodtjänstlagen, mervärdesskattelagen, skattekontolagen, lagen om informationssystemet för byggnaders energicertifikat och punktskattelagen. Dessa ändringar är i huvudsak laghänvisningar och andra tekniska ändringar.

Lagarna avses träda i kraft den 1 juli 2016.

INNEHÅLL

ALLMÄN MOTIVERING

1 Inledning

Tjänsterna för elektronisk identifiering och elektroniska underskrifter ger för sin del allmänheten möjligheter att använda elektroniska tjänster. De offentliga och kommersiella elektroniska tjänsterna som kräver stark autentisering av personer ökar. I Finland regleras tillhandahållandet av och kvaliteten på stark autentisering och certifikattjänster för elektroniska underskrifter genom lag.

Europaparlamentet och rådet har utfärdat förordningen (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden (nedan EU:s förordning om elektronisk identifiering eller eIDAS-förordningen). I förordningen motiverades ett system för interoperabilitet i elektronisk identifiering med syftet att i framtiden möjliggöra att man med elektroniska identifieringsverktyg som beviljats i en medlemsstat kan identifiera sig i en annan medlemsstat i offentliga eller privata tjänster som kräver elektronisk identifiering. Ett interoperabilt system för elektronisk identifiering som omfattar hela EU har krävt att gemensamma tillitsnivåer för elektronisk identifiering fastställs på EU-nivå. Enligt förordningen måste den offentliga förvaltningen i bruket av sina elektroniska tjänster även godkänna bruket av identifieringsverktyg med motsvarande tillitsnivå från en annan medlemsstat från och med hösten 2018. Detta medför uppgifter för finländska myndigheter som gäller verkställande och tillsyn och som enligt förslaget regleras i denna regeringsproposition.

eIDAS-förordningen träder i kraft stegvis. Sommaren 2016 träder föreskrifter om betrodda tjänster såsom elektronisk underskrift och elektronisk stämpel i kraft som direkt ska tillämpas i medlemsstaterna. Avsikten med förordningen är att förenhetliga bestämmelserna om betrodda tjänster i EU. Det föreslås att ändringarna i den nationella lagstiftningen som följd av det görs genom denna regeringsproposition.

Utöver de europeiska ändringarna ändras också den nationella marknaden för elektronisk identifiering genom de föreskrifter om ett förtroendenätverk för stark autentisering som riksdagen antog 2015. Två slag av aktörer är verksamma i förtroendenätet: leverantörer av identifieringsverktyg och leverantörer av tjänster för identifieringsförmedling. Det föreslås att olika aktörers skyldigheter preciseras genom denna proposition.

2 Nuläge

2.1 Elektronisk identifiering

I nuläget utnyttjas elektroniska verktyg för stark autentisering huvudsakligen av tre servicesektorer: bank- och försäkringstjänster, servicen inom den offentliga förvaltningen samt övriga privata tjänster. Mätt i antalet identifieringstransaktioner är de elektroniska tjänster som erbjuds av bank- och försäkringssektorn samt den offentliga förvaltningen de mest betydande. I framtiden förväntas användningen av elektronisk identifiering öka i servicen inom den offentliga förvaltningen och i handeln på webben.

Tjänster för stark autentisering produceras för närvarande av banker, mobilföretag och Befolkningsregistercentralen. Tillsynen över aktörernas verksamhet inom stark autentisering sköts av Kommunikationsverket som även ansvarar för registreringen av leverantörerna av stark autentisering.

Bankkoderna innehar den största marknadsandelen i fråga om antalet användare och transaktioner när det gäller identifieringsverktyg för allmänheten. Mobilföretagens mobilcertifikat

samt medborgarcertifikat som anknyts till de identitetskort som Befolkningsregistercentralen ger ut har inte uppnått en betydande ställning på marknaden för elektronisk identifiering inom de tjänster som erbjuds allmänheten. Med mobilcertifikatet är det möjligt att använda största delen av de elektroniska tjänster som tillhandahålls, men vanligen inte banktjänsterna.

Vid beredningen av lagen om stark autentisering och elektroniska signaturer (617/2009, nedan även autentiseringslagen) 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 autentisering skulle kunna användas i större utsträckning i olika tjänster både inom den privata och inom den offentliga sektorn. Av de ovan nämnda skälen antog riksdagen i början av 2015 bestämmelser om ett nätverk för leverantörer av identifieringstjänster i autentiseringslagen (RP 272/2014 rd). Genom föreskrifterna i 12 a § skapas möjligheter för att ett omfattande förtroendenät ska uppkomma.

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

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

I de flesta elektroniska kundtjänster som produceras av den offentliga sektorn är det möjligt att identifiera sig med alla de identifieringsverktyg som används av de leverantörer av stark autentisering som har lämnat en anmälan till Kommunikationsverket. En del av den offentliga förvaltningens tjänster godkänner dock inte alla identifieringsverktyg till exempel 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 utarbetas en gemensam styrningstjänst för identifiering inom den offentliga förvaltningen, som under övergångsperioden kommer att ersätta tunnistus.fi-tjänsten och senare Vetuma-tjänsten. Den nya styrningstjänsten för identifiering sammanförs med den nationella roll- och fullmaktstjänst som ska utvecklas under åren 2015–2017.

2.2 Elektronisk underskrift

I Finland tillhandahålls elektroniska underskrifter av flera aktörer. I praktiken är elektroniska underskrifter som görs med hjälp av identifieringsverktyg de vanligaste. Det typiska sättet att underteckna på elektronisk väg är att underskriften grundar sig på stark autentisering av undertecknaren (t.ex. bankkoder). Kunden godkänner ett dokument till exempel med sina bankkoder och därefter verifieras det undertecknade dokumentets integritet. Leverantörer av elektroniska underskrifter är i Finland till exempel Signicat och Suomen Onlineallekirjoitus Oy (Onnistuu.fi).

Kvalificerade certifikat för elektroniska underskrifter som definieras i autentiseringslagen tillhandahålls i dagens läge i Finland endast av Befolkningsregistercentralen. Kvalificerat certifikat för elektronisk underskrift från Befolkningsregistercentralen ingår i det identitetskort som beviljas medborgare och certifikatkort som centralen beviljar organisationer.

3 Lagstiftning och praxis

3.1 Elektronisk identifiering

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 autentisering som ska tillhandahållas allmänheten. Lagen och de bestämmelser som utfärdats med stöd av den ställer krav på att leverantören är tillförlitlig samt på tjänstens teknik, tillförlitlighet och informationssäkerhet. Den som tillhandahåller stark autentisering ska anmäla saken. Tjänsteleverantören ska anmäla sig till Kommunikationsverket. Anmälan ska innehålla uppgifter om hur aktören uppfyller villkoren i lagen. Kommunikationsverket för register över de aktörer som anmält sig. Om en aktör inte uppfyller lagens villkor kan Kommunikationsverket förbjuda aktören att tillhandahålla tjänster för stark autentisering.

Vid ingången av 2015 utökades autentiseringslagen med bestämmelser om ett nätverk för leverantörer av identifieringstjänster (12 a §) samt en föreskrift om att man med hjälp av ett befintligt verktyg för stark autentisering ska kunna ansöka om ett elektroniskt identifieringsverktyg på motsvarande nivå (sammankopplad inledande identifiering 17 § 4 mom.). Dessutom föreskrevs det att en leverantör av identifieringstjänster och elektroniska signaturer alltid ska kräva personbeteckning för identifiering av en person och kontrollera uppgifterna i befolkningsdatasystemet. Bestämmelserna om förtroendenätet tillämpas från och med den 1 maj 2017. För närvarande bereds föreskrifter som gäller förtroendenätets praktiska verksamhet och regler för nätverkets praxis och verksamhetsstruktur.

De identifieringstjänster som Befolkningsregistercentralen producerar regleras förutom i autentiseringslagen i lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009).

Ansvaret för lagstiftningen om stark 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.

Utöver autentiseringslagen inverkar även övriga lagar på stark autentisering och elektroniska underskrifter. 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).

3.2 Tillgången på elektroniska identifieringsverktyg

De privata aktörernas roll i fråga om att bevilja officiell elektronisk identitet grundar sig på att karaktären av de affärsekonomiska tjänster som avses i lagförslaget till den grad har ansetts (GrUU 16/2009) distanserat sig från karakteristika som gäller för offentliga myndighetsuppdrag, att verksamheten inte längre kan betraktas som en offentlig förvaltningsuppgift trots att verktygen för stark elektronisk autentisering och certifiering har betydelse i olika typer av rättshandlingar. Även i till exempel Sverige har man kommit fram till en liknande lösning. Genom elektronisk identifiering som kraftigt byggs upp utgående från marknadsbaserade aktörer strävar man också efter en teknologineutral utveckling av identifieringstjänsterna.

Vid ansökan om ett identifieringsverktyg för stark autentisering verifieras användarens identitet, och utgående från det kan den sökande beviljas ett verktyg. Till det fogas minst sådana

identifikationsuppgifter att användarens identitet kan verifieras på elektronisk väg. För att en leverantör av identifieringsverktyg för stark autentisering ska kunna bevilja ett identifieringsverktyg måste sökanden ha en finländsk personbeteckning i befolkningsdatasystemet och ett pass eller ett identitetskort som beviljats av en myndighet i en medlemsstat inom Europeiska ekonomiska samarbetsområdet, Schweiz eller San Marino. Leverantören av identifieringstjänster har kunnat, om denne så önskat, bevilja identifieringsverktyg också genom att identifiera den sökande på basis av ett giltigt körkort som efter den 1 oktober 1990 beviljats av en myndighet i en medlemsstat i Europeiska ekonomiska samarbetsområdet eller av ett giltigt pass som beviljats av en myndighet i en 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. Inledande identifiering som utförs av polisen är en avgiftsbelagd tjänst för den som ansöker om identifieringsverktyg.

Enligt bestämmelser som trädde i kraft vid ingången av 2016 kan leverantören av identifieringsverktyg även bevilja verktyg på basis ett tidigare verktyg för stark autentisering som personen redan har. Tidigare har detta varit möjligt endast genom ett avtal mellan två aktörer. I fortsättningen får identifieringsverktyg sammankopplas fritt.

Grunden för beviljandet av identifieringsverktyg är alltså att personuppgifterna finns i befolkningsdatasystemet. Avsikten med det är att säkerställa att specificerade uppgifter om en person fogas till verktyget. En uppgift som identifierar en person kan vara personbeteckningen i befolkningsdatasystemet eller en elektronisk kommunikationskod med uppgifter som upprätthålls av en myndighet. I 7 § i lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster anges de föremål för registrering som ska registreras i befolkningsdatasystemet och i 9 § om förutsättningarna för registrering av utländska medborgare. Utländska medborgare kan ges personbeteckning och personuppgifterna kan registreras i befolkningsdatasystemet trots att personen inte har ett pass eller något annat dokument som bevisar identiteten på ett tillförlitligt sätt.

Boende i Finland använder oftast de identifieringsverktyg som tillhandahålls av bankerna som verktyg för stark autentisering. Även de så kallade mobilcertifikaten som mobilföretagen tillhandahåller har blivit vanligare på sista tiden, men mobilcertifikaten och medborgarcertifikat som anknyts till de identitetskort som Befolkningsregistercentralen ger ut har inte uppnått en betydande ställning på marknaden för elektronisk identifiering som erbjuds allmänheten. Med tanke på jämlikheten är det viktigt att identifieringsverktygen finns allmänt tillgängliga när privata och offentliga tjänster blir allt mer elektroniska. De ovan nämnda elektroniska identifieringsverktygen är avgiftsbelagda för användaren och hör ofta, men inte nödvändigtvis, ihop med andra tjänster (banktjänster eller mobilanslutning). Till exempel tillhandahåller åtminstone en bank och vissa mobilföretag avgiftsbelagda identifieringsverktyg också till personer som inte har någon annan kundrelation till banken eller mobilföretaget.

3.3 Elektronisk underskrift

Autentiseringslagen innehåller också bestämmelser om elektronisk underskrift. Bestämmelserna grundar sig på Europaparlamentets och rådets direktiv 1999/93/EG om ett gemenskapsramverk för elektroniska signaturer. eIDAS-förordningen upphäver det aktuella direktivet den 1 juli 2016, och då ersätts direktivet av föreskrifterna om elektroniska underskrifter i eIDAS-förordningen som ska tillämpas direkt.

Den gällande lagen reglerar elektroniska signaturers rättsliga verkan (5 §). Lagen om elektronisk kommunikation i myndigheternas verksamhet samt flera andra lagar har i fråga om elektroniska underskrifters rättsliga verkan en hänvisning till 5 § i autentiseringslagen.

Autentiseringslagen har föreskrifter om avancerad elektronisk signatur samt avancerad elektronisk signatur som baserar sig på ett kvalificerat certifikat och som grundar sig på direktivet. Leverantörer av kvalificerat certifikat för elektroniska signaturer ska anmäla sin verksamhet till Kommunikationsverket som för ett offentligt register över dem som beviljar kvalificerat certifikat. Kommunikationsverket ska förbjuda en aktör att tillhandahålla sina certifikat som kvalificerade certifikat om certifikatutfärdaren eller om de certifikat som utfärdaren tillhandahåller inte uppfyller villkoren i lagen. Lagen har utgående från direktivet föreskrifter om kvalificerade certifikats säkerhet, tillförlitlighet, utgivning, återkallande samt skadeståndsansvar för certifikatutfärdare som tillhandahåller kvalificerade certifikat. Dessutom innehåller lagen nationella ansvarsregler i fall av obehörig användning av signaturframställningsdata och certifikatutfärdarens ansvar för skada.

3.4 Lag om elektronisk kommunikation i myndigheternas verksamhet

Finland har ingen gällande lagstiftning om andra betrodda tjänster som regleras i eIDAS-förordningen än om elektronisk underskrift. eIDAS-förordningen innehåller också föreskrifter om till exempel certifikat för elektroniska stämplar, elektroniska tidsstämplar, elektroniska tjänster för leverans och certifikat för autentisering av webbplatser som ska tillämpas direkt. I 3, 9, 16 och 18 § i lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003) hänvisas det till autentiseringslagen. Betydande delar av den lagen behöver upphävas för att eIDAS-förordningen träder i kraft.

Enligt de nuvarande 9 och 16 § kan både en kund hos myndigheten och myndigheten använda åtminstone en sådan avancerad elektronisk signatur som baserar sig på ett kvalificerat certifikat och har skapats med en säker anordning för signaturframställning. Elektroniska signaturer ska dock inte förvägras rättslig verkan enbart på den grunden att de har skapats på något annat sätt än vad som anges ovan.

När en handling som ska delges bevisligen avhämtas ska parten eller dennes företrädare enligt 18 § i lagen om elektronisk kommunikation i myndigheternas verksamhet identifiera sig. Vid identifieringen används ett identifieringsverktyg eller ett kvalificerat certifikat som avses i autentiseringslagen eller någon annan motsvarande identifieringsteknik som är datatekniskt tillförlitlig och bevislig.

I lagen om elektronisk kommunikation i myndigheternas verksamhet finns det inga ovillkorliga krav på ett bestämt slag av elektronisk underskrift. Enligt situationen kan också ett annat slag av elektronisk underskrift duga. Vid avhämtningen av en handling som ska delges bevisligen har det inte heller ställts något ovillkorligt krav på ett bestämt slag av identifieringsteknik.

I tillämpningspraxis har huvudregeln varit den att en elektronisk handling som anländer till en myndighet inte behöver kompletteras med underskrift. Även de högsta laglighetsövervakarna har fäst uppmärksamhet vid att handlingar inte enligt lagen måste kompletteras med underskrifter (till exempel justitieombudsmannens avgörande 26.6.2008 (3355/4/06) och biträdande justitieombudsmannens avgörande 30.10.2011 (AOA 3666/4/10) 3666/4/10).

I 16 § i lagen om elektronisk kommunikation i myndigheternas verksamhet lämnas bestämmelsen rätt öppen i fråga om hurdana elektroniska signaturer myndigheten får använda. I en utredning som finansministeriet beställt (Sähköisen asioinnin lainsäädännön seuranta- ja kehittämistutkimus "Undersökning om uppföljning och utveckling av lagstiftningen om elektronisk kommunikation", på finska, Finansministeriets publikationer 30/2013) bedöms det att bestämmelserna i 16 § i praktiken inte har någon betydelse med tanke på användningen av signatur i myndigheternas handlingar och beslut.

4 EU-lagstiftningen

Syftet med eIDAS-förordningen är att öka förtroendet för elektroniska transaktioner på den inre marknaden genom att tillhandahålla en gemensam grund för ett säkert elektroniskt samspel mellan medborgare, företag och offentliga myndigheter. Därigenom ökar effektiviteten hos offentliga och privata nättjänster, elektronisk affärsverksamhet och e-handel i unionen. Målet är att uppnå en tillräckligt hög tillitsnivå på elektronisk identifiering och betrodda tjänster.

Förordningen tillämpas på de system för elektronisk identifiering som medlemsstaterna har anmält och på de leverantörer av betrodda tjänster som är etablerade i unionen. Förordningen föreskriver under vilka förutsättningar medlemsstaterna måste godkänna de system för elektronisk identifiering som en annan medlemsstat har anmält och de verktyg för elektronisk identifiering som ingår där. Förordningen har föreskrifter om betrodda tjänster och skyldigheter för leverantörerna av dem som ska tillämpas direkt. Förordningen reglerar följande betrodda tjänster och deras rättsliga verkan: elektroniska underskrifter, elektroniska stämplar, tjänster för validering och bevarande av elektroniska underskrifter och stämplar, elektronisk tidsstämpling, elektroniska tjänster för rekommenderade leveranser, certifikattjänster för autentisering av webbplatser och elektroniska dokument. Förordningen tillämpas inte på tillhandahållandet av sådana betrodda tjänster som beroende på nationell rätt eller på avtal inom en bestämd deltagargrupp används i slutna system.

4.1 Elektronisk identifiering

Enligt artikel 6 i eIDAS-förordningen ska, när det krävs elektroniska identifieringsverktyg, för att få åtkomst till en nättjänst som tillhandahålls av ett offentligt organ i en medlemsstat, de elektroniska identifieringsverktyg som utfärdats i en annan medlemsstat erkännas för gränsöverskridande autentisering för den tjänsten via internet. Detta förutsätter dock att identifieringsverktyget är utfärdat inom ramen för ett system för elektronisk identifiering som medlemsstaten har anmält till Europeiska kommissionen och att det aktuella systemet ingår i den förteckning över gränsöverskridande system för identifiering som kommissionen upprätthåller. Dessutom ska det utländska identifieringsverktyget ha en tillitsnivå som är lika hög eller högre och det offentliga organet använda tillitsnivån väsentlig eller hög i samband med åtkomst till nättjänsten.

Systemet för elektronisk identifiering anmäls till kommissionen som gränsöverskridande system på det sätt som anges i artiklarna 7–9 i eIDAS-förordningen. Förordningen föreskriver hurdana system för elektronisk identifiering medlemsstaterna får anmäla till kommissionen, hur anmälan ska ske och vilka krav som ställs på systemen för identifiering och identifieringsverktygen. I förordningen och de genomförandeakter som utfärdats med stöd av den har tre tillitsnivåer för identifieringstjänster fastställts: låg, väsentlig och hög.

Artikel 10 innehåller föreskrifter om hur medlemsstaterna ska agera i samband med säkerhetsincidenter. Artikel 11 innehåller bestämmelser om ansvaret hos den medlemsstat som anmäler ett system för elektronisk identifiering och skadeståndsansvaret hos den part som utfärdat ett elektroniskt identifieringsverktyg om de inte uppfyller skyldigheterna i förordningen.

4.2 Betrodda tjänster

eIDAS-förordningen reglerar tillhandahållandet av betrodda tjänster. Enligt förordningen är bland annat följande betrodda tjänster: elektroniska underskrifter, elektroniska stämplar, validering och bevarande av elektroniska underskrifter och stämplar, elektroniska tidsstämplingar,

elektroniska tjänster för rekommenderade leveranser och certifikat för autentisering av webbplatser. Föreskrifterna i eIDAS-förordningen tillämpas på alla leverantörer av ovan nämnda betrodda tjänster. Förordningen tillämpas dock inte när betrodda tjänster används i slutna system inom en bestämd deltagargrupp, till exempel i företag eller i system inom offentlig förvaltning som inrättats för administration av interna förfaringssätt. Endast betrodda tjänster som tillhandahålls allmänheten och som inverkar på tredje parter måste uppfylla kraven i förordningen. Förordningen tillämpas endast på tjänster som i allmänhet tillhandahålls mot ersättning, det vill säga i ekonomiskt syfte.

Betrodda tjänster såsom elektroniska underskrifters rättsliga verkan regleras i eIDAS-förordningen, men nationella kompletterande föreskrifter tillåts också. Enligt artikel 25 i förordningen får en elektronisk underskrift inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att underskriften har elektronisk form eller inte uppfyller kraven för kvalificerade elektroniska underskrifter. Vidare ska enligt artikel 25 en kvalificerad elektronisk underskrift ha motsvarande rättsliga verkan som en handskriven underskrift.

För att öka användningen av betrodda tjänster och produkter i anslutning till dem tas begreppen kvalificerad betrodd tjänst och kvalificerad tillhandahållare av betrodda tjänster i bruk i eIDAS-förordningen. Enligt den ska medlemsstaterna utse en tillsynsmyndighet som har tillsynen över att föreskrifterna om betrodda tjänster enligt förordningen iakttas. Kommunikationsverket föreslås bli tillsynsmyndighet enligt förordningen. I förordningen görs emellertid en anmärkningsvärd skillnad på kvalificerade och icke kvalificerade tillhandahållare av betrodda tjänster. Icke-godkända betrodda tjänster är i och för sig samtliga samma sorts tjänster för vilka man kan skaffa statusen betrodd tjänst, men för dem gäller endast i enlighet med artikel 19 i eIDAS-förordningen de allmänna villkoren om underhåll av informationssäkerheten och kontroll över störningssituationer samt skyldighet att underrätta myndigheterna om alla säkerhetsincidenter eller integritetsförluster som medför betydande påverkan. Enligt artikel 17.3 ska Kommunikationsverket som tillsynsmyndighet vidta tillsynsåtgärder endast om Kommunikationsverket får anmälan om att en icke-kvalificerad betrodd tjänst inte uppfyller kraven i förordningen.

En leverantör får statusen kvalificerad tillhandahållare av betrodda tjänster genom att i enlighet med eIDAS-förordningen underställa sin verksamhet bedömning av organet för bedömning av överensstämmelse. Med organet för bedömning av överensstämmelse avses det organ som definieras i Europaparlamentets och rådets förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93, den s.k. NLF-förordningen. Efter bedömningen ska aktören anmäla sin avsikt och lämna in en rapport om överensstämmelsebedömning som utfärdats av ett organ för bedömning av överensstämmelse till Kommunikationsverket. Om Kommunikationsverket kommer fram till att tillhandahållaren av betrodda tjänster och de betrodda tjänster som denne tillhandahåller uppfyller de krav som avses i förordningen, ska det bevilja status som kvalificerad tillhandahållare av betrodda tjänster och registrera tjänsten i förteckningen över betrodda tjänster (Trusted list) och den kvalificerade tillhandahållaren får använda EU:s förtroendemärkning.

5 Målsättning och de viktigaste förslagen

5.1 Målsättning

Syftet med propositionen är att sätta i kraft de ändringar i lagstiftningen som är nödvändiga på grund av eIDAS-förordningen. Målet med förslaget är att göra det möjligt för Finland att delta i det interoperabila system för elektronisk identifiering som regleras i eIDAS-förordningen.

Propositionen har också som syfte att främja regeringens spetsprojekt att skapa en tillväxtmiljö för digital affärsverksamhet. Byggandet av en tillväxtmiljö för digital affärsverksamhet koncentreras på att främja digitalisering av näringslivet. Målet med spetsprojektet är att Finland ska ha gynnsamma verksamhetsförhållanden för digitala tjänster och modeller för digitalbaserad affärsverksamhet. Avsikten är att allmänhetens och näringslivets förtroende för internet och elektroniska tjänster bibehålls och att man i framtiden i all affärsverksamhet drar nytta av de digitala möjligheterna.

Syftet med den föreslagna lagstiftningen är att i Finland genomföra de praktiska åtgärder som gör det möjligt att använda de elektroniska identifieringsverktyg som används i Finland i offentliga och privata tjänster i de andra EU-staterna i framtiden. På motsvarande sätt kan man genom den föreslagna lagstiftningen genomföra de praktiska åtgärder som behövs för att den finländska offentliga förvaltningen ska ha beredskap att ta emot och godkänna bruket av identifieringsverktyg som används i de andra medlemsstaterna i service inom den finländska offentliga förvaltningen och även inom privata sektorns elektroniska tjänster om tjänsteleverantörerna så önskar. De ovan avsedda gränsöverskridande identifieringsverktygens tillförlitlighet och egenskaper i fråga om informationssäkerhet regleras i EU:s lagstiftning.

Avsikten med propositionen är att kräva minst samma villkor för tillförlitlighet och informationssäkerhet av de system för stark autentisering som används i Finland som eIDAS-förordningen och genomförandeakterna kräver av de gränsöverskridande systemen för elektronisk identifiering med tillitsnivån väsentlig. Det underlättar för aktörerna inom stark autentisering i Finland att söka så kallad status som gränsöverskridande identifieringsverktyg för sina verktyg. Å andra sidan har den offentliga förvaltningen i Finland underlag för jämförelse mellan identifieringsverktyg som används i Finland och verktyg som används i de andra medlemsstaterna i EU när samma tillitsnivåer följs i Finland som i eIDAS-förordningen, och den finländska offentliga förvaltningen kan kräva samma tillitsnivå på de andra staternas identifieringsverktyg som i för dem som används i Finland.

Avsikten med justeringarna av lagen är att klargöra skyldigheterna för två olika slag av tjänsteleverantörer som agerar i förtroendenätet för elektronisk identifiering, det vill säga skyldigheterna för leverantörer av identifieringsverktyg och för leverantörer av tjänster för identifieringsförmedling.

eIDAS-förordningen innehåller föreskrifter om elektronisk underskrift och andra betrodda tjänster som definieras i förordningen som ska tillämpas direkt. Förordningen har föreskrifter om elektroniska underskrifters rättsliga verkan som ska tillämpas direkt. Det kräver ändringar i lagen om elektronisk kommunikation i myndigheternas verksamhet samt i flera andra lagar. Ändringarna ändrar dock inte det rådande rättsläget för elektroniska underskrifters rättsliga verkan.

5.2 De viktigaste förslagen

Elektronisk identifiering

I propositionen föreslås det att minst samma villkor för tillförlitlighet och informationssäkerhet ska krävas av de system för stark autentisering som används i Finland som eIDAS-förordningen med genomförandeakter kräver av de gränsöverskridande systemen för elektronisk identifiering med tillitsnivån väsentlig. Därför ska det i de gällande bestämmelserna göras preciseringar och hänvisningar till kommissionens genomförandeförordning som utfärdats med stöd av eIDAS-förordningen. I praktiken bedöms de system för stark autentisering som används i Finland vad gäller tekniska krav och krav på informationssäkerhet redan från förut huvudsakligen uppfylla kraven på tillitsnivån väsentlig enligt eIDAS-förordningen.

Som ett nytt krav på leverantörer av de identifieringstjänster som används i Finland föreskrivs i denna proposition bestämmelser som motsvarar bestämmelserna om skyldigheten i fråga om bedömning av identifieringstjänster, det vill säga kvalitetsrevision, i eIDAS-förordningen. Avsikten med revisionen är att bedöma hur väl identifieringstjänsten och företagets verksamhet motsvarar de krav som ställs. Propositionens bestämmelser om överensstämmelsebedömning av tjänsterna finns i 4 kap. I propositionen föreslås det (28 §) att de kvalitetsrevisioner som krävs kan utföras av 1) ett organ för bedömning av överensstämmelse 2) ett annat organ för bedömning enligt en allmänt använd standard (annat utomstående bedömningsorgan) samt 3) intern oberoende bedömning hos tjänsteleverantören (internt kontrollorgan). eIDAS-förordningen föreskriver om det först nämnda organet för bedömning av överensstämmelse. I propositionen föreslås det att Kommunikationsverket i Finland godkänner organet för bedömning av överensstämmelse efter att Säkerhets- och kemikalieverkets ackrediteringsenhet har ackrediterat den aktuella aktören och Kommunikationsverket har bedömt att aktören uppfyller de krav som ställs (32 §).

Trots att kraven på kvalitetsrevision av elektroniska identifieringstjänster kommer från genomförandeakter som utfärdats med stöd av eIDAS-förordningen och de endast gäller identifieringsverktyg som används över gränserna, finns det också ett nationellt behov av de föreslagna kvalitetsrevisionerna hos aktörerna beroende på föreskriften om förtroendenät för elektronisk identifiering i 12 a § i den gällande lagen. För att aktörerna ska kunna förlita sig på identifieringsuppgifterna de förmedlar sinsemellan i förtroendenätet är måste det krävas minst intern oberoende kvalitetsrevision av dem. Införandet av skyldigheten att utföra kvalitetsrevision för leverantörer av identifieringstjänster i Finland stöds också av att detta är ett etablerat underhållsförfarande för informationssäkerheten och aktörerna redan sedan tidigare utnyttjar olika former av kvalitetsrevision. Enligt den övergångsbestämmelse som föreslås bör en leverantör av stark autentiseringstjänst lämna en bedömningsrapport över verkställd oberoende bedömning av identifieringstjänsten i enlighet med den föreslagna lagen och uppgifter om de ändrade principerna för identifiering som avses i 14 § till Kommunikationsverket senast den 31 januari 2017.

Kommunikationsverket föreslås även få normgivningsbemyndigande i fråga om grunderna för bedömning av stark autentisering (dvs. grunderna för kvalitetsrevision). Kommunikationsverket föreslås, ytterligare i samband med förtroendenätet för elektronisk identifiering, få normgivningsbemyndigande avseende egenskaperna i det tekniska förtroendenätets gränssnitt.

De två slagen av aktörer inom elektronisk identifiering som arbetar i förtroendenätet definieras i lagen och de skyldigheter de redan har enligt lagen preciseras. Det föreslås att definitionerna i 2 § i lagen ändras så att begreppet leverantör av identifieringstjänster i den gällande lagen fortfarande ska gälla som överbegrepp. Under det definieras leverantör av identifieringsverktyg som tillhandahåller identifieringsverktyg för användare samt leverantör av tjänster för identifieringsförmedling som i förtroendenätet förmedlar identifieringstransaktioner baserade på stark autentisering till en part som förlitar sig på elektronisk identifiering.

Begreppet stark autentisering ändras enligt förslaget så att även juridiska personer kan beviljas identifieringsverktyg. I den gällande lagen föreskrivs att till ett verktyg vid behov kan fogas en uppgift om att en person i enskilda fall kan företräda en juridisk person. Den möjligheten har tills vidare inte använts åtminstone i omfattande utsträckning, men avsikten är att den bibehålls i lagen även om det blir möjligt att bevilja en juridisk person ett självständigt elektroniskt identifieringsverktyg. Det kan i framtiden finnas behov av att bevilja juridiska personer identifieringsverktyg vilket är möjligt även enligt eIDAS-förordningen. Sålunda föreslås det att identifieringsverktyg för stark autentisering även kan beviljas juridiska personer. Vad gäller identifiering av juridiska personer föreslås det nya paragrafer: 7 a § om användning av uppgif-

ter i patent- och registerstyrelsens register samt 17 a § om identifiering när en juridisk person ansöker om identifieringsverktyg.

I propositionen föreslås det att Kommunikationsverket ges nya uppgifter i anslutning till systemet för interoperabilitet i elektronisk identifiering mellan medlemsstaterna enligt eIDAS-förordningen. Befolkningsregistercentralen får i uppgift att i Finland bygga och upprätthålla en nationell så kallad nod som bildar ett gränssnitt för de andra EU-staternas identifieringsverktyg när de används i finländska elektroniska tjänster för ärendehantering.

Enligt förslaget får identifieringsverktyg från början av 2019 inte längre beviljas endast på basis av körkort som beviljats i Finland eller i det övriga EES-området. Ändringen av praxis kan motiveras med att det finns riskfaktorer i samband med körkort som identifieringshandling. Inrikesministeriet har gjort en riskanalys beträffande körkort. (Inrikesministeriets publikation 32/2010, på finska). http://www.intermin.fi/ download/16144_Identiteettiohjelman_ loppuraportti.pdf

För närvarande har cirka 3,5 miljoner finländare pass och cirka 600 000 finländska identitetskort har beviljats. Det finns cirka 3,7 miljoner finländska körkort. När en persons identitet inte längre kan säkerställas endast med stöd av körkort inverkar detta på situationen för personer som har körkort men inte pass, identitetskort eller något tidigare identifieringsverktyg.

I 17 § i propositionen föreslås att bestämmelserna om inledande identifiering så att de är i samklang med de bestämmelser som utfärdats med stöd av eIDAS-förordningen. Detta medför också nya förfaranden i fråga om inledande identifiering av en person.

Elektroniska underskrifter och övriga betrodda tjänster

eIDAS-förordningen innehåller bestämmelser om elektroniska underskrifter och andra betrodda tjänster som definieras i förordningen, såsom elektroniska stämplar och certifikattjänster för autentisering av webbplatser. Därför kommer de centrala ändringarna i lagstiftningen som gäller dessa aktörers verksamhet från bestämmelser i eIDAS-förordningen som ska tillämpas direkt. I propositionen föreslås det att Kommunikationsverket ser till att leverantörerna av betrodda tjänster i Finland iakttar föreskrifterna i eIDAS-förordningen.

Trots att eIDAS-förordningen nu i praktiken täcker lagstiftningen om kraven på betrodda tjänster förutsätter den kompletterande föreskrifter om bedömningen av leverantörerna av betrodda tjänster, det vill säga kvalitetsrevision. Bestämmelserna som föreslås finns i 4 kap. i lagförslaget.

eIDAS-förordningen förutsätter att bestämmelserna om elektroniska signaturer och kvalificerat certifikat för elektroniska signaturer i den gällande lagen upphävs. Det föreslås dock att föreskrifterna om tjänsteleverantörens och användarens rättigheter och skyldighet i fall där användaren förlorar en anordning för signaturframställning av elektroniska signaturer eller stämplar bibehålls i lagen (de föreslagna § 39 och 40). eIDAS-förordningen har inga motsvarande föreskrifter.

Förordningen har föreskrifter om rättslig verkan av elektroniska underskrifter, elektroniska stämplar, elektronisk tidsstämpling och elektroniska dokument som ska tillämpas direkt. Bestämmelserna om elektroniska underskrifters rättsliga verkan (artikel 25) som ska tillämpas direkt förutsätter ändringar i lagen om elektronisk kommunikation i myndigheternas verksamhet samt i flera andra lagar som det i nuläget hänvisas till i 5 § i autentiseringslagen. Det föreslås att 5 § i autentiseringslagen upphävs eftersom motsvarande bestämmelser finns i artikel 25 i

eIDAS-förordningen. Ändringarna ändrar dock inte det rådande rättsläget avseende elektroniska underskrifters rättsliga verkan. Också 4 § i autentiseringslagen föreslås bli upphävd.

Lag om elektronisk kommunikation i myndigheternas verksamhet

Enligt förslaget ändras bestämmelserna om elektronisk signatur och identifieringsteknik i 9, 16 och 18 § i lagen om elektronisk kommunikation i myndigheternas verksamhet. Avsikten med ändringarna är inte att ändra rättsläget så att strängare krav än i nuläget skulle ställas på underskrifter eller identifieringsteknik. Användningen av de nuvarande systemen för elektronisk ärendehantering eller utvecklingen av kommande system ska alltså inte försvåras.

Vad gäller handlingar som ska lämnas till myndigheter ska enligt förslaget huvudregeln fortfarande vara den att en elektronisk handling inte behöver kompletteras med underskrift. En underskrift kan krävas om en handling saknar uppgift om avsändare eller om det finns skäl för att ifrågasätta en handlings autenticitet eller integritet. Då föreslås det inga särskilda krav på den elektroniska underskriftens kvalitet.

Det föreslås att 16 § i lagen om elektronisk kommunikation i myndigheternas verksamhet får en föreskrift om att myndigheten vid elektronisk signering av ett beslut antingen använder kvalificerad elektronisk underskrift som avses i artikel 26 i eIDAS-förordningen eller något annat sätt som gör det möjligt att säkerställa handlingens autenticitet och integritet. Ett visst krav på materiell kvalitet på underskriften ställs alltså i lagen. Underskriften binds dock inte ovillkorligen till någon typ av underskrift enligt eIDAS-förordningen.

Det föreslås att hänvisningen till autentiseringslagen i fråga om identifieringsverktyg och kvalificerat certifikat i 18 § i lagen om elektronisk kommunikation i myndigheternas verksamhet stryks. Enligt bestämmelsen ställs fortfarande krav på informationssäkerhet och bevislig delgivning i den identifieringsteknik som används när handlingen avhämtas.

Övriga ändringar i lagstiftningen

Ändringen av namnet på autentiseringslagen och upphävandet av 5 § i lagen som föreslås i denna proposition föranleder ändringar också i lagstiftningen på övriga förvaltningsområden som har föreskrifter om elektroniska signaturer och som hänvisar till autentiseringslagen. De föreslagna ändringarna har beretts så att de inte orsakar ändringar i det rådande rättsläget.

6 Propositionens konsekvenser

6.1 Ekonomiska konsekvenser

De ändringar i den nationella lagstiftningen som föreslås om stark autentisering bedöms inte orsaka betydande ökade kostnader för leverantörerna av identifieringstjänster. Cirka 70 företag har anmält sig till Kommunikationsverket som leverantörer av identifieringstjänster. Merparten av dem är banker, övriga aktörer är mobilföretag samt Befolkningsregistercentralen. Vad gäller det nationella förtroendenätet för elektronisk identifiering är aktörerna skyldiga att med stöd av 10 § i den gällande lagen anmäla ändringar som gäller verksamheten till Kommunikationsverket. I propositionen föreslås det att leverantörer av identifieringstjänster också är skyldiga att låta utföra en bedömning av överensstämmelse i sin verksamhet enligt det föreslagna 4 kap. Enligt propositionen kan leverantörer av identifieringstjänster som agerar endast på tillitsnivån väsentlig i enlighet med EU-lagstiftningen låta göra bedömningen av överensstämmelse också genom ett oberoende internt bedömningsorgan (intern kontroll). På basis av en preliminär enkät uppskattas det att de nuvarande leverantörerna av identifieringstjänster redan nu regelbundet låter göra bedömningar av informationssäkerheten i sina identifierings-

tjänster. Dessutom ger också bedömningarna av överensstämmelse som krävs i EU-lagstiftningen och i den inhemska lagstiftningen företag som utövar verksamheten möjligheter till affärsverksamhet i Finland och utomlands.

I fråga om gränsöverskridande elektronisk identifiering enligt eIDAS-förordningen kan leverantörerna av identifieringstjänster i Finland, liksom även andra tjänsteleverantörer på EU-området, sträva efter att bli ett anmält system för identifieringstjänst och på så sätt göra det möjligt för sina egna kunder att använda identifieringsverktyget också på annat håll på EU-området i framtiden.

Enligt de föreslagna föreskrifterna kan endast juridiska personer vara leverantörer av identifieringstjänster. Det är också fallet med de nuvarande leverantörerna av identifieringstjänster. Det föreslås att den årliga tillsynsavgiften som Kommunikationsverket tar ut av leverantörer av identifieringstjänster höjs från 12 000 euro till 14 000 euro. Enligt förslaget ska de avgifter som Kommunikationsverket tar ut av leverantörer av nya betrodda tjänster som verket godkänner vara lika stora som avgifterna för leverantörer av identifieringstjänster. I det här skedet är det svårt att uppskatta hur många leverantörer av betrodda tjänster (till exempel leverantörer av elektroniska underskrifter och elektroniska stämplar) som strävar efter status som kvalificerad tillhandahållare av betrodda tjänster. Man uppskattar emellertid att Kommunikationsverkets intäkter med de föreslagna avgifterna och det nuvarande antalet aktörer hålls på nuvarande nivå.

Propositionens ekonomiska konsekvenser gäller huvudsakligen Kommunikationsverket och Befolkningsregistercentralen.

6.2 Konsekvenser för myndigheterna

I lagen föreslås Kommunikationsverket och Befolkningsregistercentralen få nya uppgifter.

Kommunikationsverket får nya uppgifter med anledning av EU:s system för interoperabilitet i elektronisk identifiering och det anknytande samarbetsnätverket. Kommunikationsverket är en del av det samarbetsnätverk som inrättats i kommissionens genomförandeförordning (EU) 2015/296. Nätverket bedömer de system för elektronisk identifiering som anmälts till Europeiska kommissionen i samarbete med de andra medlemsstaternas myndigheter. Kommunikationsverket har även som uppgift att anmäla finländska system för elektronisk identifiering till Europeiska kommissionen. Kommunikationsverket får som uppgift att som tillsynsmyndighet enligt eIDAS-förordningen utöva tillsyn över de betrodda tjänster som regleras i den. Dessutom föreslås Kommunikationsverket få en särskild uppgift som gäller informationsutbyte i det nationella förtroendenätet för elektronisk identifiering.

Kommunikationsverket har uppskattat att de nya uppgifterna på grund av ändringarna i autentiseringslagen och EU:s förordning minst kommer att fördubbla verkets uppgifter jämfört med nuläget. Enligt Kommunikationsverkets bedömning ökar uppgifterna som föreslås för verket i regeringens proposition dess uppgifter med 1–2 årsverken. I nuläget har Kommunikationsverket anvisat ett årsverke för tillsynen enligt autentiseringslagen och kostnaderna för den nuvarande tillsynsverksamheten har gått att finansiera med de lagstadgade avgifter som tagits ut av tjänsteleverantörerna. De framtida avgifterna beror på antalet leverantörer av identifieringstjänster och kvalificerade betrodda tjänster. Det uppskattas att Kommunikationsverket fortfarande kan finansiera kostnaderna för skötseln av de nya uppgifterna med de avgifter som tas ut. Vid behov kan ämbetsverket också omfördela sina resurser.

Befolkningsregistercentralen föreslås få i uppgift att skapa och upprätthålla en nationell nod som hör ihop med det gränsöverskridande bruket av elektroniska identifieringsverktyg. Be-

folkningsregistercentralens uppgift i anslutning till den nationella noden regleras i den föreslagna 42 c §. Avsikten är att den nationella noden skapas som en del av ett projekt för identifieringstjänst i programmet Nationell servicearkitektur. Det bedöms kosta cirka 200 000 euro att skapa noden och Befolkningsregistercentralen har uppskattat att produktion och vidareutveckling av den kräver ett årsverke. Noden gör det möjligt för organisationerna inom den offentliga förvaltningen att i sina tjänster för elektronisk ärendehantering beakta användare av identifieringsverktyg från andra medlemsstater. Befolkningsregistercentralen föreslås få som uppgift att upprätta ett register där elektroniska identitetsuppgifter från en enskild annan EU-medlemsstat har omvandlats till nationell form. Kostnaderna för den nationella noden finansieras med medel inom ramen för tillgängliga anslag för Befolkningsregistercentralen.

6.3 Konsekvenser för medborgarna

I propositionen föreslås att det av säkerhetsskäl från ingången av 2019 när ett identifieringsverktyg för stark autentisering beviljas en person inte längre är tillräckligt att personens identitet säkerställs utifrån ett körkort som beviljats av en myndighet i en stat inom Europeiska ekonomiska gemenskapen, dvs. att inledande identifiering av personen inte enbart kan grunda sig på ett körkort. Ändringen görs av säkerhetsskäl, eftersom en persons identitet inte längre kontrolleras av en myndighet när ett körkort beviljas i Finland. Detsamma gäller också körkort om beviljats i andra medlemsstater inom Europeiska ekonomiska samarbetsområdet. Körkortet är inte längre en legitimationshandling, utan ett bevis på körrätt.

Största delen av identifieringsverktygen för stark autentisering beviljas av banker och vanligen beviljar bankerna identifieringsverktygen på basis av körkort. I lagstiftningen om penningtvätt tillåts att kunden identifieras med körkort, men då krävs också tilläggsuppgifter om kunden. Med stöd av den föreslagna 17 § kan t.ex. bankerna vid den inledande identifieringen av en person utnyttja uppgifter från ett tidigare kundförhållande.

I och med eIDAS-förordningen kan finländare från och med hösten 2018 använda finländska elektroniska identifieringsverktyg också i andra medlemsstaters sådana offentliga elektroniska tjänster som kräver elektronisk identifiering. Detta förutsätter dock att den leverantör av identifieringsverktyg som den finländska användaren använder sig av via Kommunikationsverket ansöker om att bli en så kallad anmäld Europeisk leverantör av identifieringsverktyg.

Propositionen bedöms inte ha några könsrelaterade konsekvenser.

6.4 Konsekvenser för informationssamhället

Syftet med eIDAS-förordningen och de föreskrifter som kompletterar den är att öka förtroendet för elektroniska transaktioner genom att tillhandahålla en gemensam grund för ett säkert elektroniskt samspel mellan medborgare, företag och offentliga myndigheter. Därigenom ökar effektiviteten hos offentliga och privata nättjänster, elektronisk affärsverksamhet och e-handel i unionen. Målet är att uppnå en tillräckligt hög tillitsnivå på elektronisk identifiering och betrodda tjänster.

Syftet med propositionen är att främja verksamheten på marknaden för inhemska identifieringstjänster och verksamheten i förtroendenätet för elektronisk identifikation genom att komplettera bestämmelserna i den gällande lagen. Propositionen innehåller de nationella bestämmelser som förutsätts i eIDAS-förordningen för att elektronisk identifiering över statsgränserna inom Europeiska ekonomiska samarbetsområdet ska kunna genomföras.

7 Beredningen av ärendet

Propositionen har beretts av kommunikationsministeriet med hjälp av Kommunikationsverket. Lagförslaget om ändring av lagen om elektronisk kommunikation i myndigheternas verksamhet har beretts av justitieministeriet. Under beredningen har Befolkningsregistercentralen hörts och diskussioner har förts med experter vid finansministeriet och inrikesministeriet.

De ändringar som planeras i lagen och som gäller leverantörer av identifieringstjänster har även diskuterats i en arbetsgrupp för förvaltningsmodell för förtroendenätet som tillsatts av finansministeriet.

7.1 Utlåtanden och hur de har beaktats

Utkastet till regeringsproposition sändes på remiss i januari–februari 2016. Kommunikationsministeriet fick 35 yttranden. De enskilda yttrandena finns i statsrådets projektregister (HARE) med ärendenummer LVM070:00/2015.

Nästan utan undantag förhöll sig remissinstanserna positiva till lagförslagen och de ansågs främja elektronisk ärendehantering, användningen av elektroniska tjänster och utvecklingen av digitala tjänster. I flera yttranden understöddes propositionens syfte att ställa minst samma krav på tillförlitlighet och informationssäkerhet i fråga om de inhemska systemen för stark autentisering som EU-lagstiftningen minst ställer på tillitsnivån väsentlig i fråga om de system för elektronisk identifiering som fungerar över EU:s gränser. I några utlåtanden förhöll man sig kritiskt till de föreslagna ändringarna, eftersom den elektroniska identifieringen befinner sig i ett övergångsskede i EU och utvecklingen av det nationella förtroendenätet för elektronisk identifiering ännu pågår. I yttrandena betonades EU:s nya reglering om betaltjänster, som också reglerar bankerna samtidigt som bankerna fungerar som leverantörer av identifieringstjänster.

Med anledning av justitieministeriets yttrande har ett avsnitt om propositionens förhållande till grundlagen och lagstiftningsordning införts i propositionen.

Tillgången på identifieringsverktyg och konsumentfrågor

Undervisnings- och kulturministeriet, Folkpensionsanstalten och Konkurrens- och konsumentverket fäste i sina yttranden uppmärksamhet vid tillgången på identifieringsverktyg i synnerhet när det gäller personer som har betalningsstörning och minderåriga. I yttrandena önskades åtgärder eller bestämmelser genom vilka konsumentens rätt att få identifieringsverktyg tryggas.

I Konkurrens- och konsumentverkets yttrande ansågs att det finns skäl att på lagnivå föreskriva om ansvar och tillräckliga påföljder i anknytning till användningen av identifieringstjänster och betrodda tjänster när det gäller situationer då uppdraget från identifieringsverktygets användare inte genomförs eller då verktyget används obehörigen, t.ex. genom användning av ett borttappat eller stulet verktyg eller vid intrång i informationssystem. Kommunikationsministeriet konstaterar att i 27 § i den gällande lagen finns bestämmelser som reglerar ansvaret för innehavaren av identifieringsverktyget i situationer där verktyget har använts obehörigt.

Slopandet av körkort som medel för första identifiering från ingången av 2019

Förslaget i enlighet med 17 § att användningen av körkort slopas bland de handlingar som kan användas för att konstatera identiteten ansågs bland de som lämnade yttrande vara av stor

praktisk betydelse, eftersom alla inte har en officiell identitetshandling (pass eller identitetskort) och dessa personer har vant sig vid att identifiera sig enbart genom att visa körkortet.

I yttrandena ansågs det att myndigheterna ska svara för informationen till medborgarna om den ändring som berör dem. Efter remissbehandlingen ändrades 17 § om inledande identifiering så att det är tillåtet att utföra den inledande identifieringen på det sätt som föreskrivs i kommissionens genomförandeförordning (EU) 2015/1502 om fastställande av tekniska minimispecifikationer och förfaranden för tillitsnivåer för medel för elektronisk identifiering i enlighet med artikel 8.3 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden (nedan förordningen om tillitsnivåer vid elektronisk identifiering). Detta möjliggör också inledande identifiering på basis av ett så kallat tidigare kundförhållande. Utifrån yttrandena ansågs det motiverat att i detaljmotiveringen till övergångsbestämmelsen i lagförslaget införa ett omnämnande om att det i fråga om sådan inledande identifiering vid beviljande av identifieringsverktyg som gjorts på basis av körkort före utgången av 2018 inte krävs att personen identifierar sig på nytt med någon annan handling efter den 1 januari 2019.

Identifieringsverktyg för juridiska personer

På grund av bland annat motsvarande EU-lagstiftning föreslås det i propositionen att det ska vara tillåtet att bevilja identifieringsverktyg också till juridiska personer. I princip förhöll man sig positivt till möjligheten att bevilja identifieringsverktyg också till juridiska personer, men enligt remissinstanserna behöver bestämmelserna preciseras. Av denna anledning har propositionen kompletterats. Det är tillsvidare svårt att förutse efterfrågan på elektroniska identifieringsverktyg för juridiska personer och behoven av anknytande förfaranderegler, varför det inte i detta skede föreslås några närmare förfaranderegler i lagen. Vid behov kan man stödja sig på annan lagstiftning i fråga om förhållandet mellan juridiska och fysiska personer.

Ansvaret för leverantörer av betrodda tjänster

Justitieministeriet konstaterade att en hänvisning till skadeståndslagen av det slag som föreslås i 41 § är problematisk i en speciallag, eftersom tillämpningen av vissa bestämmelser i skadeståndslagen med tanke på syftet med speciallagen kan leda till ett inkonsekvent resultat (t.ex. när det gäller begränsningarna av avtalsansvar och ren sakskada). På grund av detta stannade man i den fortsatta beredningen för att slopa denna hänvisning till skadeståndslagen med beaktande av artikel 13.3 i eIDAS-förordningen, enligt vilken ansvarsbestämmelserna i eIDAS-förordningen tillämpas i enlighet med nationella bestämmelser om skadeståndsansvar.

Enligt inledande sats 37 i eIDAS-förordningen påverkar förordningen inte nationella bestämmelser om t.ex. definitionen av skada, avsikt, oaktsamhet eller relevanta tillämpliga procedurregler.

Krav på system för elektronisk identifiering och autentiseringsfaktorer

Utifrån remissyttrandena har 8 och 8 a § i lagförslaget preciserats.

Utifrån remissyttrandena har autentiseringsfaktorerna i anknytning till system för elektronisk identifiering definierats teknikneutralt. I utlåtandena fästes uppmärksamhet vid de dynamiska autentiseringsfaktorer för identifieringsmetoden som krävs enligt 8 a § i förslaget och till denna del har propositionen kompletterats.

Uppdatering av uppgifterna i befolkningsdatasystemet

I flera utlåtanden begärdes komplettering av 7 § i den lag som trädde i kraft vid ingången av 2016 i fråga om hur ofta leverantörer av identifieringsverktyg och certifikatutfärdare som tillhandahåller betrodda tjänster ska uppdatera de uppgifter ur befolkningsdatasystemet som de behöver för tillhandahållandet av identifieringstjänsterna. I några yttranden ansågs dessutom att dessa kontroller i befolkningsdatasystemet ska vara avgiftsfria. Bestämmelsen i paragrafen har nyligen trätt i kraft. Uppgifterna ska dock uppdateras så pass ofta att man i tillräcklig utsträckning kan försäkra sig om att uppgifterna inte är föråldrade. Kommunikationsverket övervakar att bestämmelsen iakttas.

Bedömning av överensstämmelse i fråga om identifieringstjänster

I de utlåtanden som lämnades ansågs det å ena sidan att bedömningen av överensstämmelse förbättrar informationssäkerheten för elektronisk identifiering, men å andra sidan ansågs det som problematiskt att bedömningarna ska vara gjorda redan vid utgången av 2016 trots att bedömningsgrunderna ännu inte är klara.

I fråga om bemyndigandena för Kommunikationsverket att utfärda föreskrifter ansågs det i vissa yttranden att de auditeringskriterier som gäller leverantörer av identifieringstjänster ska avgränsas noggrannare i lagen. Kommunikationsverkets föreskrifter behandlas under punkten lagstiftningsordning i propositionen. Utifrån de yttranden som lämnades har bestämmelserna om att utse organ för bedömning av överensstämmelse och de hänvisningar som ska göras till dem preciserats.

I fråga om organen för bedömning av överensstämmelse i 4 kap. i lagförslaget ansåg justitieministeriet att de eventuella offentliga förvaltningsuppgifterna för dessa organ och organisationer måste bedömas. Frågan behandlas under punkten lagstiftningsordning i propositionen.

Kommunikationsverkets befogenheter och tillsyn

Enligt förslaget ska Kommunikationsverket ha rätt att utföra inspektioner av leverantörer av identifieringstjänster och andra aktörer som föreskrivs i lagen eller av deras tjänster för att övervaka efterlevnaden av åligganden enligt autentiseringslagen och EU:s förordning om elektronisk identifiering.

FiCom ry motsatte sig att Kommunikationsverkets inspektionsbefogenheter definieras så att Kommunikationsverket skulle har rätt att utföra inspektion endast i syfte att utöva tillsyn över den nationella lagstiftningen eller EU-lagstiftningen utan skäl att misstänka att aktören väsentligen har brutit mot lagen eller EU-lagstiftningen. Kommunikationsverkets granskningsrätt i enlighet med denna proposition säkerställer dock att Kommunikationsverket har effektiva metoder för att utöva tillsyn över efterlevnaden av den nationella lagstiftningen och EU-lagstiftningen. Den föreslagna granskningsrätten har samma innehåll som exempelvis i informationssamhällsbalken (917/2014).

Enligt propositionens har Kommunikationsverket rätt att meddela närmare föreskrifter om egenskaperna hos förtroendenätets gränssnitt. Motiveringen till bestämmelsen har kompletterats så att Kommunikationsverket får bestämma det gränssnitt som ska tillämpas, men avsikten är inte att begränsa möjligheten för tjänsteleverantörerna inom förtroendenätet att komma överens om att så länge det behövs använda sådana gränssnitt som redan nu används.

I sitt yttrande förslog Kommunikationsverket flera ändringar och tillägg i fråga om tillsyn och påföljder. Efter remissbehandlingen har propositionen kompletterats med möjligheten för

Kommunikationsverket att ge en anmärkning till den som bryter mot autentiseringslagen och ålägga aktören att rätta till felet eller försummelsen på samma sätt som det föreskrivs i informationssamhällsbalken. Till förslaget har dessutom fogats befogenhet för Kommunikationsverket att meddela ett interimistiskt beslut i brådskande fall. Också enligt eIDAS-förordningen krävs effektiva befogenheter för tillsynsmyndigheten så att den snabbt kan ingripa i förfaranden som strider mot bestämmelserna.

Uppgifter som föreslås för myndigheterna och konsekvenser för myndigheterna

Det ansågs befogat och att de uppgifter som föranleds av eIDAS-förordningen ges till Kommunikationsverket och Befolkningsregistercentralen och detta understöddes.

I yttrandena begärdes en uppskattning av konsekvensen av propositionen på Patent- och registerstyrelsens intäktsflöden och på Säkerhets- och kemikalieverkets ackrediteringsverksamhet. Det är svårt att uppskatta propositionens konsekvenser när det gäller Patent- och registerstyrelsens inkomster. Hur efterfrågan på identifieringsverktyg som tillhandahålls för juridiska personer och elektroniska stämplar kommer att utvecklas i Finland är också svårt att förutspå. Förslaget bedöms inte i någon betydande omfattning öka arbetsbördan vid Säkerhets- och kemikalieverkets ackrediteringsenhet.

Inrikesministeriet och Polisstyrelsen understödde förslaget om att identifieringsverktyg för stark autentisering inte längre ska kunna beviljas på basis av körkort. Samtidigt begärde de en bedömning av konsekvenserna av detta när det gäller beviljande av körkort och pass till dem som i fortsättningen skulle ha använt sig av körkort i enlighet med den gällande lagen.

Avgifter som ska tas ut hos aktörerna (47 §)

I fråga om tillsynsavgifter som ska tas ut hos aktörerna fästes i vissa av yttrandena uppmärksamhet vid hur avgifterna inverkar på aktörer som är på väg in i branschen och om avgifterna är aktörs- eller tjänstespecifika. I yttrandena ansågs att det skulle vara bättre att inte föreskriva om tillsynsavgifterna på lagnivå. Eftersom avgifterna måste anses vara av skattenatur är detta dock inte möjligt.

Många aktörer ansåg att de föreslagna avgifterna som ska betalas till Kommunikationsverket är för höga eller så motsatte de sig dem helt och hållet. Avsikten är dock att avgifterna till Kommunikationsverket ska täcka de kostnader som föranleds av Kommunikationsverkets tillsyn, varför de inte har kunnat strykas ur propositionen. Utifrån yttrandena föreslås det i propositionen att begäran om omprövning tas i bruk i fråga om de av Kommunikationsverkets beslut som gäller avgifter i enlighet med 47 § autentiseringslagen.

Övergångsbestämmelser

I vissa utlåtanden betonades frågor i anknytning till övergångsperioden för genomförandet av eIDAS-förordningen och de föreslagna lagändringarna.

Kommunikationsverket föreslog också övergångsbestämmelser som säkerställer att den starka statusen för nuvarande och nya identifieringsverktyg kvarstår och gör den tydligare och säkerställer och klargör bedömningen av de tillitsnivåer som föreskrivs i EU-lagstiftningen före bestämmelserna om förtroendenätverk börjar tillämpas den 1 maj 2017. I propositionen har övergångsbestämmelser med detta syfte införts.

Övriga lagförslag

Justitieministeriet påpekade att det i skattelagarna i utkastet till proposition föreslogs att det i fråga om underskrift av handlingar som lämnas till myndigheter fortfarande krävs avancerad elektronisk signatur. Vid den fortsatta beredningen har bestämmelserna till denna del gjorts mer flexibla.

8 Förhållande till andra propositioner

Regeringen lämnade riksdagen proposition RP 29/2016 med förslag till lagstiftning om reformering av beskattningsförfarandet och skatteuppbörden, där det föreslås en ny lag om beskattningsförfarande för skatter som betalas på eget initiativ. I 80 § i propositionen hänvisas till lagen om stark autentisering och elektroniska signaturer. Från och med den 1 juli i år borde i detta lagrum hänvisas till EU:s förordning om elektronisk identifiering.

Regeringen lämnade i april 2016 riksdagen en proposition till lag om identitetskort och till vissa lagar som har samband med den, RP 41/2016 rd, och en proposition till lag om gemensamma stödtjänster för e-tjänster och lag om ändring av lagen om anordnande av statens gemensamma informations- och kommunikationstekniska tjänster, RP 59/2016 rd. I de föreslagna lagarna hänvisas det till lagen om stark autentisering och elektroniska signaturer, vars namn föreslås bli ändrat i denna proposition. I propositionen med förslag till lag om identitetskort och till vissa lagar som har samband med den föreslås det dessutom ändringar i 61, 66 och 68 § i lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster, som också föreslås bli ändrade i denna proposition.

Vid finansministeriet pågår ett lagstiftningsprojekt med syftet att genomföra Europaparlamentets och rådets direktiv 2014/92/EU om jämförbarhet för avgifter som avser betalkonto, byte av betalkonto och tillgång till betalkonto med grundläggande funktioner (betalkontodirektivet). I samband med genomförandet av direktivet bedöms om det i Finland ska krävas av kreditinstituten att de som en del av de grundläggande banktjänsterna också tillhandahåller sådana starka elektroniska identifieringsverktyg som avses i autentiseringslagen.

DETALJMOTIVERING

1 Lagförslag

1.1 Lagen om stark autentisering och betrodda elektroniska tjänster

Terminologin. I terminologin på området används på finska allmänt orden ’tunnistaminen’ ja ’tunnistus’ som parallella termer, och det görs ingen egentlig betydelseskillnad mellan orden. I den gällande autentiseringslagen används ordet ’tunnistaminen’ när det förekommer ensamt eller som efterled i ett sammansatt ord. Ordet ’tunnistus’ används som förled i sammansatta ord såsom ’tunnistusväline’ (identifieringsverktyg), ’tunnistuspalvelu’ (identifieringstjänst) och ’tunnistustapahtuma’ (identifieringstransaktion) och det finns veterligen ingen risk för förväxling med terminologi som används på andra områden. På svenska används ordet ’identifiering’, utom i fråga om ’vahva sähköinen tunnistaminen’ och sammansättningar där ’vahva sähköinen’ ingår. Då används ’stark autentisering’ och sammansättningar med ’stark autentisering’.

1 §. *Tillämpningsområde*. I förslaget ändras paragrafen om lagens tillämpningsområde. Paragrafen reglerar tillämpningsområdet och begränsningarna av det med beaktande av EU:s förordning om elektronisk identifiering. I paragrafens 1 och 2 mom. fastställs tillämpningsområdet och i 3–4 mom. preciseringar och undantag från tillämpningsområdet i 1 och 2 mom.

I paragrafens 1 mom. föreskrivs det om stark autentisering samt tillhandahållande av identifieringstjänster till de tjänsteleverantörer som har förtroende för dem och till allmänheten. Efter den föreslagna lagändringen gäller största delen av bestämmelserna i lagen stark autentisering och uttryckligen tillhandahållandet av identifieringstjänster. Elektroniska underskrifter och övriga betrodda tjänster regleras i fortsättningen i eIDAS-förordningen. Lagen gäller inte så kallad svag identifiering som karaktäriseras av att den grundar sig på användarnamn och lösenord som en person själv har bestämt.

Allmänheten tillhandahålls tjänster för stark autentisering såsom i den gällande 1 §. Med allmänheten avses en på förhand obegränsad grupp fysiska eller juridiska personer. En grupp som är begränsad till exempel på grund av arbets- eller tjänsteförhållande räknas inte till allmänheten.

Identifieringstjänster tillhandahålls tjänsteleverantörer som har förtroende för dem. Ett typfall där identifieringstjänst tillhandahålls kan anses vara en tjänst där en tjänsteleverantör som använder stark autentisering för att tillhandahålla sin övriga service överför den som ska identifieras att identifiera sig utanför den egna tjänsten. Karaktäristiskt för ett sådant arrangemang är att det mellan leverantörer av tjänster för stark autentisering, tjänsteleverantörer som använder stark autentisering och innehavare av identifieringsverktyg råder ett rättsläge som fastställts genom ett avtalsförhållande. En leverantör av tjänster för identifieringsförmedling förmedlar till tjänsten för ärendehantering identifieringstransaktioner från leverantörer av identifieringsverktyg i det förtroendenät som det föreskrivs om i 12 a §.

Enligt det föreslagna 2 mom. föreskrivs det i lagen om tillsynen över eIDAS-förordningen genom en komplettering av förordningen. I förordningen föreskrivs det om kraven på betrodda tjänster och tillhandahållandet av dem. Med betrodda tjänster avses enligt eIDAS-förordningen och definitionen i den föreslagna 2 § elektroniska tjänster som i allmänhet tillhandahålls mot ersättning och som består av elektroniska underskrifter, elektroniska stämplar eller elektronisk tidsstämpling, elektroniska tjänster för rekommenderade leveranser och tjänster för skapande, kontroll och validering av certifikat i anslutning till dem. Också skapande,

kontroll och validering av certifikat för autentisering av webbplatser samt bevarande av elektroniska underskrifter, stämplar eller certifikat i anslutning till dem är betrodda tjänster.

Tjänsterna för elektroniska underskrifter och de övriga betrodda tjänsterna som nämns ovan regleras i fortsättningen genom lagstiftning från EU som ska tillämpas direkt, så största delen av föreskrifterna om elektroniska signaturer och signeringscertifikat i den gällande lagen måste upphävas. Det föreslås dock att föreskrifterna om återkallande av ett godkänt certifikat för signatur (36 § i den gällande lagen) och föreskrifterna om obehörig användning av signaturframställningsdata (40 § i den gällande lagen) bibehålls i lagen. Det föreslås att i lagen införs vissa av bestämmelserna om begränsning av ansvaret för tillhandahållare av betrodda tjänster i den gällande lagen (41 § i förslaget).

Medlemsstaterna ska dessutom utse ett nationellt tillsynsorgan, det vill säga en myndighet, som kontrollerar att eIDAS-förordningen iakttas. Enligt den föreslagna 42 a § är det i Finland Kommunikationsverket som kontrollerar att förordningen följs. I propositionen föreslås det även att eIDAS-förordningen kompletteras, till exempel i fråga om behörighetskraven för organ för bedömning av överensstämmelse för betrodda tjänster och andra oberoende bedömningsorgan samt i fråga om Kommunikationsverkets och Befolkningsregistercentralens uppgifter i anslutning till eIDAS-förordningen.

Enligt det föreslagna 3 mom. tillämpas denna lag på identifieringsverktyg som anmälts till EU och på förmedling av gränsöverskridande elektronisk identifiering bara om annat inte följer av eIDAS-förordningen. I förordningen föreskrivs det om tre tillitsnivåer i elektronisk identifiering (låg, väsentlig och hög) och i EU:s genomförandeakt har kraven på system för elektronisk identifiering specificerats för olika tillitsnivåer. Systemen ska uppfylla kraven som gäller respektive tillitsnivå för att de ska få anmälas till Europeiska kommissionen som gränsöverskridande system för elektronisk identifiering. EU:s medlemsstater ska under vissa förutsättningar i sina offentliga tjänster godkänna elektroniska identifieringsverktyg som andra EU-stater har anmält.

I eIDAS-förordningen föreskrivs det om förfarandet som gäller anmälning av system för elektronisk identifiering till kommissionen (artiklarna 7–10) och ett interoperabilitetsramverk som medlemsstaterna upprätthåller (artikel 12) där de system som medlemsstaterna anmält fungerar interoperabelt samt om medlemsstaternas administrativa samarbetsnätverk kring detta.

I det föreslagna 4 mom. preciseras tillämpningsområdet genom att vissa fall utesluts ur tillämpningsområdet för lagen. I fråga om elektronisk identifiering motsvarar begränsningarna av tillämpningsområdet den gällande lagen. Tillämpningsområdet för bestämmelserna om elektroniska underskrifter såsom även för andra betrodda tjänster fastställs i eIDAS-förordningen.

Enligt det föreslagna 4 mom. tillämpas lagen inte på tillhandahållandet av tjänster som används för intern identifiering i en sammanslutning. Samma leverantör av identifieringstjänster kan tillhandahålla samma tjänst såväl allmänt för en tjänsteleverantör som använder identifieringstjänsten i förtroendenätet för identifiering av en grupp som inte bestämts på förhand som för en sammanslutning att användas för dennas interna behov. Det första fallet hör till tillämpningsområdet för lagen medan det andra inte gör det.

Enligt den andra satsen i det föreslagna 4 mom. hör inte heller de fall till tillämpningsområdet där en sammanslutning använder en egen identifieringsmetod för att i samband med sina egna tjänster identifiera de egna kunderna. I den verksamheten är det inte alls egentligen fråga om

tillhandahållande av en stark autentiseringstjänst; tjänsteleverantörens syfte är att tillhandahålla en annan egen tjänst och identifieringen ingår där endast som en biprodukt.

Tillämpningsområdet för den gällande lagen och begränsningarna som gjorts i den är en direkt följd av att man genom lagen har velat ge grundläggande bestämmelser för allmänt använda verktyg för stark autentisering på marknaden. Om gruppen som använder ett verktyg är begränsad i förväg kan den inte konkurrera på den öppna marknaden med sikte på allmänt använda metoder och verktyg. De som använder företags och organisationers interna system behöver inte heller skydd på samma sätt som de som själva, ofta i egenskap av konsumenter, skaffar sina verktyg på marknaden. De som använder identifieringsverktyg som är avsedda för ett visst slutet ändamål har också ett mindre behov av skydd, för de eventuella riskerna är mindre vid användningen av dem.

Dessutom ska det beaktas att tillhandahållandet av tjänster för elektronisk identifiering fortfarande befinner sig i en utvecklingsfas och under kommande år är det också möjligt att nya identifieringsmetoder skapas i och med den tekniska utvecklingen. Därför är det synnerligen viktigt att lagstiftningen ger verksamhetsmöjligheter till nya arrangemang som utvecklas. Nya metoder kan till exempel testas i slutna miljöer innan de tillhandahålls som allmänt använda verktyg på öppna marknaden. Tjänsterna omfattas av lagstiftningen först när de som stark autentisering börjar tillhandahållas användargrupper som inte har begränsats i förväg.

2 §. *Definitioner*. Jämfört med den gällande lagen föreslås det att en stor del av definitionerna i paragrafen ändras eller upphävs som överlappande beroende på eIDAS-förordningen. Även 12 a § om förtroendenätet för leverantörer av identifieringstjänster som fogades till lagen 2015 kräver ändringar i definitionerna. För tydlighetens skull föreslås det att 2 § ändras helt.

I paragrafens 1 mom. 1 punkt definieras *stark autentisering*. Med det avses identifiering av en person, en juridisk person eller en fysisk person som företräder en juridisk person och verifiering av identifikatorns autenticitet och riktighet genom tillämpning av en elektronisk metod där identifieringen och verifieringen grundar sig på tillitsnivån väsentlig eller hög som definieras i artikel 8 i eIDAS-förordningen (EU) nr 910/2014. Definitionen är i övrigt den samma som i förordningen, men till definitionen på stark autentisering hör endast tillitsnivåerna väsentlig och hög som fastställs i förordningen. I förordningen och i kommissionens genomförandeakter som utfärdats med stöd av den anges även tillitsnivån låg, men den ska inte ingå i definitionen på stark autentisering i Finland.

I paragrafens 1 mom. 2 punkt definieras *identifieringsverktyg*. I eIDAS-förordningen används i samma betydelse termen medel för elektronisk identifiering som därför har tagits med i definitionen på identifieringsverktyg. I lagen bibehålls parallellt med medel för elektronisk identifiering termen identifieringsverktyg, som språkligt sett ofta är begripligare. Definitionen är till innehållet den samma som i den gällande lagen. Definitionen är teknologineutral och beskriver allt det som i fysisk eller elektronisk form eller i form av data tillsammans bildar ett identifieringsverktyg. Med ett verktyg kan således avses till exempel ett certifikat på ett SIM-kort eller något annat kort och den PIN-kod som behövs för att kunna använda certifikatet, användaridentifikation i kombination med ett växlande lösenord eller fingeravtryck som kombineras med en PIN-kod. Verktyget bildar en helhet.

I paragrafens 1 mom. 3 punkt definieras leverantör av identifieringstjänster. Definitionen bibehålls i sak, men efter tillägget av 12 a § om förtroendenät har det uppstått ett behov av att använda leverantörer av identifieringstjänster som överbegrepp för leverantör av identifieringsverktyg som definieras i paragrafens 4 punkt och leverantör av tjänster för identifieringsförmedling som definieras i 5 punkten. Skyldigheterna för en leverantör av rena förmedlingstjänster klarläggs i lagen i förhållande till skyldigheterna för en leverantör av identifierings-

verktyg. I 9 § i förslaget ställs allmänna krav på tillförlitligheten hos leverantörer av identifieringstjänster. Leverantörer av starka autentiseringstjänster ska med stöd av 9 § alltid vara juridiska personer.

Med leverantör av identifieringsverktyg avses enligt 1 mom. 4 punkten en tjänsteleverantör som tillhandahåller eller ger ut tjänster för stark autentisering till allmänheten. Leverantörer av identifieringsverktyg lämnar en anmälan som avses i 10 § till Kommunikationsverket varefter den antecknas i registret enligt 12 § och ingår i förtroendenätet som regleras i 12 a §. I förtroendenätet ska en leverantör av identifieringsverktyg tillhandahålla leverantörer av förmedlingstjänster sitt verktyg, men leverantören av identifieringsverktyg kan dessutom genom egen tjänst för identifieringsförmedling tillhandahålla förlitande parter sitt identifieringsverktyg, och agerar då även i rollen som leverantör av tjänster för identifieringsförmedling.

Med allmänheten avses en grupp användare som inte har begränsats i förväg såsom i 1 § 1 mom. Tjänsteleverantören kan använda ett medel för stark autentisering för att identifiera sina egna kunder och tillhandahålla andra förlitande parter eller en annan leverantör av tjänster för identifieringsförmedling som definieras nedan i 6 § samma medel för stark autentisering. Det föregående fallet, där tjänsteleverantören använder medel för stark autentisering för att identifiera sina egna kunder, hör inte till tillämpningsområdet för autentiseringslagen. Däremot hör det senare fallet till lagens tillämpningsområde. Beskrivningen gäller till exempel banker som använder bankkoder för de egna kundernas bankärenden och tillhandahåller samma koder att användas för andra tjänster där elektronisk identifiering utnyttjas.

Med *leverantör av tjänster för identifieringsförmedling* avses i 1 mom. 5 punkten en tjänsteleverantör som förmedlar identifieringstransaktioner baserade på stark autentisering till en förlitande part. Definitionen är ny och behövs på grund av förtroendenätet som regleras i 12 a §. Leverantörer av tjänster för identifieringsförmedling lämnar en anmälan som avses i 10 § till Kommunikationsverket varefter den antecknas i registret enligt 12 § och ingår i förtroendenätet som regleras i 12 a §.

Leverantören av tjänster för identifieringsförmedling ingår avtal med leverantörer av identifieringsverktyg som avses i 4 punkten om vidare förmedling av identifieringsdata (identifieringstransaktioner) som avses i 12 a § till parter som förlitar sig på identifieringen, det vill säga till exempel tjänsteleverantörer som utnyttjar stark autentisering i sina egna tjänster. Ett exempel på en förlitande part är en nätbutik eller en annan organisation som skaffar en identifieringstjänst för sin elektroniska tjänst för ärendehantering eller en identifieringstjänst för allmänheten som ska byggas upp i samband med en nationell servicekanal som inte förmedlar identifieringstransaktioner utanför statsförvaltningen och organisationer som sköter offentliga uppgifter.

Med *innehavare av identifieringsverktyg* avses i denna lag en fysisk eller en juridisk person som har ett identifieringsverktyg för stark autentisering på basis av laglig rätt. Om den berättigade innehavaren råkar tappa bort ett verktyg kan till exempel inte den som hittar det bli en innehavare som avses i definitionen. Definitionen ändras jämfört med definitionen i den gällande lagen, och på så vis kan identifieringsverktyg även beviljas och överlåtas till juridiska personer. Då överensstämmer den med definitionen i eIDAS-förordningen. I 23 § 2 mom. i lagen fastslås det klart att innehavaren av ett identifieringsverktyg inte får överlåta verktyget för att användas av någon annan.

Med *inledande identifiering* som definieras i paragrafens 7 punkt avses verifiering av identiteten hos en fysisk person eller verifiering av en juridisk persons status som juridisk person innan verktyget beviljas. Den inledande identifieringen är den centrala grundpelaren i fråga om tillförlitligheten i stark autentisering. Den regleras i 17 § i den gällande lagen. Inledande iden-

tifiering är en term som etablerats i autentiseringslagen. Med hjälp av den ville man tydligt skilja denna särskilda identifiering från senare identifieringstransaktioner som upprepas flera gånger.

Enligt 17 § i gällande lag kan inledande identifiering ske på två sätt (RP 272/2014 rd): 1) om en sökande inte redan har ett identifieringsverktyg för stark autentisering enligt denna lag ska identifieringen ske personligen, 2) en sökande som redan har ett elektroniskt identifieringsverktyg för stark autentisering får ansöka om ett identifieringsverktyg som avses i denna lag på elektronisk väg. I denna proposition föreslås att bestämmelserna om inledande identifiering ändras så att i Finland är det möjligt att identifiera en fysisk person på det sätt som föreskrivs i avsnitt 2.1.2 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering.

Definitionerna på *certifikat och certifikatutfärdare* motsvarar definitionerna i den gällande lagen (RP 36/2009).

Med *förtroendenätet* avses ett nätverk av leverantörer av identifieringstjänster som anmält sig hos Kommunikationsverket. Definitionen motsvarar definitionen i den gällande lagen (RP 272/2014).

Enligt den föreslagna 11 punkten avses med organ för bedömning av överensstämmelse ett organ enligt artikel 2.13 i förordning (EG) nr 765/2008 (s.k. NLF-förordningen) som är ackrediterat i överensstämmelse med den förordningen. Bestämmelser om bedömningar utförda av organet för bedömning av överensstämmelse finns i eIDAS-förordningen.

I det föreslagna 2 mom. räknas de definitioner upp som har samma betydelse som de har i eIDAS-förordningen. Med *elektronisk underskrift* avses i förordningen uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra uppgifter i elektronisk form och som används av undertecknaren för att skriva under. En elektronisk underskrift uppstår genom att elektroniska data fogas till varandra på ett sådant sätt att de bildar en unik kombination som gör det möjligt att verifiera undertecknaren. Enkel elektronisk underskrift är ett vitt begrepp. Syftet med enkla elektroniska underskrifter är att identifiera den person som skriver under och att verifiera uppgifter. Det kan röra sig om något så enkelt som att underteckna ett e-postmeddelande med en persons namn, men egentliga krav hör ihop med elektroniska underskrifter som görs med godkända anordningar för underskrift baserade på avancerade eller kvalificerade certifikat.

Med *betrodd tjänst* avses i eIDAS-förordningen en elektronisk tjänst som vanligen tillhandahålls mot ekonomisk ersättning och som består av: 1) skapande, kontroll och validering av elektroniska underskrifter, elektroniska stämplar eller elektroniska tidsstämplingar, elektroniska tjänster för rekommenderade leveranser och certifikat med anknytning till dessa tjänster, eller 2) skapande, kontroll och validering av certifikat för autentisering av webbplatser, eller 3) bevarande av elektroniska underskrifter, stämplar eller certifikat med anknytning till dessa tjänster.

Med *avancerad elektronisk underskrift* avses en elektronisk underskrift som uppfyller kraven enligt artikel 26 i eIDAS-förordningen. Den elektroniska underskriften ska vara unikt knuten till undertecknaren och undertecknaren ska kunna identifieras genom den. En avancerad elektronisk underskrift är skapad på grundval av uppgifter för skapande av elektroniska underskrifter som undertecknaren med hög grad av tillförlitlighet kan använda uteslutande under sin egen kontroll. Vidare ska en avancerad elektronisk underskrift vara kopplad till de uppgifter som den används för att underteckna på ett sådant sätt att alla efterföljande ändringar av uppgifterna kan upptäckas.

Med *system för elektronisk identifiering* avses i eIDAS-förordningen ett system för elektronisk identifiering genom vilket medel för elektronisk identifiering utfärdas till en fysisk eller juridisk person eller en fysisk person som företräder en juridisk person. Begreppet används till exempel i 8 §.

Med *förlitande part* avses en fysisk eller juridisk person som förlitar sig på en elektronisk identifiering eller betrodda tjänster.

6 §. *Behandling av personuppgifter*. Det föreslås att ett nytt 2 mom. fogas till paragrafen, de gällande1 och 3 mom. föreslås bli ändrade så att i dem hänvisas till certifikatutfärdare som tillhandahåller betrodda tjänster och laghänvisningarna i 4 mom. föreslås bli justerade.

Det har bedömts att en tjänst för identifieringsförmedling i förtroendenätet som avses i 12 a § i autentiseringslagen fungerar som en självständig registerförare. Denna ansvarar då för hantering av personuppgifter och bland annat för att den överlåter uppgifter endast till aktörer vilkas rätt att hantera uppgifter grundar sig på lag eller avtal. Enligt det föreslagna nya 2 mom. har leverantörer av tjänster för identifieringsförmedling rätt att vid förmedling av identifiering överlåta personuppgifter till en förlitande part, om den förlitande parten har rätt att behandla personuppgifter enligt lag.

Om Tjänsten för identifieringsförmedling hanterar och förmedlar även andra personuppgifter än de som är nödvändiga med tanke på identifiering (s.k. komplettering av personuppgifter) kan avgörandet om ansvarig registerförare separeras i fråga om personuppgifter som är nödvändiga för identifieringen och övriga personuppgifter som ska förmedlas.

7 §. *Användning av uppgifter i befolkningsdatasystemet*. Det föreslås att paragrafens 1 mom. preciseras så att skyldigheten att hämta och uppdatera uppgifter som behövs för tillhandahållandet av identifieringstjänsterna i befolkningsdatasystemet gäller leverantörer av identifieringsverktyg och inte leverantörer av tjänster för identifieringsförmedling. Uppgifterna ska uppdateras så pass ofta att man på ett tillräckligt sätt kan försäkra sig om att de inte är föråldrade. Kommunikationsverket övervakar att bestämmelsen iakttas.

7 a §. *Användning av uppgifter i företags- och organisationsregister*. Lagen föreslås få en ny bestämmelse enligt vilken leverantörer av identifieringsverktyg och certifikatutfärdare som tillhandahåller betrodda tjänster ska hämta och uppdatera uppgifter om juridiska personer som de behöver för tillhandahållandet av de betrodda tjänsterna i företags- och organisationsregistren. Föreskrifter om registren, som Patent- och registerstyrelsen för, finns i handelsregisterlagen (129/1979), i stiftelselagen (487/2015) samt i föreningslagen (503/1989) och i föreningsregisterförordningen (506/1989). Patent- och registerstyrelsens priser för handels-, stiftelse- och företagsinteckningsregistret grundar sig på lagen om avgifter för patent- och registerstyrelsens prestationer (1032/1992).

8 §. *Krav på system för elektronisk identifiering*. Det föreslås att paragrafen ändras. I 1 mom. räknas fyra faktorer upp som utgör förutsättningen för att ett system som tillhandahåller identifieringstjänster ska kunna anses starkt. Eftersom samma krav ställs på säkerhet i systemen för stark autentisering som i EU innehåller paragrafen hänvisningar till kommissionens genomförandeförordning som utfärdats med stöd av eIDAS-förordningen. Förordningen om tillitsnivåer vid elektronisk identifiering innehåller kraven som ställs på de olika tillitsnivåerna i systemen för identifiering.

Enligt den föreslagna 1 punkten ska identifieringsmetoden grunda sig på en omsorgsfull inledande identifiering så att uppgifterna om den kan kontrolleras i efterskott. Inledande identifiering definieras i 2 § 1 mom. 8 punkten och regleras i 17 och 17 a §. Enligt 24 § i lagen ska le-

verantören av identifieringsverktyg registrera de uppgifter som behövs om den inledande identifieringen och om den handling som anlitats.

Enligt den föreslagna 2 punkten ska metoden medge entydig identifiering av innehavaren av identifieringsverktyget så att åtminstone kraven för tillitsnivån väsentlig enligt avsnitt 2.1.2, 2.1.3 och 2.1.4 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering uppfylls.

Enligt den föreslagna 3 punkten ska det med hjälp av identifieringsmetoden med den tillförlitlighet som krävs för minst tillitsnivån väsentlig enligt avsnitt 2.3 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering gå att säkerställa att endast innehavaren av identifieringsverktyget kan använda verktyget.

Enligt den föreslagna 4 punkten ska identifieringsmetoden vara säker och tillförlitlig på det sätt som föreskrivs i avsnitt 2.2.1, 2.3.1 och 2.4.6 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering, med hänsyn till de informationssäkerhetsrisker som är förknippade med den teknik som används och de lokaler som används för tillhandahållandet av identifieringstjänsten är säkra på det sätt som föreskrivs i avsnitt 2.4.5 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering.

Enligt den föreslagna 5 punkten ska informationssäkerhetshanteringen skötas minst på tillitsnivån väsentlig i enlighet med det inledande stycket i avsnitt 2.4 och avsnitt 2.4.3 och 2.4.7 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering. I avsnitt 2.4.3 föreskrivs att ledningssystemet för informationssäkerhet följer utprovade standarder eller principer för hantering och kontroll av informationssäkerhetsrisker. Enligt avsnitt 2.4.7 förutsätts på tillitsnivån väsentlig regelbundna och oberoende interna eller externa revisioner som omfattar alla delar som är relevanta för tillhandahållandet av tjänster. Bestämmelser om dessa bedömningar finns i den föreslagna 29 §.

Ledning avseende informationssäkerhet regleras i avsnitt 2.4.3. i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering. På tillitsnivån väsentlig krävs det att leverantörer av identifieringstjänster har ett effektivt ledningssystem för informationssäkerhet för hantering och kontroll av informationssäkerhetsrisker. Dessutom ska ledningssystemet för informationssäkerhet följa utprovade standarder för hantering och kontroll av informationssäkerhetsrisker.

Det föreslagna 2 mom. ska vara likalydande som i den gällande lagen. Kommunikationsverkets bemyndigande att utfärda närmare tekniska föreskrifter enligt 8 § 3 mom. i den gällande lagen flyttas enligt förslaget till 42 §. Kommunikationsverkets behörighet att meddela tekniska föreskrifter definieras noggrannare än för närvarande till att gälla endast det som nämns i 1 mom. 4 och 5 punkten.

8 a §. *Autentiseringsfaktorer som ska användas i identifieringsmetoden*. Enligt det föreslagna 1 mom. måste i en identifieringsmetod minst två av autentiseringsfaktorerna som räknas upp användas. En bestämmelse motsvarande den föreslagna bestämmelsen ingår i definitionen på stark autentisering enligt 2 § i den gällande lagen. Den föreslagna bestämmelsen i 1 mom. ingår även i förordningen om tillitsnivåer vid elektronisk identifiering. Den föreslagna bestämmelsen har utformats teknikneutralt. Med kunskapsbaserade autentiseringsfaktorer avses något som personen måste kunna visa att den har kunskap om, exempelvis ett lösenord. Med innehavsbaserade autentiseringsfaktorer avses något som personen måste kunna visa att den innehar, exempelvis en nyckeltalslista, ett smartkort eller mobilcertifikat. Egenskapsbaserade autentiseringsfaktorer utgår från en kroppslig egenskap hos en fysisk person, exempelvis fingeravtryck.

Enligt det föreslagna 2 mom. måste man i varje identifieringsmetod använda en sådan i avsnitt 2.3.1 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering avsedd dynamisk autentisering som kan ändras vid varje ny autentisering mellan en person och det system som kontrollerar personens identitet. Det bedöms att de nuvarande starka elektroniska identifieringsverktygen uppfyller dessa krav.

9 §. *Krav som gäller leverantörer av identifieringstjänster*. Enligt förslaget ändras paragrafens 1 mom. så att endast juridiska personer får vara leverantörer av identifieringstjänster medan fysiska personer inte längre får vara det. På så sätt överensstämmer föreskriften med avsnitt 2.4.1.1 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering. I praktiken har redan nu kraven på tillräckliga ekonomiska resurser i 13 § i autentiseringslagen lett till att fysiska personer inte har varit leverantörer av identifieringstjänster. Enligt det föreslagna 1 mom. får juridiska personer som fungerar som leverantörer av identifieringstjänster eller fysiska personer som handlar för deras räkning samt ledamöter eller ersättare i styrelsen eller förvaltningsrådet för en sammanslutning eller stiftelse som är tjänsteleverantör, liksom dess verkställande direktör och ansvariga bolagsmän eller andra personer i motsvarande ställning vara myndiga, inte vara försatta i konkurs och deras handlingsbehörighet får inte vara begränsad. I praktiken kan begränsningarna av handlingsbehörighet vara en följd av till exempel omyndighet.

Punkt 2.4.1 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering förutsätter att tillhandahållare av identifieringstjänster är juridiska personer. I övrigt motsvarar 1 mom. i sak det gällande 1 mom. (RP 36/2009 rd).

10 §. *Skyldighet för leverantörer av identifieringstjänster att anmäla att verksamheten inleds*. Enligt förslaget fogas till paragrafens 2 mom. en ny 5 punkt samt flyttas Kommunikationsverkets bemyndigande att meddela föreskrifter som ingår i 4 mom. till 42 § där Kommunikationsverkets befogenheter att meddela föreskrifter ska samlas. För tydlighetens skull föreslås det att hela paragrafen ändras.

Enligt paragrafens 1 mom. ska en leverantör av identifieringstjänster som är etablerad i Finland göra en skriftlig anmälan till Kommunikationsverket innan verksamheten inleds. Anmälan kan också göras av en sådan sammanslutning av leverantörer av identifieringsverktyg som administrerar en tjänst som ska betraktas som en enda identifieringstjänst. Enligt förslaget fogas till paragrafens 2 mom. en ny 5 punkt enligt vilken leverantören av en identifieringstjänst i sin anmälan också ska ha uppgifter om ett tillämpat bedömningsförfarande och resultaten av bedömningen. I det föreslagna 4 kap. i lagen föreskrivs det om behörigheten för bedömningsorganen för leverantörer av identifieringstjänster samt vilken typ av bedömningsorgan som ska användas i olika tjänster. De krav som ett bedömningsorgan enligt lagen bedömer en identifieringstjänst mot föreskrivs i lag och vid behov preciseras kraven genom föreskrift av Kommunikationsverket.

I 10 § 4 mom. i den gällande lagen ingår befogenhet för Kommunikationsverket att utfärda föreskrifter om det närmare innehållet i uppgifterna enligt 10 §. Det föreslås att befogenheten flyttas till 42 §. Kommunikationsverket kan i sin föreskrift beakta att det på grund av 12 a § kommer nya leverantörer av tjänster för identifieringsförmedling på marknaden och med tanke på tillsynen är det ändamålsenligt att kräva att leverantörer av identifieringstjänster anmäler olika allmänna uppgifter om de tjänster de tillhandahåller. Kommunikationsverket kan i sin föreskrift kräva nödvändiga uppgifter om de tjänster som tillhandahålls, till exempel om tjänsteleverantören tillhandahåller identifieringsverktyg eller tjänster för identifieringsförmedling eller både och. Med tanke på tillsynen är det dessutom nödvändigt att tjänsteleverantören anmäler på vilka tillitsnivåer (väsentlig, hög) enligt definitionerna i förordningen om tillitsnivåer vid elektronisk identifiering tjänsterna tillhandahålls.

Enligt bestämmelsen om den föreslagna lagändringens ikraftträdande gäller de föreskrifter Kommunikationsverket meddelat med stöd av den gällande lagen tills nya föreskrifter meddelats med stöd av den ändrade 42 §.

13 §. *Allmänna skyldigheter för leverantörer av identifieringstjänster*. Det föreslås att paragrafens 1 mom. ändras så att förvaringen av uppgifter, personalen och de tjänster som köps av underleverantörer hos leverantörer av identifieringstjänster uppfyller kraven för minst tillitsnivån väsentlig i EU:s förordning om tillitsnivåer vid elektronisk identifiering. De föreslagna skyldigheterna gäller såväl leverantörer av identifieringsverktyg som leverantörer av tjänster för identifieringsförmedling.

Vad gäller förvar av uppgifter ska kraven i punkt 2.4.4 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering följas. Informationen som hör till identifiering ska registreras och lagras med hjälp av ett effektivt registerhanteringssystem, Informationen lagras och skyddas tills den ska förstöras på ett säkert sätt.

Anläggningar och personal samt eventuella underleverantörer hos leverantörer av identifieringstjänster ska uppfylla kraven i avsnitt 2.4.5 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering. Leverantörer av identifieringstjänster ska se till att personal och underleverantörer som de har i sin tjänst är tillräckligt utbildade, kvalificerade och erfarna i de färdigheter som krävs för att sköta sina roller. Tillräcklig personal och underleverantörer ska finnas för att korrekt driva och bemanna tjänsten. Anläggningar som används för att tillhandahålla tjänsten ska kontinuerligt övervakas och skyddas mot faktorer som kan inverka på tjänstens säkerhet. Anläggningar som används för att tillhandahålla tjänsten ska säkerställa att tillträde till utrymmen där personliga eller kryptografiska uppgifter finns eller behandlas är begränsat till auktoriserad personal eller underleverantörer.

14 §. *Principer för identifiering*. Det föreslås att paragrafens 1 och 2 mom. ändras. Den svenska språkdräkten ändras i 3 mom. Paragrafens 4 mom. bibehålls oförändrad. Enligt förslaget preciseras 1 mom. så, att i synnerhet leverantörer av identifieringsverktyg i principer för identifiering ska ange närmare hur de genomför identifieringen enligt 17 och 17 a § när identifieringsverktyg beviljas.

I 2 mom. i den gällande lagen listas de centrala uppgifterna som ska anges i principerna för identifiering. I det ändrade 2 mom. är 3, 4 och 6 punkterna nya och de övriga motsvarar den gällande lagen (RP 36/2009). För tydlighetens skull föreslås det att 2 mom. ändras helt.

Enligt den föreslagna 3 punkten ska samtliga villkor som ska tillämpas och enligt 4 punkten de principer för informationssäkerhet som tillämpas i tjänsten anges i principerna för identifiering. Kravet grundar sig på avsnitt 2.4.2. i bilagan till förordningen om tillitsnivåer i elektronisk identifiering.

Ett nytt krav på centrala uppgifter som ska anges i principerna för identifiering är enligt 6 punkten uppgifterna i enlighet med 4 kap. om en bedömning utförd av ett oberoende bedömningsorgan eller annat bedömningsorgan. Enligt den övergångsbestämmelse som föreslås bör en leverantör av identifieringstjänster lämna en bedömningsrapport över verkställd oberoende bedömning av identifieringstjänsten och uppgifter om de ändrade principerna för identifiering som avses i 14 § till Kommunikationsverket senast den 31 januari 2017. Principerna för identifiering ändras när en leverantör av identifieringstjänster inleder sin verksamhet i förtroendenätet.

15 §. *Skyldighet för leverantörer av identifieringsverktyg att lämna uppgifter innan avtal ingås*. Enligt förslaget ändras för tydlighetens skull paragrafens rubrik och det inledande stycket i 1 mom. så att skyldigheterna i paragrafen gäller endast leverantörer av identifieringsverktyg.

16 §. *Skyldighet för leverantörer av identifieringstjänster att anmäla hot och störningar som riktas mot verksamheten eller skyddet av uppgifter*. Det föreslås att paragrafens rubrik samt 1 mom. ändras. Paragrafen föreslås få nya 4 och 5 mom. De nuvarande 2 och 3 mom. kvarstår som tidigare. För tydlighetens skull föreslås att hela paragrafen ändras. Anmälningsskyldigheten enligt 16 § i den gällande lagen gäller hot och störningar som riktas mot tjänsternas informationssäkerhet och skydd av uppgifter. Paragrafen ändras så att anmälningsskyldigheten gäller betydande hot och störningar som riktas mot tjänsternas funktion, informationssäkerheten eller användningen av en elektronisk identitet.

Den föreslagna paragrafen utvidgar anmälningsskyldigheten för leverantörer av identifieringstjänster till att gälla även övriga avtalsparter i förtroendenätet. I fortsättningen kan Kommunikationsverket tekniskt förmedla de anmälningar mellan aktörerna som avses i denna paragraf till leverantörerna av identifieringstjänster i förtroendenätet. Eftersom uppgifterna innehåller sekretessbelagd information som Kommunikationsverket bör bedöma och behandla enligt sekretessbestämmelserna i lagen om offentlighet i myndigheternas verksamhet (621/1999, nedan offentlighetslagen) har det till lagen också fogats en föreskrift enligt vilken Kommunikationsverket får förmedla uppgifter i förtroendenätet för anmälarens räkning utan hinder av vad som föreskrivs i offentlighetslagen. Kommunikationsverket tillhandahåller alltså endast en teknisk plattform för informationsutbyte i förtroendenätet men kontrollerar eller bedömer inte grunderna för informationen som överlåts, det sker på överlåtarens ansvar. Överlåtaren ansvarar också för specificeringen i det tekniska förmedlingssystemet av de medlemmar i förtroendenätet till vilka överlåtaren som dess avtalsparter eller annars förmedlar uppgifterna. De anmälningar om störningar som aktörerna gör till tillsynsmyndigheten Kommunikationsverket behandlar Kommunikationsverket i enlighet med offentlighetslagen och bildar sig utgående från dem en lägesbild över tjänsternas allmänna situation samt bedömer om verksamheten har uppfyllt de föreskrivna kraven.

Enligt det föreslagna 4 mom. får en leverantör av identifieringstjänster använda uppgifter om en annan leverantör av identifieringstjänster som den får med stöd av denna paragraf endast för att skapa beredskap för de hot och störningar som avses i paragrafen. Hos tillhandahållaren av betrodda tjänster får uppgifterna behandlas endast av dem som nödvändigt behöver uppgifterna i sitt arbete. Uppgifterna måste också annars behandlas så att affärshemligheter som tillhör en annan leverantör av identifieringstjänster inte röjs och att informationssäkerheten för verksamheten inte äventyras.

Enligt 5 mom. är en leverantör av identifieringstjänster som genom att handla i strid med 4 mom. vållar en annan leverantör av identifieringstjänster skada skyldig att ersätta för skadan.

17 §. *Identifiering av en fysisk person som ansöker om ett identifieringsverktyg*. Paragrafens rubrik ändras enligt förslaget så att den i fortsättningen gäller endast identifiering av en fysisk person.

Enligt 1 mom. i den gällande lagen ska den inledande identifieringen göras personligen om sökanden inte har ett tidigare verktyg för stark autentisering. Om sökanden redan har ett verktyg för stark autentisering, har ett nytt verktyg för stark autentisering fått sökas elektroniskt med det redan befintliga identifieringsverktyget på motsvarande nivå.

I det föreslagna 17 § 1 mom. föreskrivs om inledande identifiering av en person före det starka elektroniska identifieringsverktyget beviljas. I det föreslagna 1 mom. hänvisas till avsnitt 2.1.2

i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering där det föreskrivs om styrkande och kontroll av identitet i fråga om fysiska personer som ansöker om ett identifieringsverktyg med tillitsnivån väsentlig eller hög. Bestämmelserna i det föreslagna 1 mom. ska också tillämpas på starka elektroniska identifieringsverktyg som tillhandahålls i Finland, trots att de inte har anmälts till EU som så kallade gränsöverskridande identifieringsverktyg.

När det gäller tillitsnivån väsentlig föreskrivs i förordningen om tillitsnivåer vid elektronisk identifiering fyra olika alternativa sätt för leverantörer av identifieringsverktyg att göra inledande identifiering av en person. Enligt det föreslagna 1 mom. får alla dessa fyra sätt användas också vid inledande identifiering för de identifieringsverktyg som tillhandahålls i Finland. Enligt de två första alternativa sätten i avsnitt 2.1.2 i bilagan identifieras personen utifrån en identitetshandling antingen personligen eller elektroniskt. Elektroniskt kan en person med stöd av en identitetshandling identifieras på distans eller maskinellt. De dokument som godkänns för identitetskontrollen föreskrivs i 2 mom.

Enligt det tredje alternativet i avsnitt 2.1.2 i förordningen om tillitsnivåer vid elektronisk identifiering grundar sig identifieringen på en identifiering på motsvarande tillitsnivå utifrån ett så kallat tidigare kundförhållande eller på att man känner personen sedan tidigare. I detta fall kan kontrollen av en fysisk persons identitet grunda sig på ett förfarande som en offentlig eller privat tillhandahållare av identifieringsverktyg tidigare och i annat syfte än för beviljande av ett identifieringsverktyg för stark autentisering har använt sig av och som Kommunikationsverket godkänner utifrån de bestämmelser som gäller saken och utifrån myndighetstillsynen eller utifrån en bekräftelse av ett i 28 § 1 punkten avsett organ för bedömning av överensstämmelse. Ett förfarande där kontrollen av identiteten grundar sig på ett så kallat tidigare kundförhållande kräver Kommunikationsverkets godkännande. Förfarandet kan lämpa sig för exempelvis banker, för vilka det i lagen om förhindrande och utredning av penningtvätt och av finansiering av terrorism (503/2008) föreskrivs skyldighet att säkerställa kundens identitet utifrån handlingar eller uppgifter från en tillförlitlig och oberoende källa. Bankernas verksamhet övervakas utifrån den lagstiftning om penningtvätt som gäller dem av Finansinspektionen. Förfarandet för personer som man känner sedan tidigare kan passa också på beviljandet av det Befolkningsregistercentralens elektroniska certifikat som finns på identitetskort beviljande av polisen och som enligt den lagändring i fråga om identitetskort som är under beredning i enlighet med vissa villkor beviljas på samma sätt som själva identitetskortet, utan att någon personlig identitetshandling visas upp.

Enligt det fjärde alternativet i avsnitt 2.1.2 i förordningen om tillitsnivåer vid elektronisk identifiering identifieras personen utifrån ett elektroniskt identifieringsverktyg med samma tillitsnivå som personen i fråga redan har.

Paragrafens 2 mom. ändras så att leverantören av identifieringsverktyg i inledande identifiering, när identifieringen endast grundar sig på en identitetshandling som beviljats av en myndighet, vid kontrollen av identiteten inte längre får använda endast ett körkort som beviljats av en myndighet i Finland eller i någon annan medlemsstat i Europeiska ekonomiska samarbetsområdet. Bestämmelsen har en övergångsperiod till utgången av 2018. Från och med 2019 kan ett identifieringsverktyg inte längre beviljas genom att använda endast körkort vid kontrollen av identiteten i den inledande identifieringen av en person. Ändringen av praxis är nödvändig för att körkort inte längre kan anses vara ett intyg om identitet utan ett intyg om körrätt.

I de fall när identiteten hos den som ansöker om ett identifieringsverktyg inte kan verifieras på ett tillförlitligt sätt, ska i enlighet med 17 § 3 mom. i den gällande lagen polisen utföra den inledande identifiering som gäller ansökan. Denna bestämmelse i 3 mom. ändras inte.

17 a §. *Identifiering av en juridisk person som ansöker om ett identifieringsverktyg*. En juridisk persons angivna identitet verifieras i handels-, förenings- eller stiftelseregistret som upprätthålls av Patent- och registerstyrelsen. Dessutom måste man iaktta åtminstone kraven på tillitsnivån väsentlig i 2.1.3 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering.

19 §. *Certifikatets innehåll*. Den svenska språkdräkten ändras i punkt 8 så att elektroniska signatur ändras till elektroniska underskrift.

20 §. *Beviljande av identifieringsverktyg*. Det föreslås att paragrafens 3 mom. ändras på grund av förordningen om tillitsnivåer vid elektronisk identifierig. För tydlighetens skull föreslås också att paragrafens rubrik ändras. Ett identifieringsverktyg som avses i lagen har hittills kunnat beviljas endast fysiska personer, men eIDAS-förordningen gör det möjligt att bevilja juridiska personer identifieringsverktyg och enligt förslaget ska det även bli möjligt nationellt sett. Bindningen mellan fysiska och juridiska personers identifieringsverktyg ska genomföras enligt avsnitt 2.1.4 i EU:s förordning om tillitsnivåer vid elektronisk identifiering. Enligt förordningen om tillitsnivåer vid elektronisk identifiering ska styrkandet av identiteten för en fysisk person som handlar på den juridiska personens vägnar enligt kontroll ha utförts på nivån väsentlig eller hög på det sätt som föreskrivs i förordningen om tillitsnivåer vid elektronisk identifiering. Med andra ord måste den elektroniska identifikatorn för den fysiska person som anknutits till den juridiska personens identifikator uppfylla kraven i förordningen om tillitsnivåer vid elektronisk identifiering. Bindningen mellan den juridiska personen och den fysiska personen måste vara registrerad och kontrollerad hos i någon nationellt tillförlitlig källa. En sådan tillförlitlig källa kan i Finland anses vara åtminstone de register över företag och sammanslutningar som förs av Patent- och registerstyrelsen till den del som det i registren införs uppgifter om en fysisk persons rätt att företräda ett företag eller en sammanslutning. I förordningen om tillitsnivåer vid elektronisk identifiering förutsätts dessutom att en bidning ska vara möjligt att upphäva eller återkalla och att en fysisk person ska kunna får delegera nyttjandet av bindningen till en annan fysisk person på grundval av nationellt erkända förfaranden. Tillsvidare är det svårt att bedöma behovet av förfaranden i anknytning elektroniska identifieringsverktyg för juridiska personer, varför det i detta skede inte föreslås några närmare förfarandebestämmelser i lagen. Vid behov kan man stödja sig på annan lagstiftning i fråga om förhållandet mellan juridiska och fysiska personer.

Ett identifieringsverktyg beviljas endast en fysisk eller en juridisk person. Identifieringsverktyget ska vara personligt och med det avses här alltså även en juridisk person. Till ett verktyg kan vid behov fogas en uppgift om att en person i enskilda fall även kan företräda en annan fysisk person eller en juridisk person. Detta lämpar sig alltså på fall som på något sätt definierats separat, men den ovan beskrivna bindningen mellan en juridisk persons identifieringsverktyg och en fysisk persons identifieringsverktyg ska vara permanent och i princip en obegränsad lösning vad gäller uträttande av ärenden.

21 §. *Överlåtelse av identifieringsverktyg till sökande*. I propositionen föreslås det att 21 § ändras så att leverantören av identifieringsverktyg enligt avsnitt 2.2.2 i förordningen om tillitsnivåer vid elektronisk identifiering ska säkerställa att verktyget inte obehörigt kommer i någon annans besittning vid överlåtelsen. I förordningen om tillitsnivåer vid elektronisk identifiering förutsätt exempelvis i fråga om tillitsnivån väsentlig att medlet för elektronisk identifiering ska levereras genom en mekanism så att medlet kan antas nå endast den avsedda personen.

22 §. *Förnyande av identifieringsverktyg*. I propositionen föreslås det att 22 § preciseras så att den gäller en leverantör av identifieringsverktyg som förnyar ett verktyg som leverantören överlåtit till kunden. Paragrafen föreslås få en hänvisning till avsnitt 2.2.4 med krav på minst

tillitsnivån väsentlig i förordningen om tillitsnivåer vid elektronisk identifiering. Avsnitt 2.2.4 i bilagan har olika krav på tillitsnivåerna väsentlig och hög, som enligt den föreslagna lagen ska följas vid stark autentisering i Finland.

24 §. *Registrering och användning av uppgifter om identifieringstransaktioner och identifieringsverktyg*. Paragrafen anger de uppgifter som behövs till exempel om man i efterskott måste reda ut omständigheter som hänför sig till en identifieringstransaktion eller en rättshandling mellan en tjänsteleverantör som använder identifieringstjänster och en innehavare av ett identifieringsverktyg. Jämfört med den gällande 24 § ändras paragrafen så att skyldigheterna att registrera uppgifter som i 1 mom. fastställs för leverantörer av identifieringstjänster gäller såväl leverantörer av identifieringsverktyg som leverantörer av tjänster för identifieringsförmedling. Skyldigheterna i det föreslagna 2 mom. gäller endast leverantörer av identifieringsverktyg.

Enligt paragrafens 1 mom. ska leverantörer av identifieringstjänster registrera de uppgifter som behövs för att verifiera en enskild identifieringstransaktion. Med uppgifter enligt det föreslagna 1 mom. som hänför sig till en identifieringstransaktion avses det som leverantören av identifieringstjänster i samband med identifieringen anmäler till tjänsteleverantören som använder identifieringstjänsten, alltså den förlitande parten, och vilka omständigheter anmälan har grundat sig på. Dessutom ingår bland annat klockslag och datum i uppgifterna.

Vidare ska enligt 2 punkten leverantörer av identifieringsverktyg registrera uppgifter om sådana eventuella hinder och begränsningar för användningen av verktyget som avses i 18 §. Den föreslagna bestämmelsen garanterar att sådana eventuella användningsbegränsningar som avses i 18 § kan redas ut också i efterskott. Även för deras vidkommande torde det oftast gälla utredning av ansvarsförhållanden.

Enligt den föreslagna 1 mom. 3 punkten ska leverantörer av identifieringstjänster i fråga om certifikat registrera uppgifter om certifikatets innehåll enligt 19 §. Bestämmelsen motsvarar den som gäller för närvarande.

Enligt paragrafens 2 mom. ska leverantören av identifieringsverktyg registrera de uppgifter som behövs om den inledande identifieringen av en sökande som avses i 17 och 17 a § och om den handling eller elektroniska identifiering som då har använts. De uppgifter som behövs kan vara till exempel numret på ett pass eller ett identitetskort. I vissa situationer kan det finnas behov av att spara en kopia av handlingen som använts. Det kan vara nödvändigt att verifiera en sak i efterskott om ett identifieringsverktyg har getts till fel person. Det kan bli nödvändigt att utreda processen som avses i den föreslagna 17 § bland annat för att få reda på vem som ansvarar för den eventuella skadan om det visar sig att ett identifieringsverktyg har getts till fel person. I statsförvaltningen pågår ett projekt med syftet att göra det möjligt för en leverantör av identifieringsverktyg att kontrollera om en visad identitetshandling har anmälts stulen eller försvunnen.

Det föreslagna 3 mom. innehåller bestämmelser om bevaringstiden. Enligt det ska uppgifterna som avses i 1 mom. 1 punkten bevaras fem år efter identifieringstransaktionen. Övriga uppgifter och de som ska bevaras enligt 1 och 2 mom. ska bevaras i fem år efter det att ett fast kundförhållande har upphört. De föreslagna bevaringstiderna motsvarar bevaringstiderna i den gällande lagen. Bestämmelsen motsvarar bestämmelserna om konsumentskydd och kraven i föreskrifterna om penningtvätt. Det innebär samtidigt att en leverantör av identifieringstjänster måste förvara rätt stora datamängder. I en del fall ligger det naturligtvis även i tjänsteleverantörens eget intresse att förvara uppgifter.

Enligt paragrafens 4 mom. ska personuppgifter som har samlats in i samband med en identifieringstransaktion förstöras efter transaktionen om det inte enligt 1 mom. 1 punkten är nödvändigt att spara dem för att verifiera en enskild identifieringstransaktion. Med hjälp av bestämmelsen strävar man efter att minska mängden personuppgifter som sparas i tjänsteleverantörens system.

Paragrafens 5 mom. innehåller en begränsning av ändamålet med databehandlingen. Leverantören av identifieringstjänster får behandla registrerade uppgifter för eget bruk endast för att tillhandahålla och upprätthålla tjänsterna, fakturera och trygga sina rättigheter. I det senare fallet gäller det tvister. Dessutom får leverantören av identifieringstjänster behandla uppgifter vid fall av missbruk och på begäran av antingen en tjänsteleverantör som använder identifieringstjänster eller en innehavare av ett identifieringsverktyg eller av båda. I det fallet torde det röra sig om oklarhet mellan dem om en identifieringstransaktion och en eventuell rättshandling i samband med det.

Enligt den föreslagna bestämmelsen ska leverantören av identifieringstjänster registrera uppgifter om när och varför uppgifterna behandlats och vem som gjort det. Till exempel informationssamhällsbalken (917/2014) 145 § innehåller motsvarande föreskrift om att behandlingen av identifieringsuppgifter ska dokumenteras.

Paragrafens 6 mom. gäller tjänsteleverantörer som endast ger ut identifieringsverktyg. Registreringsskyldigheten enligt det föreslagna 1 mom. 1 punkten gäller naturligtvis inte en sådan tjänsteleverantör eftersom leverantören inte har sådana uppgifter. Förvaringstiden fem år som avses i paragrafen 3 mom. räknas då från det att redskapets giltighetstid har upphört.

25 §. *Anmälan om återkallande eller förhindrande av användning av identifieringsverktyg*. Bestämmelserna i de föreslagna 1–3 mom. har preciserats så att den anmälan som avses i 1 mom. ska göras till leverantören av identifieringstjänster och skyldigheterna enligt 2–3 mom. gäller leverantörer av identifieringsverktyg och inte leverantörer av tjänster för identifieringsförmedling.

26 §. *Rätten för leverantörer av identifieringsverktyg att återkalla eller förhindra användning av identifieringsverktyg*. Bestämmelserna i den gällande paragrafen föreslås bli kompletterade så att bestämmelserna gäller leverantörer av identifieringsverktyg och inte leverantörer av tjänster för identifieringsförmedling.

IV kap. Bedömning av överensstämmelse

I lagen föreslås ett kapitel med bestämmelser om bedömningen av överensstämmelse i fråga om elektroniska identifieringstjänster och i eIDAS-förordningen reglerade betrodda tjänster eller till dem anknutna verktyg samt om certifiering.

Bedömning av överensstämmelse för betrodda tjänster görs av organ för bedömning av överensstämmelse som har godkänts av Kommunikationsverket och vars behörighet har konstaterats utifrån ett förfarande, dvs. en ackreditering, som föreskrivs i lagen om konstaterande av tillförlitligheten hos tjänster för bedömning av överensstämmelse med kraven (920/2005).

På uppdrag av leverantörerna av identifieringstjänster görs bedömning av överensstämmelse också av oberoende och utomstående samt interna bedömningsorgan. Dessa organ godkänner Kommunikationsverket inte på förhand, med också dessa bedömningsorgan ska uppfylla de behörighetskrav som ställs på dem.

28 §. *Organ för bedömning av överensstämmelse*. Enligt den föreslagna paragrafen kan överensstämmelsen hos en tjänst enligt lagen bedömas av *ett organ för bedömning av överensstämmelse* som är godkänt av Kommunikationsverket, ett annat utomstående bedömningsorgan som fungerar enligt en allmänt använd metod *(annat utomstående bedömningsorgan*) eller ett oberoende bedömningsorgan inom tjänsteleverantörens organisation som uppfyller en allmänt använd standard (*internt kontrollorgan*). Ett kontrollorgan som hör till den sist nämnda kategorin hör alltså till samma organisation som föremålet för bedömningen och utför intern men likväl oberoende bedömning.

Ett organ för bedömning av överensstämmelse enligt 1 punkten har till uppgift att i enlighet med artiklarna 20 och 21 i eIDAS-förordningen bedöma om den betrodda tjänst som bedömningen gäller uppfyller kraven på betrodda tjänster i förordningen och i kommissionens genomförandebeslut som meddelats med stöd av förordningen. Organet för bedömning av överensstämmelse kan också bedöma om en leverantör av identifieringstjänster uppfyller kraven på sådana tjänster.

Ett annat utomstående bedömningsorgan enligt 2 punkten och ett internt kontrollorgan enligt 3 punkten har till uppgift att bedöma om identifieringstjänster överensstämmer med kraven som det föreskrivs om i 29 §.

29 §. *Bedömning av överensstämmelse hos en elektronisk identifieringstjänst*. Enligt det föreslagna 1 mom. ska överensstämmelse med kraven hos det identifieringssystem som används av en leverantör av identifieringstjänster påvisas av något av de bedömningsorgan som avses i 28 § 1, 2 eller 3 punkten. I praktiken ska en identifieringstjänst som avses i denna lag och som tillhandahålls av en leverantör av identifieringstjänster åtminstone vara bedömd av ett internt bedömningsorgan. På tillitsnivån hög krävs i enlighet med 8 § 1 mom. 5 punkten och avsnitt 2.4.7 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering en bedömning av ett utomstående bedömningsorgan.

I denna proposition är avsikten att minst samma krav ska ställas på system för stark autentisering som används i Finland som EU-lagstiftningen ställer på identifieringssystem på tillitsnivån väsentlig.

Skyldigheten att påvisa att ett identifieringssystem uppfyller kraven enligt det föreslagna 1 mom. gäller även de leverantörer av identifieringsförmedlingstjänster som verkar i förtroendenätet för elektronisk identifiering.

Det föreslagna 1 mom. innehåller allmänna bestämmelser om de kriterier som ska användas vid en bedömning av överensstämmelse. En tjänst för stark autentisering måste uppfylla kraven på interoperabilitet, informationssäkerhet och dataskydd och krav på annan tillförlitlighet.

Enligt det föreslagna 2 mom. föreskrivs det om bedömning av överensstämmelse hos ett system för elektronisk identifiering som anmäls till EU i eIDAS-förordningen och i förordningen om tillitsnivåer vid elektronisk identifiering som utfärdats med stöd av den. Om en leverantör av identifieringstjänster önskar att dess identifieringssystem ska anmälas till Europeiska kommissionen, måste leverantören i alla avseenden iaktta eIDAS-förordningen och de bestämmelser om bedömning av överensstämmelse hos identifieringssystem som har utfärdats med stöd av den.

Enligt 3 mom. ska Kommunikationsverket i kraft av 42 § bestämma vilka bedömningsgrunder som ska användas vid bedömningen av överensstämmelse. Som bedömningsgrund får Kommunikationsverket utöver de bestämmelser som avses i 1 och 2 mom. fastställa bestämmelser eller riktlinjer som utfärdats av EU eller ett annat internationellt organ, publicerade och gene-

rellt eller regionalt tillämpade anvisningar för informationssäkerhet samt datasäkerhetsstandarder eller förfaranden som används allmänt. Bestämmelsen i 3 mom. begränsar Kommunikationsverkets behörighet att meddela föreskrifter.

30 §. *Bedömning av överensstämmelse hos den nationella noden för elektronisk identifiering*. Enligt det föreslagna 1 mom. ska överensstämmelsen hos det nationella gränssnitt kallat den nationella noden som ingår i EU:s interoperabilitetsramverk för elektronisk identifiering påvisas genom en bedömning som utförs av ett bedömningsorgan enligt 28 § 1 punkten eller ett annat externt bedömningsorgan enligt 28 § 2 punkten. Den nationella noden ska i Finland upprätthållas av Befolkningsregistercentralen enligt 42 c §. Den nationella noden förmedlar identifieringshändelser över EU:s gränser i överensstämmelse med eIDAS-förordningen. Noden förmedlar bara identifieringshändelser. Den har ingen roll vid förmedlingen av elektroniska underskrifter eller andra betrodda tjänster som regleras i eIDAS-förordningen.

Kommunikationsverket ska enligt 42 § meddela föreskrifter om vilka bedömningsgrunder som ska användas vid bedömningen av överensstämmelse. Villkoren för Kommunikationsverkets föreskrifter är de samma som i 29 §. Bestämmelser om de krav som ställs på den nationella noden finns i EU:s förordning (EU) 2015/1501 om interoperabilitetsramverket för elektronisk identifiering Enligt artikel 10 i förordningen ska den nationella noden uppfylla kraven för standarden ISO/IEC 27001 genom certifiering, eller genom en likvärdig bedömningsmetod, eller genom att följa nationell lagstiftning. Dessutom innerhåller artiklarna 5–9 krav som gäller bland annat dataskyddet, interoperabiliteten och informationssäkerheten.

31 §. *Inspektionsberättelse*. Enligt den föreslagna paragrafen ska leverantören av identifieringstjänster för identifieringstjänsten låta det bedömningsorgan som utfört bedömningen utarbeta en inspektionsberättelse över bedömningen av överensstämmelse i enlighet med 29 §. Också Befolkningsregistercentralen ska låta utarbeta en inspektionsberättelse över bedömningen av överensstämmelse i fråga om den nationella noden för elektronisk identifiering. Inspektionsberättelserna ska lämnas till Kommunikationsverket. Inspektionsberättelsen är i kraft den tid som anges i standarden som användes vid bedömningen, dock högst i 2 år.

32 § *Fastställande av överensstämmelse hos betrodda tjänster*. I paragrafen föreskrivs det om kvalificerade tillhandahållare av betrodda tjänster som definieras i eIDAS-förordningen och om bedömningen av deras tjänster. Enligt förslaget ska det bedömningsorgan för överensstämmelse som avses i 28 § 1 mom. bedöma överensstämmelsen hos en kvalificerad betrodd tjänst i enlighet med artikel 20 i EU:s förordning om elektronisk identifiering.

I det föreslagna 2 mom. föreskrivs det om de grunder som ska tillämpas vid bedömningen. Bestämmelser om kraven på betrodda tjänster finns i eIDAS-förordningen. Dessutom ska Kommunikationsverket i kraft av 42 § kunna bestämma att man som bedömningsgrunder kan använda bestämmelser eller riktlinjer som utfärdats av EU eller ett annat internationellt organ, publicerade och generellt eller regionalt tillämpade anvisningar för informationssäkerhet samt datasäkerhetsstandarder eller förfaranden som används allmänt. En föreskrift av Kommunikationsverkets kan behövas för att göra bedömningskriterierna klarare till exempel om EU-kommissionen inte meddelar tillämpliga genomförandeakter, vilket den är behörig att göra enligt artikel 20 i eIDAS-förordningen. I regel utarbetas och fastställs standarderna i anknytning till bedömningskriterierna annars i samband med arbetet med utarbeta standarder för betrodda tjänster, vilket stöds av EU. Enligt den föreslagna 42 § ska Kommunikationsverket kunna meddela närmare föreskrifter om de grunder för bedömningen som avses i 2 mom. Kommunikationsverkets behörighet att meddela föreskrifter begränsas av beskrivningen av möjliga källor till bedömningsgrunder i 2 mom.

33 §. *Allmänna krav för bedömningsorgan*. Bestämmelser om behörighetsvillkoren för bedömningsorgan finns i 1 mom. Enligt den föreslagna 1 punkten ska ett bedömningsorgan enligt 28 § vara funktionellt och ekonomiskt oberoende av dem som bedömningen gäller. Om bedömningsorganet ingår i den organisation som tillhandahåller tjänsten vars överensstämmelse organet bedömer, det vill säga om organet fungerar som internt bedömningsorgan enligt 28 § 3 punkten, ska det kunna identifieras som en separat enhet i organisationen, och dess funktioner måste klart kunna särskiljas från den övriga organisationen. Dessutom ska organets personal ha god teknisk och yrkesinriktad utbildning samt tillräckligt omfattande erfarenhet av de uppgifter som ingår i verksamheten. Organet ska därtill förfoga över den utrustning och de lokaler, hjälpmedel och system som behövs för bedömningsverksamheten, och det ska ha ändamålsenliga riktlinjer för verksamheten och uppföljningen av den. Enligt 42 § 2 mom. 6 punkten kan Kommunikationsverket vid behov meddela närmare föreskrifter om behörigheten för de bedömningsorgan som föreskrivs i 1 mom.

Enligt det föreslagna 2 mom. måste ett organ för bedömning av överensstämmelse som avses i 28 § 1 punkten visa att kraven i 1 mom. 1–3 punkten är uppfyllda genom en ackreditering beviljad av den nationella ackrediteringsenheten i enlighet med förordning (EG) nr 765/2008 och lagen om konstaterande av tillförlitligheten hos tjänster för bedömning av överensstämmelse med kraven (920/2005). I Finland den nationella ackrediteringsenheten FINAS. Det är alltså FINAS som enligt förslaget ska ackreditera de bedömningsorgan som avses i 1 mom. 1–3 punkten. FINAS utför bedömningen enligt fastställda kriterier, och ger ett utlåtande om organets kompetens, vilket myndigheten tar som underlag för sitt beslut om godkännande.

Enligt 3 mom. ska kompetensen hos de bedömningsorgan som avses i 28 § 2 och 3 mom. (dvs. övriga bedömningsorgan och interna bedömningsorgan) påvisas i den anmälan till Kommunikationsverket som föreskrivs i 10 §. Att kraven i 1 mom. 1–3 punkten är uppfyllda kan visas genom en ackreditering enligt 2 mom. eller genom ett annat, oberoende förfarande som grundar sig på en allmänt använd standard. I lagen om konstaterande av tillförlitligheten hos tjänster för bedömning av överensstämmelse med kraven (6 § 3 mom.) föreskrivs det om sådan bedömning av kompetens som är jämförbar med ackreditering. Förutom en bedömning av kompetens som är jämförbar med ackreditering, kan det också bli fråga om något annat oberoende förfarande som används allmänt och är erkänt.

En ackreditering som beviljas av en utländsk ackrediteringsenhet motsvarar det ackrediteringsbeslut som avses i 3 och 4 mom.

34 §. *Godkännande av organ för bedömning av överensstämmelse.* Enligt det föreslagna 1 mom. godkänner Kommunikationsverket de organ för bedömning av överensstämmelse som avses i 28 § 1 mom. efter ackrediteringen. Bestämmelser om villkoren för godkännandet finns i 33 §. Enligt 2 mom. kan ett bedömningsorgan godkännas för viss tid, om det finns särskilda skäl till detta. Kommunikationsverket kan i ett beslut om godkännande ange nödvändiga begränsningar och villkor rörande bedömningsorganets behörighetsområde, tillsynen över organet och organets verksamhet.

Övriga i 28 § avsedda bedömningsorgan behöver inte godkännas eller ackrediteras på samma sätt som sådana organ för bedömning av överensstämmelse som avses i 28 § 1 mom. Deras oberoende och kompetens måste likväl utredas. En leverantör av identifieringstjänster och ett organ för bedömning av överensstämmelse ska dock i den anmälan som föreskrivs i 10 § för Kommunikationsverket lägga fram en utredning om att det andra utomstående bedömningsorgan eller interna kontrollorgan som avses i 28 § 2 och 3 mom. uppfyller kraven i enlighet med 33 §.

Ett bedömningsorgan får ansöka om ackreditering hos Säkerhets- och kemikalieverkets ackrediteringstjänst FINAS. I lagen föreslås det likväl inga bestämmelser om det förfarande som tillämpas när kompetensen och oberoendet hos ett organ för bedömning av identifieringstjänster verifieras. För en leverantör av identifieringstjänster är det viktigt att redan innan den lämnar en anmälning om inledning eller ändring av verksamhet enligt 10 §, kunna försäkra sig om att det bedömningsorgan som leverantören anlitar uppfyller kraven i den föreslagna 33 §.

Bedömningen av bedömningsorganets kompetens kan göras på organets eget initiativ eller också kan leverantören av identifieringstjänster ta initiativ till den. Det är motiverat att i lagen inte kräva att bedömningsorganet lämnar en ansökan, eftersom det gör det möjligt att också anlita sådana internationella bedömningsorgan som inte har ett tillräckligt kommersiellt intresse för att ansöka om särskilt godkännande i Finland. Eftersom det inte föreslås bestämmelser om förfarandet, ska bedömningsorganens kompetens avgöras inom ramen för Kommunikationsverkets tillsyn över efterlevnaden av lagen samt de allmänna förvaltningsförfarandena. Bedömningsorganet eller leverantören av identifieringstjänster får be Kommunikationsverket om råd i ärendet, men det avgörs i regel först när en utredning om organets kompetens lämnas myndigheten i samband med att leverantören av identifieringstjänster anmäler att verksamheten inleds eller att en förändring i den har skett.

Ur leverantörernas synvinkel ökas förutsägbarheten emellertid av att Kommunikationsverket enligt 42 § får precisera kompetenskraven för bedömningsorgan genom föreskrifter. Vid Kommunikationsverket bereds sådana föreskrifter i regel av arbetsgrupper tillsammans med representanter för branschen, varvid aktörernas synpunkter blir beaktade och aktörerna får information om kraven.

35 §. *Ansökan om att bli organ för bedömning av överensstämmelse.* Kommunikationsverket godkänner organ för bedömning av överensstämmelse på ansökan. Till ansökan fogas Säkerhets- och kemikalieverkets ackrediteringsenhets (ackrediteringstjänsten FINAS) ackrediteringsbeslut, eller, om ett sådant saknas, en motsvarande utredning gjord av ackrediteringstjänsten FINAS om att villkoren för godkännande i 33 § 1 mom. 1–3 punkten är uppfyllda. Ansökan ska dessutom innehålla övriga uppgifter om organets verksamhet som behövs för en bedömning av om villkoren i 33 § är uppfyllda.

Kommunikationsverket godkänner ett organ för bedömning av överensstämmelse om det uppfyller villkoren i 33 §, vilket avgörs utifrån utredningar som verket har mottagit och ackrediteringsenhetens beslut samt vid behov inspektioner som verket utfört. När Kommunikationsverket behandlar en ansökan får verket begära utlåtanden samt anlita utomstående experter för att bedöma ansökan och de uppgifter som ges i ansökan.

Kommunikationsverket får vid behov med stöd av 42 § meddela föreskrifter om de uppgifter som ska anges i ansökan och hur de ska skickas till verket.

36 §. *Certifiering av en anordning för skapande av kvalificerade elektroniska underskrifter eller kvalificerade elektroniska stämplar.* Enligt det föreslagna 1 mom. är det Kommunikationsverket som avgör vilka offentliga eller privata certifieringsorgan enligt artiklarna 30 och 39 i EU:s förordning om elektronisk identifiering som får certifiera anordningar för skapande av kvalificerade elektroniska underskrifter eller kvalificerade elektroniska stämplar. Certifiering är påvisande av överensstämmelse genom ett intyg (certifikat) eller märke.

Enligt artiklarna 30 och 39 i eIDAS-förordningen är certifieringen av anordningar för skapande av kvalificerade elektroniska underskrifter och kvalificerade elektroniska stämplar obligatorisk. En medlemsstat måste underrätta kommissionen om de organ som får utföra certifieringen. I den gällande 29 § i autentiseringslagen föreskrivs om motsvarande av Kommunikat-

ionsverket utsedda kontrollorgan med uppgift att bedöma om anordningar för signaturframställning uppfyller kraven i lagen. Några sådana kontrollorgan har dock inte utsetts i Finland.

Anordningarna kan vara fysiska, såsom elektroniska chip, eller bestå av en kombination av program och servrar. Vid certifieringen av egentliga anordningar är situationen förmodligen den samma som för närvarande, det vill säga chip tillverkas utanför Finland och tillverkaren ser till att de blir certifierade i etableringslandet. Certifieringar har sökts allmänt även hittills, fastän lagstiftningen inte har förutsatt detta.

Enligt den föreslagna 42 § får Kommunikationsverket vid behov meddela preciserande föreskrifter om de krav som ställs på certifieringsorgan, förfarandet vid certifiering och kraven på anordningar för skapande av underskrifter eller stämplar med beaktande av vad som bestäms i eIDAS-förordningen och kommissionens genomförandebeslut rörande förordningen.

Kraven såväl på anordningarna för skapande som på certifieringen anges i regel i eIDAS-förordningen och då behöver och får nationella krav inte föreskrivas. Kommissionen får med stöd av artikel 30.2 i eIDAS-förordningen fastställa standarder för säkerhetsutvärdering av informationsteknikprodukter och enligt artikel 30.3 ange särskilda krav på certifikatutfärdare.

Kommissioner bereder en genomförandeakt för de standarder som nämns ovan. Någon lagstiftning som kompletterar kraven på en certifieringsorganisation är däremot inte under beredning. De standarder för informationssäkerheten som ska fastställas täcker ännu inte heller tjänster av ny typ. Till dessa delar kan det därför vara nödvändigt att komplettera förordningen med nationell lagstiftning. Behovet av precisering kan gälla förfarandet som tillämpas vid bedömning, säkerhetsegenskaperna hos anordningar för skapande av underskrifter (s.k. skyddsprofiler) eller andra motsvarande frågor.

37 §. *Allmänna skyldigheter för certifieringsorgan och organ för bedömning av överensstämmelse*. Ett organ för bedömning av överensstämmelse som avses i 28 § 1 mom. och ett certifieringsorgan som avses i 36 § ska utföra sina uppgifter i enlighet med eIDAS-förordningen och denna lag. Kommissionen kan också med stöd av eIDAS-förordningen utfärda genomförandebestämmelser där verksamheten för organ för bedömning av överensstämmelser och certifieringsorgan regleras.

Enligt det föreslagna 2 mom. får organ för bedömning av överensstämmelse och certifieringsorgan när de utför sina uppgifter anlita personer som inte hör till organisationen. Organen ansvarar också för det arbete som dessa utför.

Enligt det föreslagna 3 mom. ska organ för bedömning av överensstämmelse och certifieringsorgan när de utför offentliga förvaltningsuppgifter iaktta de allmänna förvaltningslagar som räknas upp i paragrafen. På bedömningsorganets och certifieringsorganets personal tillämpas bestämmelserna om straffrättsligt tjänsteansvar. Bestämmelser om skadeståndsansvar finns i skadeståndslagen (412/1974).

38 §. *Återkallande av godkännande som organ för bedömning av överensstämmelse eller utseende till certifieringsorgan.* I paragrafen föreslås bestämmelser om situationer när ett organ för bedömning av överensstämmelse eller ett certifieringsorgan inte längre uppfyller de villkor som ställs på organet. Om organen inte längre uppfyller de villkor som särskilt ställs på organet i lag eller inte iakttar villkoren i beslutet om godkännande eller utseende eller annars i väsentlig grad handlar i strid med gällande bestämmelser, ska Kommunikationsverket fastställa en tillräcklig frist för att ställa saken till rätta. Kommunikationsverket ska återkalla sitt beslut om organet inte har korrigerat sin verksamhet inom den fastställda fristen.

IV a kap. **Betrodda tjänster**

Enligt förslaget ska lagen kompletteras med ett nytt 4 a kapitel som ska innehålla bestämmelser om elektroniska underskrifter motsvarande dem som finns i gällande lag. Motsvarande bestämmelser finns inte i eIDAS-förordningen.

39 §. *Återkallande av certifikat*. Till sitt sakinnehåll ska den föreslagna paragrafen motsvara 36 § 1 och 2 mom. i gällande lag, men bestämmelsen ska tillämpas också på innehavare av elektronisk stämpel. Bestämmelsen gäller den skyldighet som innehavaren av ett kvalificerat certifikat och elektronisk stämpel har enligt eIDAS-förordningen att begära att certifikatet återkallas, om innehavaren har grundad anledning att misstänka att framställningsdata för en underteckning eller stämpel kan användas obehörigen. Certifikatutfärdaren ska enligt 2 mom. utan dröjsmål återkalla ett kvalificerat certifikat om undertecknaren eller innehavaren av stämpeln begär det. Begäran om återkallande av ett kvalificerat certifikat anses ha kommit in till certifikatutfärdaren då den har stått till utfärdarens förfogande så att den har kunnat behandlas. När det gäller ett meddelande som har skickats i elektronisk form innebär detta tidpunkten då begäran stått till certifikatutfärdarens förfogande i mottagningsanordningen eller informationssystemet.

40 §. *Ansvar för obehörig användning av framställningsdata för en underteckning eller elektronisk stämpel*. Det föreslås att paragrafen ändras på grund av terminologin i eIDAS-förordningen en ändrad laghänvisning. I 1 mom. talas det om kvalificerade certifikat för elektroniska underskrifter (artikel 28 i eIDAS-förordningen) och kvalificerade certifikat för elektroniska stämplar (artikel 38 i eIDAS-förordningen). I paragrafen finns en hänvisning till 39 § 2 mom. i den föreslagna lagen. I 2 mom. 3 punkten finns en hänvisning till begäran om återkallande enligt 39 § 1 mom.

41 §. *Det ansvar som vilar på tillhandahållare av betrodda tjänster*. Det föreslås att paragrafen ändras på grund av artikel 13 i eIDAS-förordningen som innehåller bestämmelser om det skadeståndsansvar som åligger tillhandahållare av betrodda tjänster. Enligt artikel 13.3 ska det skadeståndsansvar som anges i förordningen tillämpas i enlighet med nationella bestämmelser om skadeståndsansvar. Enligt skäl 37 i ingressen innebär detta till exempel att skada, avsikt och oaktsamhet definieras och relevanta tillämpliga procedurregler fastställs enligt nationella bestämmelser.

I den mån tillhandahållarens ansvar grundar sig på artikel 13 i eIDAS-förordningen ska nationell rätt tillämpas på bestämmelserna om bland annat jämkning av skadestånd, den skadelidandes medverkan, solidariskt ansvar när fler än en är ansvariga för en skada samt preskription av skadeståndsyrkanden tillämpas.

Den gällande 41 § kan tillämpas bara på kvalificerade certifikat enligt EU-lagstiftningen. Artikel 13 i eIDAS-förordningen har ett större tillämpningsområde som omfattar alla betrodda tjänster enligt eIDAS-förordningen.

Den föreslagna bestämmelsen i 2 mom. motsvarar bestämmelserna i 41 § 1 mom. 5 punkten och 2 mom. i den gällande lagen och gäller situationer när certifikatutfärdaren eller en person som denne anlitat inte har återkallat ett kvalificerat certifikat på det sätt som anges i den föreslagna 39 §.

42 §. *Allmän styrning och Kommunikationsverkets föreskrifter*. I propositionen föreslås det att rubriken för 42 § ändras så att den omfattar den allmänna styrningen rörande elektronisk identifiering samt mera detaljerad styrning genom föreskrifter av Kommunikationsverket. Enligt

det föreslagna 1 mom. ska Kommunikationsministeriet svara för den allmänna styrningen och utvecklingen av stark autentisering och betrodda tjänster.

Det föreslagna 2 mom. innehåller en förteckning över de frågor om vilka Kommunikationsverket får meddela närmare föreskrifter. I jämförelse med gällande lag har bemyndigandena att meddela föreskrifter i den föreslagna lagen samlats i en paragraf, och de har getts en precisare avgränsning. Kommunikationsverket ska inte framöver ha en sådan generellare behörighet att meddela föreskrifter än den som anges i 42 § 2 mom. Enligt den föreslagna 1 punkten får verket meddela föreskrifter om säkerheten och tillförlitligheten hos ett identifieringssystem som avses i 8 § 1 mom. 4 och 5 punkten. Det föreslagna bemyndigandet motsvarar bemyndigandet enligt 42 § 2 mom. i gällande lag, men noggrannare definierat så att det bara gäller 4 och 5 punkten i det föreslagna 1 mom. Det gäller föreskrifter som är nödvändiga för tillsynen.

Enligt den föreslagna 2 punkten får verket meddela föreskrifter om det närmare innehållet i de uppgifter som ska anmälas enligt 10 § och om hur de ska lämnas till Kommunikationsverket, när föreskrifterna är nödvändiga för tillsynen. Bemyndigandet motsvarar 10 § 3 mom. i gällande lag.

Enligt den föreslagna 3 punkten får verket meddela närmare föreskrifter om de egenskaper hos förtroendenätets gränssnitt som avses i 12 a § 2 mom. Kommunikationsverket ska till exempel med stöd av en teknisk föreskrift och i samarbete med branschorganisationer kunna utarbeta nationella profiler på en ändamålsenlig precisionsnivå utgående från standarderna OpenID Connect och SAML. De nationellt definierade gränssnitten ska enligt den information som nu finns tillgänglig vara högst tre till antalet.

Enligt det föreslagna 4 punkten kan Kommunikationsverket meddela vid behov närmare föreskrifter om vad som ska ingå i en anmälan enligt 16 § 1 mom., vilken form anmälan ska ha och när och hur den ska lämnas. Detta gäller skyldigheten för leverantören av identifieringstjänster att anmäla hot och störningar som riktas mot verksamheten eller skyddet av uppgifter. Kommunikationsverket utreder de tekniska möjligheterna för en praxis där Kommunikationsverket förmedlar anmälningar från leverantörer av identifieringstjänster i förtroendenätet för elektronisk identifiering.

Enligt den föreslagna 5 punkten får verket meddela föreskrifter om de grunder för bedömningen av överensstämmelsen hos en identifieringstjänst, en betrodd tjänst eller den nationella noden som avses i 29, 30 och 32 §. Innehållet i föreskrifterna och begränsningarna i tillämpningen behandlas i motiveringarna till paragraferna i fråga.

Enligt den föreslagna 6 punkten kan Kommunikationsverket vid meddela behov närmare föreskrifter om de behörighetsvillkoren för organ för bedömning av överensstämmelse som avses i 33 § med beaktande av det som föreskrivs i eIDAS-förordningen och kommissionens genomförandebestämmelser rörande den förordningen. Kommissionen kan exempelvis genom genomförandebestämmelser fastställa att vissa standarder ska iakttas vid ackreditering av organ för bedömning av överensstämmelse. Det är emellertid fortfarande oklart om kommissionen kommer att utfärda sådana genomförandebestämmelser. I det fallet att sådana inte utfärdas måste nationella föreskrifter utfärdas i saken.

Enligt den föreslagna 7 punkten kan Kommunikationsverket vid behov meddela föreskrifter om vilka uppgifter som ska ingå i en sådan ansökan om att bli organ för bedömning av överensstämmelse som avses i 35 §.

Enligt den föreslagna 8 punkten får verket vid behov meddela preciserande föreskrifter om krav som ställs på de certifieringsorgan som avses i 36 §, förfarandet vid certifiering och kra-

ven på kraven på anordningar för skapande av underskrifter eller stämplar med beaktande av vad som bestäms i eIDAS-förordningen och kommissionens genomförandebeslut rörande förordningen.

42 a §. *Kommunikationsverkets uppgifter*. Enligt förslaget ska en ny 42 a § fogas till lagen. Paragrafens 1 mom. omfattar Kommunikationsverkets nuvarande uppgift att se till att lagen om stark autentisering och betrodda elektroniska tjänster och de bestämmelser som utfärdats med stöd av den iakttas.

I 2 mom. föreskrivs för Kommunikationsverket nya uppgifter som uppkommer på grund av eIDAS-förordningen. Enligt 1 punkten ska Kommunikationsverket delta i samarbetet mellan EU:s medlemsstater i det interoperabilitetsramverk för elektronisk identifiering som avses i artikel 12 i förordningen och som gemensam kontaktpunkt i det samarbetsnätverk som upprättats enligt kommissionens genomförandebeslut 2015/296. I samarbetsnätverket ska Kommunikationsverket tillsammans med motsvarande myndigheter i övriga medlemsstater delta i sakkunnigbedömningen av de identifieringssystem som ska anmälas till kommissionen.

Enligt den föreslagna 2 punkten ska Kommunikationsverket anmäla finska system för elektronisk identifiering till Europeiska kommissionen i enlighet med artiklarna 7–10 i förordningen.

Enligt den föreslagna 3 punkten ska Kommunikationsverket fungera som tillsynsorgan, det vill säga tillsynsmyndighet, för betrodda tjänster enligt artikel 17 i förordningen och sköta de uppgifter som åligger tillsynsmyndigheten enligt förordningen. Enligt artikel 17 i förordningen ska Kommunikationsverket genom tillsynsverksamhet på förhand och i efterhand utöva tillsyn över kvalificerade tillhandahållare av betrodda tjänster samt genom tillsynsverksamhet i efterhand se till att icke-kvalificerade tillhandahållare av betrodda tjänster uppfyller kraven i förordningen.

Enligt 4 punkten ska Kommunikationsverket i enlighet med artikel 22 i förordningen föra och publicera förteckningar över kvalificerade tillhandahållare av betrodda tjänster i Finland och de kvalificerade betrodda tjänster som de tillhandahåller.

I 2 mom. föreslås en förtydligande bestämmelse om att Kommunikationsverkets beslutanderätt inte omfattar avtalsförhållanden mellan parter eller frågor om ersättningsskyldighet.

42 b §. *Dataombudsmannens uppgifter*. Den föreslagna bestämmelsen motsvarar bestämmelsen i 42 § 3 mom. i autentiseringslagen.

42 c §. *Befolkningsregistercentralens uppgifter*. Befolkningsregistercentralen ska enligt förslaget svara för den nationella nod som definieras i artikel 12.8 i eIDAS-förordningen. Denna nod utgör gränssnittet mellan finska och övriga EU-medlemsstaters identifieringssystem, och den möjliggör gränsöverskridande elektronisk ärendehantering.

Noden deltar i verifieringen av personers identitet över gränserna och kan identifiera och behandla eller överföra uppgifter till andra noder genom att tillhandahålla den nationella infrastrukturen för elektronisk identifiering ett gränssnitt mot övriga medlemsstaters infrastrukturer för elektronisk identifiering. Noden konstrueras med hjälp av PEPS-lösningar (Pan-European Proxy Server) som är specifika för medlemsstaterna.

43 §. *Rätt till information*. Enligt förslaget ska 1 mom. ändras, eftersom det gällande 1 mom. innehåller en hänvisning till paragrafer som ska upphävas enligt denna proposition. Bestämmelsen i det föreslagna 1 mom. om Kommunikationsverkets rätt att få information är till sin ordalydelse allmännare än den nuvarande och motsvarar 315 § i informationssamhällsbalken.

44 §. *Myndighetssamarbete och rätt att lämna information*. Det föreslås att 1 mom. i paragrafen ändras så att Kommunikationsverket och dataskyddsombudsmannen har rätt att lämna Finansinspektionen och Konkurrens- och konsumentverket den information som dessa behöver för att kunna fullgöra sina uppgifter. Uppgifter som berörs av sekretessbestämmelser och andra begränsningar som gäller utlämnande kan behövas i de tillsynsuppgifter som utförs av Konkurrens- och konsumentverket. Syftet med momentet är att minska mängden onödigt arbete vid myndigheterna och dem som tillsynen gäller genom att möjliggöra utbyte av information mellan myndigheter även i fråga om information som ska hållas hemlig.

45 §. *Administrativa tvångsmedel*. Det föreslås att 1 mom. ändras så att Kommunikationsverket kan tillgripa de tvångsmedel som räknas upp i paragrafen även vid tillsynen över efterlevnaden av eIDAS-förordningen och de genomförandeakter som utfärdats med stöd av den. I momentet har dessutom införts rätt för Kommunikationsministeriet att ge en anmärkning till den som bryter mot autentiseringslagen eller EU-lagstiftning i saken. På detta sätt kan Kommunikationsverket snabbare informera aktörerna om fall där bestämmelserna inte har följts, i synnerhet i fråga om kortvarig verksamhet som strider mot bestämmelserna. Den föreslagna ordalydelsen motsvarar 330 § i informationssamhällsbalken.

45 a §. *Interimistiska beslut*. I lagen föreslås en likartad bestämmelse om Kommunikationsverkets interimistiska beslut som i 331 § i informationssamhällsbalken. Tillhandahållandet av identifieringstjänster och betrodda tjänster kan vara förknippat med överträdelser och störningssituationer som innebär att myndigheten behöver fatta beslut om interimistiska åtgärder. Sådana kan exempelvis vara situationer enligt artikel 10 i eIDAS-förordningen, när ett system för elektronisk identifiering som anmälts i enlighet med artikel 9.1 eller den autentisering som avses i artikel 7 f utsätts för intrång eller delvis äventyras på ett sätt som påverkar tillförlitligheten i systemets gränsöverskridande autentisering. I sådana fall ska i enlighet med artikel 10 i eIDAS-förordningen den anmälande medlemsstaten utan dröjsmål tillfälligt upphäva eller återkalla denna gränsöverskridande autentisering eller de berörda utsatta delarna.

Allvarliga dataintrång i rotcertifikat där certifikatutfärdarens enskilda signeringsnyckel hamnar i fel händer och andra motsvarande ovan nämnda allvarliga händelser i anknytning till identifieringstjänster och betrodda tjänster kan också kräva snabba beslut av Kommunikationsverket.

46 §. *Inspektionsrätt*. Det föreslås att paragrafen om Kommunikationsverkets inspektionsrätt ska ändras så att inspektionsrätten också gäller de aktörer som anges i eIDAS-förordningen. I 46 § i gällande lag är en av omständigheterna under vilka Kommunikationsverket ska få förrätta en inspektion att aktören på ett väsentligt sätt har brutit mot lagen eller mot föreskrifter som har utfärdats med stöd av den. Det föreslås att också detta villkor ska ändras. Bestämmelsen i 2 mom. i gällande lag upphävs enligt förslaget, eftersom ett organ för bedömning av överensstämmelse kommer att bedöma aktörerna regelbundet.

I 2–3 mom. föreslås det att den finska termen för certifikatutfärdare som tillhandahåller kvalificerade certifikat ändras så att den överensstämmer med terminologin i eIDAS-förordningen, i övrigt motsvarar de i sak de nuvarande bestämmelserna.

De föreslagna 4 och 5 mom. motsvarar 5 och 6 mom. i den gällande lagen.

47 §. *Avgifter till Kommunikationsverket*. Största delen av momenten i den gällande lagen ändras varför det föreslås att hela paragrafen ändras. Enligt det föreslagna 1 mom. höjs tillsynsavgiften som leverantörer av identifieringstjänster ska betala Kommunikationsverket med 2 000 euro. Därmed är de årliga tillsynsavgifter som Kommunikationsverket debiterar för identifieringstjänster och för de betrodda tjänster som avses i eIDAS-förordningen, som före-

slås i 2 mom., lika höga, det vill säga 14 000 euro. Med denna avgiftsnivå bevaras dessutom Kommunikationsverkets intäkter av avgifterna på nuvarande nivå. Kommunikationsverket tar ut avgifter endast hos tillhandahållare av kvalificerade av betrodda tjänster.

Enligt det föreslagna 2 mom. ska en tillhandahållare av betrodda tjänster och en tillhandahållare av kvalificerade betrodda tjänster ska alltså för varje betrodd tjänst som Kommunikationsverket godkänt betala Kommunikationsverket en registreringsavgift på 5 000 euro samt årligen en tillsynsavgift på 14 000 euro för den första betrodda tjänst som de tillhandahåller och en årlig tillsynsavgift på 9 000 euro för de därpå följande kvalificerade betrodda tjänster som de tillhandahåller. Kommunikationsverkets årliga tillsyn av betrodda tjänster består dels av tillsyn av tjänsteleverantören och dels av tillsyn av den godkända betrodda tjänsten. Eftersom samma tjänsteleverantör övervakas för flera olika godkända tjänster är det motiverat att ta ut en mindre årlig tillsynsavgift när tjänsteleverantören tillhandahåller fler godkända betrodda tjänster.

Enligt de föreslagna 3 och 4 mom. ska ett godkänt organ för bedömning av överensstämmelse och ett certifieringsorgan betala Kommunikationsverket en utnämningsavgift på 10 000 euro och en årlig tillsynsavgift på 15 000 euro. Avgifterna motsvarar de avgifter som enligt 29 § i den gällande lagen tas ut hos kontrollorgan som utsetts av Kommunikationsverket och som bedömer om anordningarna för signaturframställning uppfyller kraven. För närvarande finns inget sådant utsett organ, men det motsvarar det certifieringsorgan som nu föreslås i 36 §.

I det föreslagna 5 mom. konstateras att Kommunikationsverkets tillsynsverksamhet finansieras med avgifterna. Avgifterna räcker dock inte till för att täcka kostnaderna för Kommunikationsverkets tillsynsverksamhet i och med den ökade arbetsmängden, varför Kommunikationsverket måste omfördela sina resurser för annan verksamhet. På samma sätt som i den gällande lagen ska tillsynsavgiften betalas till fullt belopp också under det första verksamhetsåret, även om verksamheten inleds under året. Tillsynsavgifter återbetalas inte även om tjänsteleverantören upphör med sin verksamhet under året.

Det föreslagna 6 mom. motsvarar 5 mom. i den gällande lagen, förutom att då det i bestämmelsen om sökande av ändring hänvisas till 49 § 1 mom. ändras denna också på samma sätt. Med stöd av det föreslagna 49 § 1 mom. begärs omprövning av ett beslut av Kommunikationsverket som gäller en avgift som ska betalas till Kommunikationsverket enligt 47 § i första hand hos Kommunikationsverket.

Det föreslagna 7 mom. motsvarar nuvarande 6 mom. I det föreslagna 8 mom., som gäller kostnader för Kommunikationsverkets inspektioner som tas ut hos leverantören eller tillhandahållaren, infogas som en ny aktör också tillhandahållare av betrodda tjänster.

49 §. *Sökande av ändring i myndighetsbeslut*. Lagens 49 § föreslås bli ändrad och uppdaterad så att bestämmelserna om sökande av ändring ändras jämfört med nuläget så att besvärstillståndssystemet mer omfattande tas i bruk i ändringssökandet. Enligt 1 mom. tas rättelseyrkande i bruk för de av Kommunikationsverkets beslut som gäller avgifter som ska betalas till Kommunikationsverket.

Enligt 2 mom. får Kommunikationsverkets omprövningsbeslut samt andra beslut av Kommunikationsverket överklagas genom besvär hos förvaltningsdomstolen på det sätt som föreskrivs i förvaltningsprocesslagen.

I 3 mom. föreskrivs att förvaltningsdomstolens beslut i ett ärende som gäller återkallande av ett beslut om att godkänna av ett bedömningsorgan eller utse ett certifieringsorgan får överklagas genom besvär på det sätt som anges i förvaltningsprocesslagen. Detta innebär att det

för sådana ärenden av tvångsmedels- och påföljdsnatur inte krävs besvärstillstånd till högsta förvaltningsdomstolen. Andra beslut av förvaltningsdomstolen får överklagas genom besvär endast om högsta förvaltningsdomstolen beviljar besvärstillstånd.

De föreslagna 4 och 5 mom. motsvarar 49 § 2 och 3 mom. i den gällande lagen.

49 a §. *Sökande av ändring i beslut av organ för bedömning av överensstämmelse och certifieringsorgan*. I paragrafen föreskrivs som omprövning av ett beslut som gäller en rapport för överensstämmelsebedömning och som fattats av ett organ för bedömning av överensstämmelse och om beslut som gäller certifiering av anordningar för elektronisk underskrift eller anordningar för skapande av elektroniska stämplar och som fattats av ett certifieringsorgan. Till de delar som organ för bedömning av överensstämmelser och certifieringsorgan utför sådan bedömning av överensstämmelser eller certifiering som grundar sig på lag, är detta en offentlig förvaltningsuppgift i enligt med 124 § i grundlagen. Vidare enligt 124 § i grundlagen ska kraven på rättssäkerhet tryggas när privaträttsliga rättssubjekt sköter offentliga förvaltningsuppgifter. Därmed ska det vara möjligt att söka ändring i beslut av de ovan nämnda aktörerna till de delar som det gäller förvaltningsbeslut.

Enligt förslaget hänvisas det i bestämmelsen om omprövningsbegäran i 1 mom. till förvaltningslagen. Allmänna bestämmelser om förfarandet vid omprövning finns i 7 a kap. i förvaltningslagen. Det föreslås att det i momentet föreskrivs att omprövning av ett beslut som fattats av ett organ för bedömning av överensstämmelse eller ett certifieringsorgan får begäras hos Kommunikationsverket på det sätt som anges i förvaltningslagen.

Enligt 2 mom. får omprövningsbeslut överklagas genom besvär hos förvaltningsdomstolen i enlighet med förvaltningsprocesslagen. Beslut av förvaltningsdomstolen får överklagas bara om högsta förvaltningsdomstolen beviljar besvärsrätt.

Övergångsbestämmelser

I 1 mom. föreslås en ikraftträdandebestämmelse.

Enligt 2 mom. får en leverantör av identifieringsverktyg till och med den 31 december 2018 som ett i 17 § 2 mom. i denna lag avsett godkänt dokument också använda ett giltigt körkort som har beviljats efter den 1 oktober 1990 av en medlemsstat i Europeiska ekonomiska samarbetsområdet. En inledande identifiering som gjorts med stöd av körkort senast den 31 december 2018 uppfyller kraven i den föreslagna lagen och den inledande identifieringen behöver inte ytterligare säkerställas på något annat sätt.

Enligt det föreslagna 3 mom. fortsätter de föreskrifter av Kommunikationsverket som är i kraft vid ikraftträdandet av lagen att gälla. Efter lagens ikraftträdande meddelar Kommunikationsverket nya föreskrifter med stöd av 42 §.

I 4–8 mom. finns övergångsbestämmelser i anknytning till att det enligt den föreslagna lagen ska ställas åtminstone samma krav på informationssäkerhet och tillförlitlighet i fråga om system för tillhandahållande av stark autentisering som det ställs på tillitsnivån väsentlig i EU:s lagstiftning i fråga om system för gränsöverskridande elektronisk identifiering. Av denna orsak ska aktörerna kunna bestämma om de vill fortsätta att tillhandahålla tjänster för stark autentisering efter att lagändringarna har trätt i kraft.

Enligt 4 mom. ska en leverantör av identifieringstjänster som är införd i det register som föreskrivs i 12 § i autentiseringslagen senast två månader från ikraftträdandet av den föreslagna lagen lämna Kommunikationsverket en ändringsanmälan enligt 10 § 3 mom., om leverantören

vill fortsätta sin verksamhet som leverantör av identifieringstjänster för stark autentisering. Den inspektionsberättelse som avses i 4 kap., uppgifter om det bedömningsorgan som leverantören av identifieringstjänster anlitar samt övriga uppgifter som krävs enligt 10 § ska lämnas in till Kommunikationsverket senast den 31 januari 2017. En leverantör av identifieringstjänster ska i fråga om de tjänster som tillhandahålls anmäla bland annat på vilken tillitsnivå enligt förordningen om tillitsnivåer vid elektronisk identifiering som identifieringstjänsterna tillhandahålls.

Enligt 5 mom. ska Kommunikationsverket behandla en ändringsanmälan enligt 3 mom. från en leverantör av identifieringstjänster och göra de anteckningar som anmälan föranleder i det register som avses i 12 § senast tre månader efter att ha mottagit ändringsanmälan och övriga uppgifter enligt 10 § i autentiseringslagen.

Första bestämmelsen i 6 mom. gäller identifieringsverktyg som har beviljats före ikraftträdandet av den föreslagna lagen. I momentet finns en allmän bestämmelse om att ett identifieringsverktyg för stark autentisering som har beviljats med stöd av de bestämmelser som gällde vid ikraftträdandet lagen fortfarande ska betraktas som ett identifieringsverktyg för stark autentisering åtminstone på tillitsnivån väsentlig i enlighet med definitionen i EU:s förordning om elektronisk identifiering under två månader efter ikraftträdandet av denna lag. Fortsättningen är beroende av om den leverantör av identifieringstjänster som beviljat verktyget anmäler sin avsikt till Kommunikationsverket att fortsätta som leverantör av identifieringstjänster för stark autentisering.

Vidare föreskrivs i 6 mom. att om leverantören av identifieringstjänster inom två månader efter lagens ikraftträdande lämnar en ändringsanmälan om sin avsikt att fortsätta som leverantör av identifieringstjänster för stark autentisering, anses ett identifieringsverktyg som leverantören av identifieringstjänster beviljat med stöd av den tidigare lagen som ett identifieringsverktyg för stark autentisering för åtminstone tillitsnivån väsentlig tills Kommunikationsverket har gjort en anteckning om leverantören av identifieringstjänster i det register som avses i 12 § och något annat inte följer av 7 mom. Utifrån den ändringsanmälan som avses i 3 mom. antecknar Kommunikationsverket i det register som avses i 12 § huruvida leverantören av identifieringstjänster tillhandahåller tjänster på tillitsnivån väsentlig eller hög enligt definitionen i eIDAS-förordningen. Kommunikationsverket kan anteckna tjänsteleverantörens identifieringssystem som ett identifieringssystem på tillitsnivån väsentlig, om systemet uppfyller de krav som i EU-lagstiftningen ställs på identifieringssystem på tillitsnivån väsentlig.

I 7 mom. föreskrivs om situationer när ett identifieringsverktyg efter lagens ikraftträdande beviljas på grundval av ett annat verktyg för stark autentisering, dvs. ett redan befintligt verktyg för stark autentisering används vid den inledande identifieringen. Under övergångsperioden måste man försäkra sig om att det vid den inledande identifieringen för ett starkt verktyg för autentisering inte används sådana identifieringsverktyg som inte längre är identifieringsverktyg för stark autentisering på grund av att tjänsteleverantören av verktyget inte har anmält sin avsikt att fortsätta som leverantör av identifieringstjänster för stark autentisering.

Enligt bestämmelsen betraktas ett elektroniskt identifieringsverktyg som ett identifieringsverktyg för stark autentisering för åtminstone tillitsnivån väsentlig när identifieringsverktyget har beviljats senast inom två månader efter lagens ikraftträdande utifrån en inledande identifiering med ett sådant elektroniskt identifieringsverktyg som avses i 17 §. I bestämmelsen utgår man från att leverantörer av identifieringstjänster när lagen träder i kraft kan fortsätta att på elektronisk väg bevilja nya identifieringsverktyg på det sätt som föreskrivs vid lagens ikraftträdande. När två månader har förflutit från lagens ikraftträdande får ett nytt identifieringsverktyg beviljas elektroniskt endast på grundval av ett sådant annat identifieringsverktyg som

har beviljats av en leverantör av identifieringsverktyg som har gjort en i 3 mom. avsedd anmälan om sin avsikt att fortsätta som leverantör av identifieringstjänster för stark autentisering.

Enlig 8 mom. betraktas ett elektroniskt identifieringsverktyg inte längre som ett identifieringsverktyg för stark autentisering, om leverantören av identifieringstjänster inte har lämnat en ändringsanmälan enligt 3 mom. inom två månader från det att lagen trädde i kraft. Kommunikationsverket ska då avföra leverantören av identifieringstjänster ur det register som avses i 12 § och underrätta leverantören om detta.

1.2 Lag om ändring av lagen om elektronisk kommunikation i myndigheternas verksamhet

3 §. *Annan lagstiftning*. Det föreslås att paragrafen ändras så att den inte längre innehåller en informativ hänvisning till lagen om stark autentisering och elektroniska signaturer. Det nuvarande 1 mom. ska som sådant utgöra 3 § i lagen.

9 §. *Krav på skriftlig form*. Det föreslås att paragrafen ändras så att hänvisningen 1 mom. till en sådan elektronisk signatur som avses i 5 § 2 mom. i lagen om stark autentisering och elektroniska signaturer tas bort. I övrigt ska paragrafen motsvara nuvarande reglering.

I paragrafens 2 mom. föreslås det att ett elektroniskt dokument som kommit in till en myndighet inte behöver kompletteras med en underskrift, om dokumentet innehåller uppgifter om avsändaren och om det inte finns anledning att betvivla dokumentets autenticitet och integritet. Med autenticitet avses i den föreslagna bestämmelsen liksom i nuvarande lag information om avsändaren av dokumentet och med integriteten att dokumentet bevaras oförändrat.

I praktiken har det i enlighet med den nuvarande bestämmelsen blivit regel att det inte krävs att dokument förses med underskrift. Misstankar rörande autenticiteten och integriteten ska ge myndigheten rätt att kräva att dokumentet lämnas antingen i original och försett med behövliga underskrifter eller att dokumentet lämnas på nytt försett med elektronisk underskrift. Underskrift ska alltså betyda såväl fysisk som elektronisk underskrift. Liksom enligt den nuvarande bestämmelsen ska myndigheten även enligt den föreslagna bestämmelsen ha rätt att avgöra hurdana underskrifter den anser tillräckliga för att säkerställa autenticiteten och integriteten hos ett dokument.

16 §. *Elektronisk signering av beslutshandlingar* Det föreslås att paragrafen ändras så att hänvisningen till 5 § 2 mom. i lagen om stark autentisering och elektroniska signaturer tas bort. Dessutom föreslås det att paragrafen ska innehålla en bestämmelse om att en myndighet ska signera en beslutshandling antingen med en avancerad elektronisk underskrift eller annars på ett sådant sätt att man kan säkerställa handlingens autenticitet och integritet.

I bestämmelsen ska det dessutom ställas kvalitativa krav på sättet att underteckna beslutshandlingar. En underteckning med ett tjänstekort som beviljats av Befolkningsregistercentralen ska till exempel uppfylla det kvalitetskrav som nämns i bestämmelsen. En avancerad elektronisk underskrift ska också kunna skapas till exempel med ett mobilcertifikat.

I lagen ska de underskrifter som en myndighet får använda likväl inte begränsas till avancerade elektroniska underskrifter. Även något annat sätt att underteckna ett dokument är tillräckligt förutsatt att det går att säkerställa dess autenticitet och integritet. Med att säkerställa autenticiteten förstås att säkerställa undertecknarens identitet och med att säkerställa integriteten att säkerställa att dokumentet inte har ändrats.

18 §. *Bevislig elektronisk delgivning*. Det föreslås att paragrafen ändras så att hänvisningen till ett identifieringsverktyg eller ett kvalificerat certifikat som avses i lagen om stark autentisering och elektroniska signaturer stryks. Som krav på identifieringstekniken föreskrivs det i den föreslagna paragrafen endast att den ska vara datatekniskt tillförlitlig och bevislig.

Det föreslås dessutom att den finska språkdräkten i 3 mom. justeras. Ändringen är teknisk och inverkar inte på den svenskspråkiga lagtexten. Inga andra ändringar i paragrafen föreslås.

1.3 Lagen om kommunikationsförvaltningen

2 §. *Kommunikationsverkets uppgifter*. Enligt förslaget ska hänvisningen till lagen om stark autentisering och elektroniska signaturer ändras så att den stämmer överens med lagens nya rubrik. Dessutom ska hänvisningarna till lagar som upphävdes när informationssamhällsbalken (917/2014) trädde i kraft ersättas med en hänvisning till informationssamhällsbalken.

1.4 Jordabalken

1 §. *Användning av ärendehanteringssystem och elektronisk identifiering i ett ärendehanteringssystem*. Enligt förslaget ska hänvisningen till lagen om stark autentisering och elektroniska signaturer ändras så att den stämmer överens med lagens nya rubrik. Hänvisningen till kvalificerat verifikat, som det tidigare föreskrevs om i autentiseringslagen, ändras till en hänvisning till kvalificerat certifikat för elektronisk underskrift som det föreskrivs om i artikel 28 i eIDAS-förordningen.

1.5 Lagen om förhindrande och utredning av penningtvätt och av finansiering av terrorism

18 §. *Skärpta krav på kontroll vid identifiering på distans*. Enligt förslaget ska hänvisningen till lagen om stark autentisering och elektroniska signaturer ändras så att den stämmer överens med lagens nya rubrik. Hänvisningen till kvalificerat verifikat, som det tidigare föreskrevs om i autentiseringslagen, ändras till en hänvisning till kvalificerat certifikat för elektronisk underskrift som det föreskrivs om i artikel 28 i eIDAS-förordningen.

1.6 Lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster

I 2 § 2 mom. 2 punkten, 6 § 2 mom., 43 § 2 mom. 2 punkten, 61 § 3 mom., 62 § 1 och 2 mom., 66 § 3 mom., 67 § 1 mom. och 68 § 1 mom. finns det hänvisningar till lagen om stark autentisering och elektroniska signaturer. I de föreslagna paragraferna ändras dessa hänvisningar så att de stämmer överens med lagens nya rubrik eller så att de refererar till EU:s förordning om elektronisk identifiering.

1.7 Lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården

2 §. *Tillämpningsområde*. Enligt förslaget ska hänvisningen till lagen om stark autentisering och elektroniska signaturer ändras så att den stämmer överens med den lagens nya rubrik.

9 §. *Elektronisk signering av handlingar*. Det föreslås att paragrafen ändras så att hänvisningen till lagen om stark autentisering och elektroniska signaturer ersätts med en hänvisning till Europaparlamentets och rådets förordning (EU) nr 910/2014, det vill säga eIDAS-förordningen.

14 §. *Riksomfattande informationssystemtjänster*. Enligt förslaget ska hänvisningen till lagen om stark autentisering och elektroniska signaturer ändras så att den stämmer överens med den lagens nya rubrik.

1.8 Lagen om beskattningsförfarande

93 a §. *Elektronisk kommunikation och signering*. Det föreslås att 2 mom. ändras så att de deklarationer och andra handlingar som får lämnas in till skattemyndigheten på elektronisk väg och som ska signeras ska certifieras med en elektronisk underskrift eller på något annat godtagbart sätt. I paragrafen hänvisas inte längre till avancerad elektronisk signatur.

1.9 Lagen om överlåtelseskatt

56 b §. *Elektronisk kommunikation och signering*. Det föreslås att 2 mom. ändras så att de deklarationer och andra handlingar som får lämnas in till skattemyndigheten på elektronisk väg och som ska signeras ska certifieras med en elektronisk underskrift eller på något annat godtagbart sätt. I paragrafen hänvisas inte längre till avancerad elektronisk signatur.

1.10 Lagen om förskottsuppbörd

6 a §. *Elektronisk kommunikation och signering*. Det föreslås att 2 mom. ändras så att de deklarationer och andra handlingar som får lämnas in till skattemyndigheten på elektronisk väg och som ska signeras ska certifieras med en elektronisk underskrift eller på något annat godtagbart sätt. I paragrafen hänvisas inte längre till avancerad elektronisk signatur.

1.11 Blodtjänstlagen

11 §. *Uppgifter som hänför sig till blodgivare*. Det föreslås att paragrafen ändras så att hänvisningen till lagen om stark autentisering och elektroniska signaturer ersätts med en hänvisning till Europaparlamentets och rådets förordning (EU) nr 910/2014, det vill säga eIDAS-förordningen.

1.12 Mervärdesskattelagen

165 §. Det föreslås att 2 mom. ändras så att de deklarationer och andra handlingar som får lämnas in till skattemyndigheten på elektronisk väg och som ska signeras ska certifieras med en elektronisk underskrift eller på något annat godtagbart sätt. I paragrafen hänvisas inte längre till avancerad elektronisk signatur.

1.13 Skattekontolagen

7 §. *Inlämnande av periodskattedeklaration*. Det föreslås att paragrafens 2 mom. ändras så att en periodskattedeklaration som lämnas in på elektronisk väg ska certifieras med elektronisk signatur eller på något annat godtagbart sätt. I paragrafen hänvisas inte längre till avancerad elektronisk signatur.

1.14 Lagen om informationssystemet för byggnaders certifikat

4 §. *Upprättande och signering av energicertifikat*. Det föreslås att paragrafen ändras så att hänvisningen till lagen om stark autentisering och elektroniska signaturer ersätts med en hänvisning till Europaparlamentets och rådets förordning (EU) nr 910/2014, det vill säga eIDAS-förordningen.

1.15 Punktskattelagen

32 §. *Sätt att lämna in skattedeklaration*. Det föreslås att paragrafens 3 mom. ändras så att den elektroniska periodskattedeklaration som avses i paragrafen ska certifieras med en elektronisk underskrift eller på något annat godtagbart sätt. I paragrafen hänvisas inte längre till avancerad elektronisk signatur.

2 Ikraftträdande

Lagarna avses träda i kraft den 1 juli 2016 när bestämmelserna om betrodda tjänster i eIDAS-förordningen träder i kraft.

3 Förhållande till grundlagen samt lagstiftningsordning

Vissa av de bestämmelser som ingår i propositionen är av betydelse med tanke på grundlagen.

Meddelande av föreskrifter

Enligt 80 § 2 mom. i grundlagen kan andra myndigheter genom lag bemyndigas att utfärda rättsnormer i bestämda frågor, om det med hänsyn till föremålet för regleringen finns särskilda skäl och regleringens betydelse i sak inte kräver att den sker genom lag eller förordning. Tillämpningsområdet för ett sådant bemyndigande ska vara exakt avgränsat. Dessutom följer av grundlagen att de frågor som bemyndigandet gäller måste preciseras exakt i lag.

I lagen ska det finnas en grundläggande bestämmelse om saken, vad man avser att föreskrifterna ska gälla och ett tillräckligt noggrant avgränsat och exakt bemyndigande att meddela föreskrifter. Exempelvis i utlåtande GrUU 10/2014 rd betonas kravet på noggrann avgränsning och exakt definition. I samma utlåtande konstaterar utskottet att det är typiskt för miljölagstiftningen att en betydande del av den detaljerade regleringen ingår i författningar på lägre nivå än lag. Detta beror enligt utskottet i stor utsträckning på att bestämmelserna behöver vara synnerligen detaljerade och av teknisk karaktär. Detta gäller också den föreslagna lagstiftningen om stark autentisering och betrodda elektroniska tjänster.

I lagförslaget ingår flera bemyndiganden för Kommunikationsverket att meddela bestämmelser på lägre nivå. I den föreslagna lagen har samtliga bemyndiganden anknutits till den paragraf där frågan regleras i sak (8, 12 a, 16, 29, 30, 32, 33, 35 och 36 §). I paragrafen för bemyndigande (42 §) i lagförslaget har bemyndigandena för fler olika paragrafer sammanställts. De grundläggande bestämmelserna i den föreslagna lagen binder och begränsar Kommunikationsverkets behörighet.

I den föreslagna lagen föreskrivs om individens rättigheter och skyldigheter samt om frågor som i enlighet med grundlagen annars hör till området för grundlagen. Bemyndigandena är noga avgränsade och exakta. Bemyndigandena i lagförslaget står inte i strid med grundlagen.

Överföring av förvaltningsuppgifter på andra än myndigheter

Lagförslaget ska bedömas med hänsyn till grundlagens 124 §. Enligt 124 § i grundlagen kan offentliga förvaltningsuppgifter anförtros andra än myndigheter endast genom lag eller med stöd av lag, om det behövs för en ändamålsenlig skötsel av uppgifterna och det inte äventyrar de grundläggande fri- och rättigheterna, rättssäkerheten eller andra krav på god förvaltning. Uppgifter som innebär betydande utövning av offentlig makt får dock ges endast myndigheter.

Den certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter eller kvalificerade elektroniska stämplar som avses i 36 § i lagförslaget och som föreskrivs i artikel 30 i eIDAS-förordningen kan anses vara en sådan offentlig förvaltningsuppgift som avses i 124 § i grundlagen. I 36 § föreslås att Kommunikationsverket får utse de offentliga eller privata certifieringsorgan som avses i artikel 30 i eIDAS-förordningen. Med beaktande av innehållet i uppgiften är det inte problematiskt att uppgiften eventuellt anförtros andra än myndigheter. Med tanke på kravet på ändamålsenlighet finns det inga hinder för att utförandet av inspektioner av teknisk natur och beviljandet av certifikat som grundar sig på dem anförtros andra än myndigheter. I utförandet av inspektionsuppgifter ingår inte sådana befogenheter som ska anses innebära betydande utövning av offentlig makt. Inspektionsuppgifter som gäller certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter eller elektroniska stämplar är sådana bedömningsuppgifter av teknisk natur som grundlagsutskottet i olika sammanhang med beaktande av 124 § i grundlagen har ansett att är ändamålsenligt att anförtro andra än myndigheter (t.ex. GrUU 43/2000 rd, GrUU 16/2000 rd och GrUU 180/2000 rd). Kommunikationsverket övervakar certifieringsorganens verksamhet och att villkoren uppfylls för att de ska godkännas med stöd av 45, 45 a och 46 §.

Den fastställande av överensstämmelse hos betrodda tjänster, som avses i 32 § i lagförslaget och som föreskrivs i eIDAS-förordningen, och som gäller kvalificerade tillhandahållare av betrodda tjänster och de kvalificerade betrodda tjänster som de tillhandahåller ska inledningsvis granskas utifrån frågeställningen om detta är en offentlig förvaltningsuppgift. Bestämmelser om denna uppgift finns i artikel 20 i eIDAS-förordningen. Trots att Kommunikationsverket, i enlighet med ordalydelsen i eIDAS-förordningen, efter att det har fått inspektionsberättelsen ännu ska kontrollera överensstämmelsen hos den betrodda tjänsten, har inspektionsberättelsen från organet för bedömning av överensstämmelse en avgörande betydelse vid Kommunikationsverket bedömning. Därmed kan uppgiften anses vara en sådan offentlig förvaltningsuppgift som avses i124 § i grundlagen. Det är inte problematiskt ur grundlagssynpunkt att anförtro uppgiften att bedöma överensstämmelsen hos betrodda tjänster till andra än myndigheter. Med tanke på kravet på ändamålsenlighet finns det inga hinder för att utförandet av inspektioner av teknisk natur anförtros andra än myndigheter. I utförandet av inspektionsuppgifter ingår inte sådana befogenheter som ska anses innebära betydande utövning av offentlig makt. Bedömningen av överensstämmelse hos betrodda tjänster är en bedömningsuppgift som kräver tekniskt specialkunnande och som med beaktande av 124 § i grundlagen kan anses vara ändamålsenlig att anförtro andra än myndigheter.

Eftersom de ovan nämnda organ för bedömning av överensstämmelse som avses i den föreslagna 28 § 1 punkten och det certifieringsorgans om avses i den föreslagna 36 § ska anses utföra en offentlig uppgift, föreslås det i 49 a § att ändring kan sökas hos Kommunikationsverket i de beslut som organen har fattat med stöd av denna lag.

Ställningen för de organ för bedömning av överensstämmelse som avses i 28 § 2 och 3 punkten måste också granskas med avseende på 124 § i grundlagen. De andra utomstående bedömningsorgan och interna kontrollorgan som avses här bedömer verksamheten hos leverantörer av identifieringstjänster på det sätt som avses i 29 § och verksamheten hos den nationella noden på det sätt som avses i 30 §. Dessa aktörers inspektionsberättelser ska leverantören av identifieringstjänster bifoga den anmälan som ska lämnas till Kommunikationsverket i enlighet med 10 §. Inspektionsberättelserna hjälper Kommunikationsverket att bedöma lagligheten i fråga om aktörernas verksamhet och verksamheten hos de organ för bedömning av överensstämmelse som avses i 28 § 2 och 3 punkten kan inte anses vara en offentlig förvaltningsuppgift.

Statliga skatter och avgifter

De föreslagna bestämmelserna i 47 § om avgifter till Kommunikationsverket måste bedömas utifrån bestämmelserna om statliga skatter och avgifter i 81 § i grundlagen. Enligt 81 § 1 mom. i grundlagen bestäms om statsskatt genom lag, som ska innehålla bestämmelser om grunderna för skattskyldigheten och skattens storlek samt om de skattskyldigas rättsskydd. Av en skattelag ska entydigt framgå skattskyldighetens omfattning. Bestämmelserna i lagen ska också vara exakt utformade så att den prövningsrätt som myndigheterna har när det gäller att bestämma skattens storlek är bunden till sin natur.

I 47 § i den gällande lagen föreskrivs om motsvarande avgifter, som nu föreslås bli ändrade. I förarbetena till den gällande lagen (RP 36/2009 rd) har karaktären för de avgifter som med stöd av 47 § ska betalas till Kommunikationsverket bedömts i statsförvaltningsrättsligt hänseende och de har ansetts vara mer av skattenatur än av avgiftsnatur. Av denna orsak har de föreslagna bestämmelserna i 47 § utarbetats så att det av bestämmelserna framgår minst grunderna för skattskyldigheten och skattens storlek, den skattskyldigas rättsskydd och omfattningen av de skattskyldiga på det sätt som krävs enligt 81 § i grundlagen. På samma sätt som i den gällande lagen kan närmare bestämmelser om andra detaljer utfärdas genom förordning av kommunikationsministeriet och ett separat bemyndigande om detta föreslås i 47 § 6 mom. De föreslagna bestämmelserna strider därmed inte mot bestämmelserna i 81 § i grundlagen.

Bedömning av lagstiftningsordningen

Med stöd av vad som anförts ovan kan lagarna behandlas i vanlig lagstiftningsordning.

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

Lagförslag

1.

Lag

om ändring av lagen om stark autentisering och elektroniska signaturer

I enlighet med riksdagens beslut

upphävs i lagen om stark autentisering och elektroniska signaturer (617/2009) 4 och 5,

ändras lagens rubrik, 1 och 2 §, rubriken för 2 §, 6 §, 7 § 1 mom., 8 §, 9 § 1 mom., 10 §, 13 § 1 mom., 14 §, rubriken för 15 §, det inledande stycket i 15 § 1 mom., 16 §, rubriken för 17 §, 17 § 1 och 2 mom., den svenska språkdräkten i 19 § 1 mom. 8 punkten, rubriken för 20 §, 20 § 3 mom., 21, 22 och 24 §, 25 § 1—3 mom., 26 §, rubriken för 4 kap., 28—42 §, 43 § 1 mom., 44 § 1 mom., 45 § 1 mom., 46, 47 och 49 §, av dem 2 och 6 § sådana de lyder delvis ändrade i lag 139/2015 samt 7 § 1 mom. och 17 § 1 och 2 mom. i lag 139/2015, och

fogas till lagen nya 7 a, 8 a och 17 a§, en ny kapitelrubrik före 39 § och till lagen nya 42 a—42 c, 45 a och 49 a § som följer:

Lag

om stark autentisering och betrodda elektroniska tjänster

1 §

Tillämpningsområde

Denna lag innehåller bestämmelser om stark autentisering och om tillhandahållande av identifieringstjänster till tjänsteleverantörer, till allmänheten och till andra leverantörer av identifieringstjänster.

Lagen innehåller bestämmelser om tillsynen över efterlevnaden av Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, nedan *EU:s förordning om elektronisk identifiering*, samt bestämmelser som kompletterar den förordningen. Dessutom innehåller lagen bestämmelser om bedömning av överensstämmelsen med kraven när det gäller identifieringstjänster och betrodda tjänster.

På gränsöverskridande identifieringssystem som anmäls till Europeiska kommissionen tillämpas denna lag endast om inte något annat följer av EU:s förordning om elektronisk identifiering.

Lagen tillämpas inte på tillhandahållande av tjänster avsedda för identifiering internt inom en sammanslutning. Lagen tillämpas inte heller på en sammanslutning som använder en egen metod för identifiering av egna kunder i samband med egna tjänster.

2 §

Definitioner

I denna lag avses med
1) *stark autentisering* identifiering av en person, av en juridisk person eller av en fysisk person som företräder en juridisk person och verifiering av identifikatorns autenticitet och riktighet genom tillämpning av en elektronisk metod som motsvarar tillitsnivån väsentlig enligt artikel 8.2 a i EU:s förordning om elektronisk identifiering eller tillitsnivån hög enligt artikel 8.2 c i den förordningen,
2) *identifieringsverktyg* ett sådant medel för elektronisk identifiering som avses i artikel 3.2 i EU:s förordning om elektronisk identifiering,
3) *leverantör av identifieringstjänster* en leverantör av tjänster för identifieringsförmedling eller en leverantör av identifieringsverktyg,
4) *leverantör av identifieringsverktyg* en tjänsteleverantör som tillhandahåller eller ger ut identifieringsverktyg för stark autentisering till allmänheten samt tillhandahåller sitt identifieringsverktyg till leverantörer av tjänster för identifieringsförmedling för förmedling i förtroendenätet,
5) *leverantör av tjänster för identifieringsförmedling* en tjänsteleverantör som förmedlar identifieringstransaktioner baserade på stark autentisering till en part som förlitar sig på en elektronisk identifiering,
6) *innehavare av identifieringsverktyg* en fysisk eller juridisk person som enligt avtal har fått ett identifieringsverktyg av en leverantör av identifieringstjänster,
7*) inledande identifiering verifiering* av identiteten hos den som ansöker om ett identifieringsverktyg, när verifieringen sker i samband med att verktyget skaffas,
8) *certifikat* ett intyg i elektronisk form som verifierar identiteten eller verifierar identiteten och kopplar ihop autentiseringsuppgifter för en betrodd tjänst med en användare av tjänsten och som kan användas vid stark autentisering och betrodda tjänster,
9) *certifikatutfärdare* en fysisk eller juridisk person som tillhandahåller allmänheten certifikat,
10) *förtroendenätet* de leverantörer av identifieringstjänster som har gjort en anmälan till Kommunikationsverket.
11) *organ för bedömning av överensstämmelse* ett av Kommunikationsverket godkänt organ enligt artikel 2.13 i Europaparlamentets och rådets förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93, som är ackrediterat i enlighet med den förordningen.
Termerna *elektronisk underskrift, betrodd tjänst, avancerad elektronisk underskrift, system för elektronisk identifiering och förlitande part* har i denna lag samma betydelse som i artikel 3 i EU:s förordning om elektronisk identifiering.

2 kap.

Lagens tvingande natur och behandling av personuppgifter

6 §

Behandling av personuppgifter

Leverantörer av identifieringstjänster får på de grunder som anges i 8 § 1 mom. 1 och 2 punkten i personuppgiftslagen (523/1999) behandla personuppgifter som behövs när identifieringsverktyg ges ut, tjänster upprätthålls och identifieringstransaktioner genomförs. På samma grunder får certifikatutfärdare som tillhandahåller betrodda tjänster behandla de personuppgif-

ter som behövs vid utfärdandet och upprätthållandet av certifikat samt inhämta personuppgifter från personen själv.

En leverantör av tjänster för identifieringsförmedling har rätt att när en sådan tjänst tillhandahålls överlåta personuppgifter till en part som förlitar sig på en elektronisk identifiering, om den förlitande parten enligt lag har rätt att behandla personuppgifter.

Personuppgifter får behandlas i andra än i 1 mom. nämnda syften endast på de grunder som anges i 8 § 1 mom. 1 punkten i personuppgiftslagen.

När leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller betrodda tjänster kontrollerar sökandens identitet ska de kräva att sökanden uppger sin personbeteckning. Leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller betrodda tjänster får behandla personbeteckningar i sina register i de syften som nämns i 1 mom. Identifieringsverktyg och certifikat får innehålla en 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.

Bestämmelser om behandlingen av personuppgifter finns dessutom i 19 och 24 § och i personuppgiftslagen.

7 §

Användning av uppgifter i befolkningsdatasystemet

Leverantörer av identifieringsverktyg och certifikatutfärdare som tillhandahåller betrodda tjänster ska hämta och uppdatera de uppgifter som de behöver för tillhandahållandet av identifieringstjänster för fysiska personer med användning av befolkningsdatasystemet. Leverantörer av identifieringstjänster ska dessutom säkerställa att de uppgifter som de behöver för tillhandahållandet av identifieringstjänster är uppdaterade enligt uppgifterna i befolkningsdatasystemet.

— —

7 a §

Användning av uppgifter i företags- och organisationsregister

Leverantörer av identifieringsverktyg och certifikatutfärdare som tillhandahåller betrodda tjänster ska hämta och uppdatera de uppgifter som de behöver för tillhandahållandet av identifieringstjänster för juridiska personer med användning av företags- och organisationsregistren. Leverantörer av identifieringstjänster ska dessutom säkerställa att de uppgifter som de behöver för tillhandahållandet av identifieringstjänster är uppdaterade enligt uppgifterna i företags- och organisationsregistren.

8 §

Krav på system för elektronisk identifiering

Ett system för elektronisk identifiering ska uppfylla följande krav:

1) identifieringsmetoden grundar sig på en identifiering enligt 17 och 17 a § så att uppgifterna om den kan kontrolleras i efterskott i enlighet med 24 §,

2) identifieringsmetoden medger entydig identifiering av innehavaren av identifieringsverktyget så att åtminstone de villkor uppfylls som gäller för tillitsnivån väsentlig enligt avsnitten 2.1.2, 2.1.3 och 2.1.4 i bilagan till kommissionens genomförandeförordning (EU) 2015/1502

om fastställande av tekniska minimispecifikationer och förfaranden för tillitsnivåer för medel för elektronisk identifiering i enlighet med artikel 8.3 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden, nedan *förordningen om tillitsnivåer vid elektronisk identifiering*,

3) med hjälp av identifieringsmetoden går det att säkerställa att endast innehavaren av identifieringsverktyget kan använda verktyget på ett sådant sätt att åtminstone de villkor uppfylls som gäller för tillitsnivån väsentlig enligt avsnitten 2.2.1 och 2.3 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering,

4) identifieringssystemet är säkert och tillförlitligt på ett sådant sätt att åtminstone de villkor uppfylls som gäller för tillitsnivån väsentlig enligt avsnitten 2.2.1, 2.3.1 och 2.4.6 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering, med hänsyn till de informationssäkerhetsrisker som är förknippade med den teknik som används vid tidpunkten, och de lokaler som används för tillhandahållandet av identifieringstjänsten är säkra på det sätt som anges i avsnitt 2.4.5 i bilagan till den förordningen,

5) ledningen avseende informationssäkerheten sköts på ett sådant sätt att de villkor uppfylls som anges i i det inledande stycket i avsnitt 2.4 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering och åtminstone de villkor uppfylls som gäller för tillitsnivån väsentlig eller högre enligt avsnitt 2.4.3 och 2.4.7 i bilagan till den förordningen

Bestämmelserna i 1 mom. hindrar inte att specifika tjänster tillhandahålls så att leverantören av identifieringstjänster meddelar den tjänsteleverantör som använder en identifieringstjänst den pseudonym som innehavaren av identifieringsverktyget använder eller endast ett begränsat antal personuppgifter.

8 a §

Autentiseringsfaktorer som ska användas i identifieringsmetoden

I en identifieringsmetod ska minst två av följande autentiseringsfaktorer användas:

1) en *kunskapsbaserad autentiseringsfaktor* som personen måste kunna visa att den har kunskap om,

2) en *innehavsbaserad autentiseringsfaktor* som personen måste kunna visa att den innehar,

3) en *egenskapsbaserad autentiseringsfaktor* som utgår från en kroppslig egenskap hos en fysisk person.

I varje identifieringsmetod ska det i enlighet med avsnitt 2.3.1 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering användas en sådan dynamisk autentisering som kan ändras vid varje ny autentisering mellan en person och det system som kontrollerar personens identitet.

9 §

Krav som gäller leverantörer av identifieringstjänster

Juridiska personer som fungerar som leverantörer av identifieringstjänster och fysiska personer som handlar för deras räkning samt ledamöter eller ersättare i styrelsen eller förvaltningsrådet för en sammanslutning eller stiftelse som är tjänsteleverantör, liksom dess verkställande direktör och ansvariga bolagsmän andra personer i motsvarande ställning ska uppfylla följande krav:

1) de ska ha uppnått myndighetsålder,

2) de får inte vara försatta i konkurs,

3) de får inte ha begränsad handlingsbehörighet.

10 §

Skyldighet för leverantörer av identifieringstjänster att anmäla att verksamheten inleds

En leverantör av identifieringstjänster som är etablerad i Finland ska göra en skriftlig anmälan till Kommunikationsverket innan verksamheten inleds. Anmälan kan också göras av en sådan sammanslutning av leverantörer av identifieringsverktyg som administrerar en tjänst som ska betraktas som en enda identifieringstjänst.

Anmälan ska innehålla

1) tjänsteleverantörens namn,

2) tjänsteleverantörens fullständiga kontaktuppgifter,

3) uppgifter om de tjänster som tillhandahålls,

4) utredning om att kraven i 8, 8 a, 9, 13 och 14 § uppfylls med avseende på sökanden och sökandens verksamhet,

5) en inspektionsberättelse om oberoende bedömning i enlighet med 29 § utarbetad av ett organ för bedömning av överensstämmelse, något annat utomstående bedömningsorgan eller ett internt kontrollorgan,

6) övriga uppgifter som behövs för tillsynen.

Leverantören av identifieringstjänster ska utan dröjsmål skriftligen underrätta Kommunikationsverket om ändringar i de uppgifter som avses i 2 mom. Anmälan ska också göras när verksamheten avslutas eller funktionerna överförs till en annan tjänsteleverantör.

13 §

Allmänna skyldigheter för leverantörer av identifieringstjänster

Hos leverantörer av identifieringstjänster ska lagringen av uppgifter som sammanhänger med identifieringen, personalen och de tjänster som köps av underleverantörer uppfylla åtminstone kraven för tillitsnivån väsentlig enligt avsnitten 2.4.4 och 2.4.5 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering. Leverantörer av identifieringstjänster ska dessutom ha en omfattande plan för identifieringstjänstens upphörande.

— —

14 §

Principer för identifiering

Leverantörer av identifieringstjänster ska ha principer för identifiering som närmare anger hur tjänsteleverantören uppfyller de skyldigheter som anges i denna lag. Det ska i synnerhet anges närmare hur leverantören av identifieringsverktyg genomför den identifiering som avses i 17 och 17 a § när identifieringsverktyg beviljas.

Principerna för identifiering ska dessutom innehålla de viktigaste uppgifterna om

1) tjänsteleverantören,

2) de tjänster som tillhandahålls och priserna på dem,

3) samtliga villkor som tillämpas,

4) de principer för informationssäkerhet som tillämpas i tjänsten,

5) tjänsteleverantörens viktigaste samarbetspartner,

6) bedömningen av överensstämmelse enligt 29 §,

7) andra omständigheter som är av betydelse för att tjänsteleverantörens verksamhet och tillförlitlighet ska kunna bedömas.

Om elektroniska underskrifter eller avancerade elektroniska underskrifter kan skapas med ett identifieringsverktyg ska leverantören av identifieringstjänster också lämna uppgifter om hur och på vilken nivå de elektroniska underskrifterna tillhandahålls samt om säkerhetsfaktorerna i fråga om underskrifterna.

Leverantören av identifieringstjänster ska hålla principerna för identifiering allmänt tillgängliga och uppdaterade.

15 §

Skyldighet för leverantörer av identifieringsverktyg att lämna uppgifter innan avtal ingås

En leverantör av identifieringsverktyg ska innan ett avtal ingås informera den som ansöker om ett identifieringsverktyg om

— —

16 §

Skyldighet för leverantörer av identifieringstjänster att anmäla hot och störningar som riktas mot verksamheten eller skyddet av uppgifter

En leverantör av identifieringstjänster ska utan ogrundat dröjsmål anmäla betydande hot och störningar som riktas mot tjänsternas funktion, informationssäkerheten eller användningen av en elektronisk identitet till de tjänsternas förlitande parter, till innehavarna av identifieringsverktyg, till övriga avtalsparter i förtroendenätet och till Kommunikationsverket. Kommunikationsverket får för anmälarens räkning på teknisk väg förmedla uppgifterna mellan parterna i förtroendenätet trots vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet (621/1999).

Om hotet eller störningen är riktat mot skydd av uppgifter som avses i 32 § i personuppgiftslagen, ska leverantören av identifieringstjänster även underrätta dataombudsmannen om saken.

I en anmälan enligt 1 mom. ska det redogöras för de åtgärder som olika aktörer har tillgång till för att avvärja hot eller störningar samt de beräknade kostnaderna för åtgärderna.

En leverantör av identifieringstjänster får använda sådana uppgifter om en annan leverantör av identifieringstjänster som den fått med stöd av denna paragraf endast för att skapa beredskap för de hot och störningar som avses i denna paragraf. Hos en leverantör av identifieringstjänster får uppgifterna behandlas endast av den personal som nödvändigt behöver uppgifterna i sitt arbete. Uppgifterna ska också annars behandlas så att affärshemligheter som tillhör en annan leverantör av identifieringstjänster inte röjs.

En leverantör av identifieringstjänster som genom att handla i strid med 4 mom. vållar en annan leverantör av identifieringstjänster skada är skyldig att ersätta för skadan.

17 §

Identifiering av en fysisk person som ansöker om ett identifieringsverktyg

Vid inledande identifiering ska identifieringen av en fysisk person göras personligen eller elektroniskt på ett sådant sätt att de krav uppfylls som gäller för tillitsnivån väsentlig eller hög enligt avsnitt 2.1.2 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering. Kontrollen av en persons identitet kan grunda sig på en identitetshandling som utfärdats av en myndighet eller ett sådant identifieringsverktyg för stark autentisering som avses i denna lag. Kontrollen av identiteten kan dessutom grunda sig på ett förfarande som en offentlig eller privat aktör tidigare och i annat syfte än för beviljande av ett identifieringsverktyg för stark au-

tentisering har använt sig av och som Kommunikationsverket godkänner utifrån de bestämmelser som gäller förfarandet och utifrån myndighetstillsynen eller utifrån en bekräftelse av ett i 28 § 1 punkten avsett organ för bedömning av överensstämmelse.

Dokument som godkänns vid inledande identifiering, när identifieringen endast sker utifrån en identitetshandling som utfärdats av en myndighet, är ett giltigt pass eller identitetskort som har utfärdats av en myndighet i en medlemsstat inom Europeiska ekonomiska samarbetsområdet, i Schweiz eller i San Marino. En leverantör av identifieringsverktyg som så önskar kan också vid kontrollen av identiteten använda ett giltigt pass som har utfärdats av en myndighet i någon annan stat.

17 a §

Identifiering av en juridisk person som ansöker om ett identifieringsverktyg

Den identitet som uppgetts av en juridisk person ska kontrolleras med användning av företags- och organisationsregistren eller på ett sådant sätt att åtminstone de krav på styrkande och kontroll av juridiska personers identitet uppfylls som gäller för tillitsnivån väsentlig enligt avsnitt 2.1.3 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering.

19 §

Certifikatets innehåll

Om identifieringsmetoden grundar sig på ett certifikat, ska certifikatet åtminstone innehålla

8) certifikatutfärdarens avancerade elektroniska underskrift.

20 §

Beviljande av identifieringsverktyg

Identifieringsverktyg beviljas endast fysiska och juridiska personer. Bindningen mellan en fysisk persons och en juridisk persons identifieringsverktyg ska genomföras i enlighet med avsnitt 2.1.4 i förordningen om tillitsnivåer vid elektronisk identifiering. Ett identifieringsverktyg ska vara personligt. Till ett identifieringsverktyg kan det vid behov fogas en uppgift om att innehavaren av identifieringsverktyget i enskilda fall även får företräda en annan fysisk person eller en juridisk person.

21 §

Överlåtelse av identifieringsverktyg till sökande

Leverantören av ett identifieringsverktyg ska överlåta identifieringsverktyget till sökanden på det sätt som anges i avtalet. Leverantören ska säkerställa att verktyget inte obehörigt kommer i någon annans besittning vid överlåtelsen, på ett sådant sätt att åtminstone de krav uppfylls som gäller för tillitsnivån väsentlig enligt avsnitt 2.2.2 i förordningen om tillitsnivåer vid elektronisk identifiering.

22 §

Förnyande av identifieringsverktyg

En leverantör av identifieringsverktyg får leverera ett nytt verktyg till en innehavare av identifieringsverktyg utan en uttrycklig begäran om det endast om ett verktyg som tidigare har tillhandahållits ska ersättas med ett nytt. När identifieringsverktyg förnyas ska de krav uppfyllas som gäller för tillitsnivån väsentlig enligt avsnitt 2.2.4 i förordningen om tillitsnivåer vid elektronisk identifiering.

24 §

Registrering och användning av uppgifter om identifieringstransaktioner och identifieringsverktyg

Leverantörer av identifieringstjänster ska registrera
1) de uppgifter som behövs för att verifiera en enskild identifieringstransaktion eller elektronisk underskrift,
2) uppgifter om i 18 § avsedda hinder och begränsningar som gäller användningen av identifieringsverktyg,
3) i fråga om certifikat, uppgifter om certifikatets innehållet i certifikat enligt 19 §.

Leverantörer av identifieringsverktyg ska registrera behövliga uppgifter om den inledande identifiering av sökande som avses i 17 och 17 a § och om de handlingar eller den elektroniska identifiering som använts i den inledande identifieringen.

De uppgifter som avses i 1 mom. 1 punkten ska lagras i fem år från identifieringstransaktionen. De övriga uppgifter som avses i 1 och 2 mom. ska lagras i fem år från det att ett fast kundförhållande har upphört.

Personuppgifter som har uppkommit i samband med en identifieringstransaktion ska förstöras efter transaktionen, om det inte är nödvändigt att registrera dem för att verifiera en enskild identifieringstransaktion.

Leverantören av identifieringstjänster får behandla registrerade uppgifter endast för att tillhandahålla och upprätthålla tjänsterna, fakturera, trygga sina rättigheter vid tvister och utreda missbruk samt på begäran av en tjänsteleverantör som använder identifieringstjänster eller en innehavare av ett identifieringsverktyg. Leverantören av identifieringstjänster ska registrera uppgifter om när och varför uppgifterna behandlats och vem som gjort det.

Om en tjänsteleverantör endast ger ut identifieringsverktyg
1) tillämpas inte 1 mom. 1 punkten och 4 mom. på tjänsteleveratören,
2) räknas den registreringstid på fem år som avses i 3 mom. från det att identifieringsverktyget upphörde att gälla.

25 §

Anmälan om återkallande eller förhindrande av användning av identifieringsverktyg

Innehavaren av ett identifieringsverktyg ska utan obefogat dröjsmål göra en anmälan till leverantören av identifieringsverktyget, eller någon annan aktör som denne har utsett, om verktyget har förkommit, obehörigen har kommit i någon annans besittning eller obehörigen har använts. Anmälan ska göras utan obefogat dröjsmål efter det att saken har upptäckts.

Leverantören av identifieringsverktyg ska se till att det är möjligt att när som helst göra en anmälan enligt 1 mom. Leverantören ska utan dröjsmål återkalla identifieringsverktyget eller förhindra dess användning efter det att anmälan har mottagits.

Leverantören av ett identifieringsverktyg ska på lämpligt sätt och utan dröjsmål i systemet registrera uppgifter om tidpunkten för återkallandet eller förhindrandet av användningen. Innehavaren av identifieringsverktyget har rätt att på begäran få ett intyg över att innehavaren har gjort den anmälan som avses i 1 mom. Intyget ska begäras inom 18 månader från anmälan
— —

26 §

Rätten för leverantörer av identifieringsverktyg att återkalla eller förhindra användning av identifieringsverktyg

Utöver vad som föreskrivs i 25 § får leverantören av ett identifieringsverktyg återkalla eller förhindra användningen av identifieringsverktyget, om
1) leverantören har skäl att misstänka att identifieringsverktyget används av någon annan än den som det har beviljats till,
2) identifieringsverktyget innehåller ett uppenbart fel,

3) leverantören har skäl att misstänka att säkerheten vid användningen av identifieringsverktyget har äventyrats,
4) innehavaren av identifieringsverktyget använder det på ett sätt som väsentligt strider mot avtalsvillkoren,
5) innehavaren av identifieringsverktyget har avlidit.
Leverantören av identifieringsverktyget ska så snart som möjligt underrätta innehavaren av identifieringsverktyget om att identifieringsverktyget har återkallats eller användningen av det förhindrats samt om tidpunkten för och orsakerna till detta.
Leverantören av identifieringsverktyget ska erbjuda en ny möjlighet att använda identifieringsverktyget eller tillhandahålla innehavaren ett nytt verktyg omedelbart efter det att en sådan orsak som avses 1 mom. 2 eller 3 punkten inte längre föreligger.

4 kap.

Bedömning av överensstämmelse

28 §

Organ för bedömning av överensstämmelse

Överensstämmelsen hos en tjänst enligt detta kapitel kan bedömas av följande bedömningsorgan
1) ett organ för bedömning av överensstämmelse,
2) ett annat utomstående bedömningsorgan som är verksamt enligt en allmänt använd metod (annat utomstående bedömningsorgan), eller
3) ett oberoende bedömningsorgan inom tjänsteleverantörens organisation som uppfyller en allmänt använd standard (internt kontrollorgan).

29 §

Bedömning av överensstämmelse hos en elektronisk identifieringstjänst

En leverantör av identifieringstjänster ska regelbundet låta ett sådant bedömningsorgan som nämns i 28 § bedöma om identifieringstjänsten uppfyller kraven på interoperabilitet, informationssäkerhet, dataskydd och annan tillförlitlighet enligt denna lag.

Bestämmelser om bedömning av överensstämmelse hos system för elektronisk identifiering som ska anmälas till Europeiska kommissionen finns i EU:s förordning om elektronisk identifiering och i förordningen om tillitsnivåer vid elektronisk identifiering.

Bestämmelser om Kommunikationsverkets rätt att meddela närmare föreskrifter om bedömningsgrunderna vid bedömningen av överensstämmelsen hos en identifieringstjänst finns i 42 §. Som bedömningsgrund kan Kommunikationsverket utöver de författningar och rättsakter som avses i 1 och 2 mom. fastställa bestämmelser eller riktlinjer som antagits av Europeiska unionen eller något annat internationellt organ, publicerade och generellt eller regionalt tillämpade anvisningar för informationssäkerhet samt datasäkerhetsstandarder eller förfaranden som används allmänt.

30 §

Bedömning av överensstämmelse hos den nationella noden för elektronisk identifiering

Överensstämmelse hos det nationella gränssnitt som hör till EU:s interoperabilitetsramverk för elektronisk identifiering (*den nationella noden*) ska påvisas genom en bedömning som görs av ett organ för bedömning av överensstämmelse eller ett annat utomstående bedömningsorgan.

Bestämmelser om kraven på den nationella noden finns i kommissionens genomförandeförordning (EU) 2015/1501 om interoperabilitetsramverket enligt artikel 12.8 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden. Bestämmelser om Kommunikationsverkets rätt att meddela närmare föreskrifter om bedömningsgrunderna vid bedömningen av överensstämmelse hos den nationella noden finns i 42 §.

31 §

Inspektionsberättelse

En leverantör av identifieringstjänster och Befolkningsregistercentralen ska över bedömningen av överensstämmelse låta utarbeta en inspektionsberättelse som lämnas in till Kommunikationsverket.

Inspektionsberättelsen är i kraft den tid som anges i den standard som användes vid bedömningen, dock högst i 2 år.

32 §

Fastställande av överensstämmelse hos betrodda tjänster

Ett organ för bedömning av överensstämmelse ska inspektera en kvalificerad tillhandahållare av betrodda tjänster och överensstämmelsen hos en kvalificerad betrodd tjänst med iakttagande av bestämmelserna i EU:s förordning om elektronisk identifiering.

Bestämmelser om Kommunikationsverkets rätt att meddela närmare föreskrifter om bedömningsgrunderna vid bedömningen av överensstämmelse finns i 42 §. Som bedömningsgrund kan Kommunikationsverket fastställa bestämmelser eller riktlinjer som antagits av Europeiska unionen eller något annat internationellt organ, publicerade och generellt eller regionalt tillämpade anvisningar för informationssäkerhet samt datasäkerhetsstandarder eller förfaranden som används allmänt.

33 §

Allmänna krav på bedömningsorgan

De bedömningsorgan som nämns i 28 § omfattas av följande kompetenskrav:
1) organet ska vara funktionellt och ekonomiskt oberoende av bedömningsobjektet,
2) organets personal ska ha god teknisk och yrkesinriktad utbildning samt tillräckligt omfattande erfarenhet av de uppgifter som ingår i bedömningsverksamheten,
3) organet ska förfoga över den utrustning och de lokaler, redskap och system som behövs för bedömningsverksamheten,
4) organet ska ha ändamålsenliga riktlinjer för verksamheten och uppföljningen av den.

Bestämmelser om Kommunikationsverkets rätt att meddela närmare föreskrifter om de krav som anges i 1 mom. finns i 42 §.

Ett organ för bedömning av överensstämmelse ska visa att kraven i 1 mom. 1–3 punkten är uppfyllda genom en ackreditering beviljad av den nationella ackrediteringsenheten med iakttagande av bestämmelserna i Europaparlamentets och rådets förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 och i lagen om konstaterande av tillförlitligheten hos tjänster för bedömning av överensstämmelse med kraven (920/2005).

En leverantör av identifieringstjänster ska i den anmälan som avses i 1 mom. lämna en redogörelse för att ett annat utomstående bedömningsorgan eller ett internt kontrollorgan som bedömt dess överensstämmelse uppfyller kraven enligt 1 mom. Att kraven i 1 mom. 1–3 punkten är uppfyllda ska visas genom en ackreditering enligt 2 mom. eller genom ett annat oberoende förfarande som grundar sig på en allmänt använd standard.

En ackreditering som beviljas av en utländsk ackrediteringsenhet motsvarar ett ackrediteringsbeslut enligt 3 och 4 mom.

34 §

Godkännande av organ för bedömning av överensstämmelse

Organ för bedömning av överensstämmelse godkänns av Kommunikationsverket. Ett organ kan godkännas för viss tid, om det finns särskilda skäl till detta. Kommunikationsverket kan förena ett beslut om godkännande med begränsningar och villkor rörande organets kompetensområde, tillsynen över organet och organets verksamhet.

35 §

Ansökan om att bli organ för bedömning av överensstämmelse

Organ för bedömning av överensstämmelse godkänns efter ansökan. Ansökan ska innehålla sådana uppgifter om sökanden och sökandens verksamhet utifrån vilka det kan avgöras om kraven i 33 § är uppfyllda.

När Kommunikationsverket behandlar en ansökan kan verket skaffa utlåtanden samt anlita utomstående experter för att bedöma ansökan och de uppgifter som ges i ansökan.

36 §

Certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter eller kvalificerade elektroniska stämplar

Kommunikationsverket får efter ansökan utse offentliga eller privata certifieringsorgan enligt artiklarna 30 och 39.2 i EU:s förordning om elektronisk identifiering som har i uppgift att certifiera anordningar för skapande av kvalificerade elektroniska underskrifter eller kvalificerade elektroniska stämplar. Certifieringsorganet kan utses för viss tid. I sin ansökan ska certifieringsorganet ange de uppgifter som Kommunikationsverket begär och som behövs för behandlingen av ansökan.

Certifieringsorganet ska vara funktionellt och ekonomiskt oberoende av tillverkarna av anordningar för skapande av elektroniska underskrifter eller elektroniska stämplar. Organet ska ha en ansvarsförsäkring som är tillräcklig med hänsyn till verksamhetens omfattning, eller något annat motsvarande arrangemang, och det ska ha tillgång till en tillräckligt stor yrkeskunnig personal och de system, den utrustning och de redskap som behövs för verksamheten.

37 §

Allmänna skyldigheter för certifieringsorgan och organ för bedömning av överensstämmelse

Ett organ för bedömning av överensstämmelse och ett certifieringsorgan får i sitt uppdrag anlita biträde av personer som inte hör till organisationen. Organen ansvarar också för det arbete som utförts av personer de anlitat.

Bestämmelser om de principer för god förvaltning som organ för bedömning av överensstämmelse och certifieringsorgan ska följa när de utför offentliga förvaltningsuppgifter som avses i denna lag finns i förvaltningslagen (434/2003), lagen om offentlighet i myndigheternas verksamhet, lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003), språklagen (423/2003) och samiska språklagen (1086/2003). På personalen vid organ för bedömning av överensstämmelse och vid certifieringsorgan och vid dotterbolag och underentreprenörer som anlitas av sådana organ tillämpas bestämmelserna om straffrättsligt tjänsteansvar när den sköter uppgifter som avses i denna paragraf,. Bestämmelser om skadeståndsansvar finns i skadeståndslagen (412/1974).

Organ för bedömning av överensstämmelse och certifieringsorgan ska underrätta Kommunikationsverket om varje ändring som har betydelse för uppfyllandet av villkoren för att godkännas eller utses.

38 §

Återkallande av godkännande som organ för bedömning av överensstämmelse eller utseende till certifieringsorgan

Om Kommunikationsverket konstaterar att ett organ för bedömning av överensstämmelse eller ett certifieringsorgan inte uppfyller föreskrivna villkor eller att organet i väsentlig grad handlar i strid med gällande bestämmelser, ska Kommunikationsverket sätta ut en tillräcklig tidsfrist inom vilken saken ska rättas till.

Kommunikationsverket kan återkalla ett beslut att godkänna ett bedömningsorgan eller utse ett certifieringsorgan om organet inte har korrigerat sin verksamhet inom den tid som satts ut enligt 1 mom. och det är fråga om en väsentlig förseelse eller försummelse.

4 a kap.

Betrodda tjänster

39 §

Återkallande av certifikat

En undertecknare eller en innehavare av en elektronisk stämpel ska utan dröjsmål begära att den certifikatutfärdare som har utfärdat ett kvalificerat certifikat ska återkalla det, om undertecknaren har grundad anledning att misstänka att framställningsdata för undertecknings eller den elektroniska stämpeln används på obehörigt sätt.

En certifikatutfärdare som tillhandahåller kvalificerade certifikat ska utan dröjsmål återkalla ett kvalificerat certifikat, om undertecknaren eller innehavaren av den elektroniska stämpeln begär det. En begäran om återkallande av ett certifikat anses ha kommit in till certifikatutfärdaren när den har stått till utfärdarens förfogande så att begäran har kunnat behandlas.

40 §

Ansvar för obehörig användning av framställningsdata för en underteckning eller elektronisk stämpel

En undertecknare och en innehavare av en elektronisk stämpel ansvarar för skada som orsakats av obehörig användning av framställningsdata för en avancerad elektronisk underskrift eller elektronisk stämpel som är baserad på ett kvalificerat certifikat tills en begäran om återkallande av certifikatet har kommit in till certifikatutfärdaren så som anges i 39 § 2 mom.

En konsument har dock ansvar enligt 1 mom. endast om

1) konsumenten har överlåtit framställningsdata till någon annan,

2) någon som är obehörig att använda framställningsdata kommit åt dem på grund av att konsumenten varit vårdslös på ett sätt som inte är lindrigt, eller

3) konsumenten på annat sätt än det som nämns i 2 punkten har förlorat besittningen till framställningsdata och därefter har underlåtit att begära att det certifikatet ska återkallas så som anges i 39 § 1 mom.

41 §

Det ansvar som vilar på tillhandahållare av betrodda tjänster

Bestämmelser om det ansvar som vilar på tillhandahållare av betrodda tjänster finns i artikel 13 i EU:s förordning om elektronisk identifiering.

Den certifikatutfärdare som tillhandahållit ett kvalificerat certifikat är ansvarig för skada som den som förlitat sig på det kvalificerade certifikatet orsakats genom att certifikatutfärdaren eller en person som denne anlitat inte har återkallat certifikatet på det sätt som anges i 39 §. Certifikatutfärdaren är fri från ansvar, om den visar att skadan inte har berott på oaktsamhet hos certifikatutfärdaren eller en person som denne anlitat.

42 §

Allmän styrning och Kommunikationsverkets föreskrifter

Kommunikationsministeriet svarar för den allmänna styrningen och utvecklingen av stark autentisering och betrodda tjänster.

Kommunikationsverket får meddela närmare föreskrifter om

1) kraven enligt 8 § 1 mom. 4 och 5 punkten på säkerhet och tillförlitlighet hos identifieringssystemet,

2) innehållet i de uppgifter som ska anmälas enligt 10 § och inlämnandet av dem till Kommunikationsverket,

3) egenskaperna enligt 12 a § 2 mom. hos förtroendenätets gränssnitt,

4) när störningar som avses i 16 § är betydande och innehållet i anmälningar enligt 16 § 1 mom. samt anmälningarnas form och inlämnandet av dem,

5) grunderna för bedömningen enligt 29, 30 och 32 § av överensstämmelsen hos en identifieringstjänst, en betrodd tjänst och den nationella noden,

6) kompetenskraven enligt 33 § för organ för bedömning av överensstämmelse med beaktande av vad som föreskrivs i EU:s förordning om elektronisk identifiering,

7) de uppgifter som ska ingå i en ansökan enligt 35 § och inlämnandet av dem till Kommunikationsverket,

8) de krav som ställs på certifieringsorgan som avses i 36 §, förfarandet vid certifiering och kraven på anordningar för skapande av underskrifter och stämplar med beaktande av vad som föreskrivs i EU:s förordning om elektronisk identifiering.

42 a §

Kommunikationsverkets uppgifter

Kommunikationsverket ska utöva tillsyn över efterlevnaden av denna lag, om inte något annat föreskrivs i denna lag.

Kommunikationsverket ska i enlighet med EU:s förordning om elektronisk identifiering

1) delta i samarbetet mellan Europeiska unionens medlemsstater i det interoperabilitetsramverk för elektronisk identifiering som avses i artikel 12 i förordningen och i det samarbetsnätverk som upprättats för detta ändamål,

2) anmäla system för elektronisk identifiering till Europeiska kommissionen i enlighet med artiklarna 7—10 i förordningen,

3) vara tillsynsorgan enligt artikel 17 i förordningen och sköta tillsynsorganets uppgifter enligt förordningen,

4) i enlighet med artikel 22 i förordningen föra och publicera förteckningar över kvalificerade tillhandahållare av betrodda tjänster i Finland och över de kvalificerade betrodda tjänster som dessa tillhandahåller.

Kommunikationsverkets beslutanderätt omfattar inte avtalsförhållanden mellan parter eller frågor om ersättningsskyldighet.

42 b §

Dataombudsmannens uppgifter

Dataombudsmannen ska övervaka att bestämmelserna om personuppgifter i denna lag iakttas.

42 c §

Befolkningsregistercentralens uppgifter

Befolkningsregistercentralen ska upprätthålla den nationella nod som avses i 30 §.

43 §

Rätt till information

När Kommunikationsverket fullgör sina uppgifter enligt denna lag har verket trots sekretessbestämmelserna rätt att få den information som behövs för skötseln av uppgifterna av dem vars rättigheter och skyldigheter denna lag gäller och av dem som handlar för dessas räkning.

— —

44 §

Myndighetssamarbete och rätt att lämna information

Utöver vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet har Kommunikationsverket och dataombudsmannen trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av uppgifter rätt att lämna Finansinspektionen och Konkurrens- och konsumentverket den information som de behöver för skötseln av sina uppgifter. Finansinspektionen och Konkurrens- och konsumentverket har motsvarande rätt att trots sekretessbestämmelserna lämna Kommunikationsverket och dataombudsmannen de uppgifter som behövs för skötseln av deras uppgifter enligt denna lag.

— —

45 §

Administrativa tvångsmedel

Kommunikationsverket kan ge en anmärkning till den som bryter mot denna lag eller bestämmelser som utfärdats eller föreskrifter eller beslut som har meddelats med stöd av den, eller mot EU:s förordning om elektronisk identifiering eller bestämmelser som har utfärdats med stöd av den, samt ålägga denne att avhjälpa felet eller försummelsen inom skälig tid. 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. Bestämmelser om vite, hot om avbrytande och hot om tvångsutförande finns i viteslagen (1113/1990).

— —

45 a §

Interimistiska beslut

Om ett fel eller en försummelse som gäller EU:s förordning om elektronisk identifiering, denna lag eller bestämmelser som utfärdats eller föreskrifter som meddelats med stöd av dem, eller en störning i datasäkerheten, omedelbart och i väsentlig grad äventyrar tillförlitligheten hos en identifieringstjänst eller betrodd tjänst, får Kommunikationsverket omgående besluta om behövliga interimistiska åtgärder oberoende av den tidsfrist som avses i 45 §.

Kommunikationsverket ska innan det beslutar om interimistiska åtgärder ge den som är föremål för beslutet tillfälle att bli hörd, utom när detta inte kan ordnas så snabbt som ärendets brådskande natur nödvändigtvis kräver.

Som interimistisk åtgärd kan Kommunikationsverket förbjuda eller avbryta

1) tillhandahållandet av en identifieringsmetod som stark autentisering,

2) tillhandahållandet av en sådan kvalificerad betrodd tjänst som avses i artikel 3.17 i EU:s förordning om elektronisk identifiering,

3) tillhandahållandet av ett system för elektronisk identifiering som anmälts enligt artikel 9.1 i EU:s förordning om elektronisk identifiering,

4) tillhandahållandet av autentisering enligt artikel 7 f i EU:s förordning om elektronisk identifiering.

De interimistiska åtgärderna kan vara i kraft i högst tre månader. Beslut om interimistiska åtgärder får överklagas separat, på samma sätt som beslut som avses i 45 § 1 mom.

46 §

Inspektionsrätt

Kommunikationsverket har rätt att utföra inspektioner av leverantörer av identifieringstjänster och av leverantörernas tjänster, av organ för bedömning av överensstämmelse som avses i 28 §, av certifieringsorgan enligt 36 § för anordningar för skapande av kvalificerade elektroniska underskrifter och elektroniska stämplar och dessa organs verksamhet, av certifikatutfärdare som tillhandahåller kvalificerade certifikat samt av tillhandahållare av betrodda tjänster och deras tjänster. En inspektion kan genomföras för att övervaka fullgörandet av skyldigheter enligt denna lag och EU:s förordning om elektronisk identifiering samt bestämmelser som utfärdats och föreskrifter och beslut som har meddelats med stöd av dem. Bestämmelser om inspektioner finns i 39 § i förvaltningslagen.

Kommunikationsverket förordnar en inspektör att utföra de inspektioner som avses i 1 mom. Den som utför inspektionen har rätt att hos en leverantör av identifieringstjänster, hos en certifikatutfärdare som tillhandahåller kvalificerade certifikat och hos en tillhandahållare av betrodda tjänster samt hos personer som dessa anlitar granska sådan maskinvara och programvara som kan vara av betydelse vid tillsynen över efterlevnaden av denna lag och de bestämmelser utfärdats och föreskrifter som meddelats med stöd av den.

Leverantörer av identifieringstjänster, certifikatutfärdare som tillhandahåller kvalificerade certifikat, tillhandahållare av betrodda tjänster och de personer som dessa anlitar ska för inspektionen ge en inspektör som avses i 2 mom. tillträde till alla andra utrymmen än sådana som används för boende av permanent natur.

Kommunikationsverket har rätt att få handräckning av polisen för att utföra inspektioner enligt denna paragraf.

Dataombudsmannen har vid fullgörandet av sina uppgifter den rätt att utföra inspektioner som anges i personuppgiftslagen.

47 §

Avgifter till Kommunikationsverket

En leverantör av identifieringstjänster och en sammanslutning av tjänsteleverantörer som har gjort en anmälan enligt 10 § ska betala Kommunikationsverket en registreringsavgift på 5 000 euro. Leverantören av identifieringstjänster och sammanslutningen ska dessutom betala Kommunikationsverket en årlig tillsynsavgift på 14 000 euro.

En kvalificerad tillhandahållare av betrodda tjänster som gjort en anmälan enligt artikel 21 i EU:s förordning om elektronisk identifiering och en certifikatutfärdare som tillhandahåller kvalificerade betrodda tjänster ska betala Kommunikationsverket en registreringsavgift på 5

000 euro för varje betrodd tjänst de tillhandahåller. Dessutom ska de betala Kommunikationsverket en årlig tillsynsavgift på 14 000 euro för den första kvalificerade betrodda tjänst som de tillhandahåller och en årlig tillsynsavgift på 9 000 euro för varje därpå följande kvalificerade betrodda tjänst som de tillhandahåller. Om en certifikatutfärdare som tillhandahåller betrodda tjänster även gör en anmälan enligt 10 §, ska certifikatutfärdaren dessutom betala den registreringsavgift som anges i 1 mom.

Ett organ för bedömning av överensstämmelse som godkänts enligt 34 § ska betala Kommunikationsverket en utnämningsavgift på 10 000 euro. Dessutom ska organet betala Kommunikationsverket en årlig tillsynsavgift på 15 000 euro.

Ett certifieringsorgan som utsetts enligt 36 § ska betala Kommunikationsverket en utnämningsavgift på 10 000 euro. Dessutom ska organet betala Kommunikationsverket en årlig tillsynsavgift på 15 000 euro.

Registreringsavgiften, utnämningsavgiften och tillsynsavgiften täcker Kommunikationsverkets kostnader för att utföra uppgifterna enligt denna lag, med undantag för de uppgifter som avses i 46 § 1 mom. Tillsynsavgiften ska betalas till fullt belopp också under det första verksamhetsåret, även om verksamheten inleds under året. Tillsynsavgiften återbetalas inte, även om tjänsteleverantören upphör med sin verksamhet under året.

Registreringsavgiften, utnämningsavgiften och tillsynsavgiften påförs av Kommunikationsverket och avgifterna är direkt utsökbara. I kommunikationsverkets beslut om påförande av avgift får ändring sökas i enlighet med 49 § 1 mom. Närmare bestämmelser om verkställigheten av avgifterna får utfärdas genom förordning av kommunikationsministeriet.

Bestämmelser om indrivning av registreringsavgiften, utnämningsavgiften och tillsynsavgiften finns i lagen om verkställighet av skatter och avgifter. Om avgifterna inte betalas senast på förfallodagen, tas årlig dröjsmålsränta ut på det obetalda beloppet enligt den räntesats som avses i 4 § i räntelagen (633/1982). I stället för dröjsmålsränta kan myndigheten ta ut en dröjsmålsavgift på fem euro om dröjsmålsräntan är mindre än detta belopp.

För en inspektion som avses i 46 § 1 mom. tas kostnaderna för inspektionen ut av föremålet för inspektionen med iakttagande av lagen om grunderna för avgifter till staten.

49 §

Sökande av ändring i myndighetsbeslut

Omprövning av ett beslut som fattats av Kommunikationsverket om en avgift som ska betalas till Kommunikationsverket enligt 47 § får begäras på det sätt som anges i 7 a kap. i förvaltningslagen.

Beslut som Kommunikationsverket fattat med anledning av en begäran om omprövning samt andra beslut av Kommunikationsverket än sådana som avses i 1 mom. får överklagas genom besvär hos förvaltningsdomstolen på det sätt som anges i förvaltningsprocesslagen (586/1996).

Förvaltningsdomstolens beslut i ett ärende som gäller återkallande av ett beslut om att godkänna ett organ för bedömning av överensstämmelse eller om att utse ett certifieringsorgan får överklagas genom besvär på det sätt som anges i förvaltningsprocesslagen. Över andra beslut av förvaltningsdomstolen får besvär anföras endast om högsta förvaltningsdomstolen beviljar besvärstillstånd.

Kommunikationsverket får i sina beslut bestämma att beslutet ska iakttas innan det har vunnit laga kraft. Besvärsmyndigheten kan dock förbjuda verkställigheten av beslutet tills besvären har avgjorts.

Bestämmelser om sökande av ändring i ett beslut av dataombudsmannen finns i personuppgiftslagen.

49 a §

Sökande av ändring i beslut av organ för bedömning av överensstämmelse och beslut av certifieringsorgan

Omprövning av ett beslut som fattats av ett organ för bedömning av överensstämmelse eller av ett certifieringsorgan med stöd av denna lag får begäras hos Kommunikationsverket på det sätt som anges i 7 a kap. i förvaltningslagen.

Beslut som fattats med anledning av en begäran om omprövning får överklagas genom besvär hos förvaltningsdomstolen på det sätt som anges förvaltningsprocesslagen. Över förvaltningsdomstolens beslut får besvär anföras endast om högsta förvaltningsdomstolen beviljar besvärstillstånd.

Beslut av organ för bedömning av överensstämmelse och beslut av certifieringsorgan ska iakttas oberoende av ändringssökande, om inte den myndighet där ändring sökts bestämmer något annat.

———

Denna lag träder i kraft den 20 .

En leverantör av identifieringsverktyg får till och med den 31 december 2018 som ett i 17 § 2 mom. i denna lag avsett godkänt dokument också använda ett giltigt körkort som har beviljats efter den 1 oktober 1990 av en myndighet i en medlemsstat i Europeiska ekonomiska samarbetsområdet.

De av Kommunikationsverket meddelade föreskrifter som gäller vid ikraftträdandet av denna lag förblir i kraft.

En leverantör av identifieringstjänster som är införd i det register som avses i 12 § ska senast två månader från ikraftträdandet av denna lag lämna Kommunikationsverket en ändringsanmälan enligt 10 § 3 mom., om leverantören vill fortsätta vara verksam som leverantör av identifieringstjänster för stark autentisering. De uppgifter som krävs enligt 10 § i denna lag ska lämnas in till Kommunikationsverket senast den 31 januari 2017.

Kommunikationsverket ska behandla en ändringsanmälan enligt 3 mom. från en leverantör av identifieringstjänster och göra de anteckningar som föranleds av anmälan i det register som avses i 12 § senast tre månader efter att ha mottagit ändringsanmälan och övriga uppgifter enligt 3 mom.

Ett identifieringsverktyg för stark autentisering som har beviljats enligt de bestämmelser som gällde vid ikraftträdandet av denna lag ska betraktas som ett identifieringsverktyg för stark autentisering för åtminstone tillitsnivån väsentlig i två månader från ikraftträdandet av denna lag. Om inte något annat följer av 7 mom. och om leverantören av identifieringstjänster lämnar en ändringsanmälan enligt 3 mom. inom utsatt tid, ska ett identifieringsverktyg leverantören beviljat före eller efter ikraftträdandet av denna lag betraktas som ett identifieringsverktyg för stark autentisering för åtminstone tillitsnivån väsentlig tills Kommunikationsverket har gjort en anteckning om identifieringstjänsten i det register som avses i 12 § utifrån uppgifterna i ändringsanmälan.

Ett elektroniskt identifieringsverktyg som har beviljats enligt 17 § i denna lag på grundval av ett elektroniskt identifieringsverktyg som sökanden tidigare innehaft ska betraktas som ett identifieringsverktyg för stark autentisering, om

1) identifieringsverktyget har beviljats senast två månader från ikraftträdandet av denna lag, eller

2) identifieringsverktyget har beviljats efter det att två månader förflutit från ikraftträdandet av denna lag på grundval av ett sådant annat identifieringsverktyg för stark autentisering som beviljats av en leverantör av identifieringstjänster som gjort en ändringsanmälan enligt 3 mom.

Ett elektroniskt identifieringsverktyg betraktas inte längre som ett identifieringsverktyg för stark autentisering, om leverantören av identifieringstjänster inte har lämnat en ändringsanmä-

lan enligt 3 mom. inom utsatt tid. Kommunikationsverket ska då avföra leverantören av identifieringstjänster ur det register som avses i 12 § och underrätta leverantören om detta.

———————

2.

Lag

om ändring av lagen om elektronisk kommunikation i myndigheternas verksamhet

I enlighet med riksdagens beslut

ändras i lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003) 3, 9, 16 och 18 §, sådana de lyder, 3 och 9 § delvis ändrade i lag 618/2009, 16 § i lag 618/2009 och 18 § i lag 924/2010, som följer:

3 §

Annan lagstiftning

Vid uträttande och behandling av ärenden hos myndigheter tillämpas i övrigt vad som föreskrivs om anhängiggörande av ärenden, delgivning av beslut, offentlighet i myndigheternas verksamhet, behandling av personuppgifter, arkivering av handlingar, det språk som används vid behandling av ärenden och om hur ärenden behandlas.

9 §

Krav på skriftlig form

Vid anhängiggörande och behandling av ärenden uppfyller också elektroniska dokument som sänts till en myndighet kravet på skriftlig form.

Ett elektroniskt dokument som kommit in till en myndighet behöver inte kompletteras med en underskrift, om dokumentet innehåller uppgifter om avsändaren och om det inte finns anledning att betvivla dokumentets autenticitet och integritet. Om ett elektroniskt dokument som sänts till en myndighet innehåller utredning om ett ombuds behörighet, behöver ombudet inte lämna in fullmakt. Myndigheten kan dock förordna att en fullmakt skall lämnas in, om den har anledning att betvivla ombudets behörighet eller behörighetens omfattning.

16 §

Elektronisk signering av beslutshandlingar

En beslutshandling får signeras elektroniskt. Myndigheten ska signera handlingen med en avancerad elektronisk underskrift som uppfyller kraven enligt artikel 26 i Europaparlamentets och rådets förordning (EU) Nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG eller annars på ett sådant sätt att man kan försäkra sig om handlingens autenticitet och integritet.

18 §

Bevislig elektronisk delgivning

En handling som enligt lag ska sändas med post mot mottagningsbevis eller delges bevisligen på annat sätt får med partens samtycke delges också som ett elektroniskt meddelande, dock inte per telefax eller på därmed jämförbart sätt. Myndigheten ska då meddela att parten eller dennes företrädare kan hämta handlingen från en av myndigheten anvisad server, databas eller någon annan fil.

Parten eller dennes företrädare ska identifiera sig när handlingen hämtas. Vid identifieringen ska då användas en identifieringsteknik som är datatekniskt tillförlitlig och bevislig.

En handling anses ha delgivits när den har hämtats från den länk som myndigheten anvisat enligt 1 mom. Om handlingen inte har hämtats inom sju dagar från myndighetens meddelande, iakttas vid delgivningen vad som annanstans i lag föreskrivs om delgivning.

Denna lag träder i kraft den 20 .

3.

Lag

om ändring av 2 § i lagen om kommunikationsförvaltningen

I enlighet med riksdagens beslut
ändras i lagen om kommunikationsförvaltningen (625/2001) 2 § 1 punkten, sådan den lyder i lag 730/2014, som följer:

2 §

Kommunikationsverkets uppgifter

Kommunikationsverket har till uppgift att
1) sköta de uppgifter som enligt informationssamhällsbalken (917/2014), postlagen (415/2011), lagen om statens televisions- och radiofond (745/1998), lagen om stark autentisering och betrodda elektroniska tjänster (617/2009), lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004), säkerhetsutredningslagen (726/2014), lagen om bedömningsorgan för informationssäkerhet (1405/2011) och lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation ankommer på Kommunikationsverket,

— —

———

Denna lag träder i kraft den 20 .

———

4.

Lag

om ändring av 9 a kap. 1 § i jordabalken

I enlighet med riksdagens beslut
ändras i jordabalken (540/1995) 9 a kap. 1 § 1 mom., sådant det lyder i lag 96/2011, som följer:

1 §

Användning av ärendehanteringssystem och elektronisk identifiering i ett ärendehanteringssystem

En förutsättning för att upprätta och godkänna elektroniska dokument i ett ärendehanteringssystem samt för att i övrigt använda ärendehanteringssystemet är att användaren identifieras på ett tillförlitligt sätt med hjälp av en sådan identifieringsmetod, tillhandahållen av en leverantör av tjänster för stark autentisering, som aves i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) eller ett sådant kvalificerat certifikat för elektronisk underskrift som föreskrivs i artikel 28 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, eller med hjälp av någon annan identifieringsteknik som är datatekniskt tillförlitlig och bevislig.

———

Denna lag träder i kraft den 20 .

———

5.

Lag

om ändring av 18 § i lagen om förhindrande och utredning av penningtvätt och av finansiering av terrorism

I enlighet med riksdagens beslut

ändras i lagen om förhindrande och utredning av penningtvätt och av finansiering av terrorism (503/2008) 18 § 3 punkten, sådan den lyder i lag 621/2009, som följer:

18 §

Skärpta krav på kontroll vid identifiering på distans

Om kunden inte är närvarande vid identifieringen och styrkandet av identiteten (identifiering på distans), ska den rapporteringsskyldiga vidta följande åtgärder för att minska risken för penningtvätt och finansiering av terrorism:

— —

3) kontrollera kundens identitet med ett identifieringsverktyg som avses i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) eller med ett kvalificerat certifikat för elektronisk underskrift som föreskrivs i artikel 28 i Europaparlamentets ock rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på inre marknaden och om upphävande av direktiv 1999/93/EG, eller med hjälp av någon annan teknik för elektronisk identifiering som är datatekniskt tillförlitlig och bevislig.

———

Denna lag träder i kraft den 20 .

———

6.

Lag

om ändring av lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster

I enlighet med riksdagens beslut

ändras i lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009) 2 § 2 mom. 2 punkten, 6 § 2 mom., 43 § 2 mom. 2 punkten, 61 § 3 mom., 62 §, 66 § 3 mom., 67 § 1 mom. och 68 § 1 mom., sådana de lyder i lag 983/2010, som följer:

2 §

Lagens tillämpningsområde

— —

Om inte något annat bestäms i denna lag, ska följande lagar tillämpas:

— —

2) i fråga om certifierad elektronisk kommunikation och behandlingen av uppgifter i det certifikatregister som avses i denna lag, lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003) och lagen om stark autentisering och betrodda elektroniska tjänster (617/2009).

6 §

Befolkningsregistercentralens certifierade elektroniska kommunikation och dess syfte

— —

Befolkningsregistercentralen för ett sådant certifikatregister över utfärdade personcertifikat som det föreskrivs om i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, nedan EU:s förordning om elektronisk identifiering). Befolkningsregistercentralen är registeransvarig för certifikatregistret.

— —

43 §

Utlämnande av identifieringsuppgifter

— —

Elektroniska kommunikationskoder som registrerats i befolkningsdatasystemet får lämnas ut endast om

— —

2) en annan i Finland etablerad certifikatutfärdare använder koden som en uppgift som identifierar innehavaren av certifikatet i certifikat som avses i lagen om stark autentisering och betrodda tjänster eller i motsvarande certifikat som används i identifieringssyfte.

— —

61 §

Tjänster som tillhandahålls vid certifierad elektronisk kommunikation

— —

Med medborgarcertifikat avses ett certifikat som utfärdats av Befolkningsregistercentralen för en fysisk person och som ingår i ett i lagen om identitetskort (829/1999) avsett identitetskort eller i en därmed jämförbar myndighetshandling eller ett tekniskt underlag och som används för verifiering av personen, för elektroniska underskrifter och för kryptering av handlingar och meddelanden. Med medborgarcertifikat avses också ett av Befolkningsregistercentralen utfärdat certifikat som ingår i en annan myndighetshandling eller ett tekniskt underlag och som används i ovan nämnda syfte och uppfyller kraven i EU:s förordning om elektronisk identifiering.

62 §

Uppgifter som ska ingå i certifikat för certifierad elektronisk kommunikation

Bestämmelser om vilka uppgifter som ska ingå i medborgarcertifikat och andra certifikat som Befolkningsregistercentralen utfärdar för fysiska personer finns i lagen om stark autentisering och betrodda tjänster och i EU:s förordning om elektronisk identifiering. Medborgarcertifikat ska innehålla en elektronisk kommunikationskod som identifierar innehavaren av certifikatet. Andra certifikat som Befolkningsregistercentralen utfärdar för fysiska personer ska innehålla en elektronisk kommunikationskod som identifierar innehavaren av certifikatet eller någon annan identifieringsuppgift som identifierar personen och som inte innehåller information om personen. Även andra tekniska uppgifter som är nödvändiga vid användningen av ett certifikat kan ingå i medborgarcertifikat och andra certifikat som Befolkningsregistercentralen utfärdar för fysiska personer. Befolkningsregistercentralen beslutar om dessa uppgifter.

En elektronisk kommunikationskod kan också ingå i andra i lagen om stark autentisering och betrodda tjänster avsedda certifikat för fysiska personer som en uppgift som identifierar innehavaren av certifikatet.

66 §

Ansökan om och utfärdande av medborgarcertifikat

— —

Den som tar emot ansökan ska iaktta de krav i personuppgiftslagen som gäller behandlingen av personuppgifter och de krav i lagen om stark autentisering och betrodda tjänster och i EU:s förordning om elektronisk identifiering som gäller utfärdande av certifikat.

67 §

Ansökan om och utfärdande av andra certifikat

Andra certifikat för fysiska personer som Befolkningsregistercentralen producerar och som inte är medborgarcertifikat kan utfärdas endast för finska medborgare samt för utlänningar som enligt lagen om hemkommun är stadigvarande bosatta i Finland och vars uppgifter har registrerats i befolkningsdatasystemet och vars identitet har kunnat konstateras på ett tillförlit-

ligt sätt. Andra certifikat än medborgarcertifikat som Befolkningsregistercentralen producerar för fysiska personer kan av särskilda och motiverade skäl också beviljas personer vars identitet har kunnat konstateras tillförlitligt även om de inte uppfyller övriga ovan nämnda villkor för att få certifikat. Sådana certifikat kan på sökandens begäran ingå i handlingar, kort och tekniska underlag som används vid elektronisk kommunikation och som utfärdas av en myndighet, ett företag eller en organisation. Befolkningsregistercentralen kan komma överens med en myndighet, ett företag eller en organisation som utfärdar handlingar eller tekniska underlag om att ansökningar om certifikat personligen kan lämnas in till myndigheten, företaget eller organisationen för vidarebefordran till Befolkningsregistercentralen. Befolkningsregistercentralen ska då se till att den som tar emot ansökan iakttar de bestämmelser i personuppgiftslagen som gäller behandlingen av personuppgifter och de bestämmelser i EU:s förordning om elektronisk identifiering som gäller utfärdande av certifikat.

— —

68 §

Ansökan om och utfärdande av certifikat i vissa fall

I stället för genom ett personligt besök kan ansökan om förnyande av ett medborgarcertifikat även göras elektroniskt och undertecknas med hjälp av ett medborgarcertifikat som sökanden använder, och ansökan om förnyande av ett annat certifikat som Befolkningsregistercentralen producerar undertecknas med hjälp av ett sådant kvalificerat certifikat enligt EU:s förordning om elektronisk identifiering som sökanden använder, om en sådan tjänst är i bruk. Vid behandlingen av ansökan iakttas bestämmelserna om utfärdande av certifikat i EU:s förordning om elektronisk identifiering.

— —

———

Denna lag träder i kraft den 20 .

———

7.

Lag

om ändring av lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården

I enlighet med riksdagens beslut

ändras i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) 2 § 3 mom., 9 § och 14 § 3 mom., sådana de lyder, 2 § 3 mom. i lag 250/2014, 9 § i lag 619/2009 och 14 § 3 mom. i lag 255/2015, som följer:

2 §

Tillämpningsområde

— —

Om inte något annat följer av denna eller någon annan lag tillämpas på behandlingen av klientuppgifter vad som föreskrivs i lagen om patientens ställning och rättigheter (785/1992), nedan patientlagen, lagen om klientens ställning och rättigheter inom socialvården (812/2000), nedan klientlagen, personuppgiftslagen (523/1999), lagen om offentlighet i myndigheternas verksamhet (621/1999), lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003), lagen om stark autentisering och betrodda elektroniska tjänster (617/2009), lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009) och arkivlagen (831/1994) eller i bestämmelser som utfärdats med stöd av dem. Vid behandlingen av kli-entuppgifter och ordnande av tjänster och funktioner enligt denna lag ska dessutom iakttas vad som föreskrivs i språklagen (423/2003) och med stöd av den. Om det informationssystem där hälso- och sjukvårdens klient- och patientuppgifter behandlas utgör sådan utrustning för hälso- och sjukvård som avses i lagen om produkter och utrustning för hälso- och sjukvård (629/2010) tillämpas på informationssystemet även den lagen och kraven i enlighet med den.

9 §

Elektronisk signering av handlingar

Klientuppgifternas integritet, oförvanskade form och oavvislighet ska säkerställas med en elektronisk underskrift vid elektronisk behandling, överföring och förvaring av uppgifterna. Vid elektronisk signering som görs av en fysisk person ska det användas en sådan avancerad elektronisk underskrift som det föreskrivs om i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG. Vid signering som görs av en organisation och datatekniska enheter ska det användas en elektronisk underskrift av motsvarande tillförlitlighet.

14 §

Riksomfattande informationssystemtjänster

— —

Befolkningsregistercentralen är certifikatutfärdare i enlighet med lagen om stark autentisering och betrodda elektroniska tjänster för yrkesutbildade personer inom social- och hälsovården och annan personal inom social- och hälsovården, tillhandahållare av social- och hälsovårdstjänster samt organisationer som deltar i tillhandahållandet av dessa tjänster, deras personal och datatekniska enheter. Befolkningsregistercentralen har rätt att för skötseln av dessa uppgifter av Tillstånds- och tillsynsverket för social- och hälsovården få den information som behövs för utfärdande och återkallande av certifikat, för certifikat, för det tekniska underlaget för certifikat och för sändande av certifikat, ur centralregistret över yrkesutbildade personer inom hälso- och sjukvården som verket upprätthåller. Tillstånds- och tillsynsverket för social- och hälsovården har på motsvarande sätt rätt att för skötseln av sina lagstadgade uppgifter av Befolkningsregistercentralen få information om de certifikat som centralen utfärdat på ovannämnda grunder. Informationen kan överlämnas med hjälp av en teknisk anslutning.

— —

———

Denna lag träder i kraft den 20 .

———

8.

Lag

om ändring av 93 a § i lagen om beskattningsförfarande

I enlighet med riksdagens beslut
ändras i lagen om beskattningsförfarande (1558/1995) 93 a § 2 mom., sådant det lyder i lag 623/2009, som följer:

93 a §

Elektronisk kommunikation och signering

— —

Deklarationer och andra handlingar som får lämnas in till skattemyndigheten på elektronisk väg och som ska signeras ska certifieras med en elektronisk underskrift eller på något annat godtagbart sätt.

— —

———

Denna lag träder i kraft den 20 .

———

9.

Lag

om ändring av 56 b § i lagen om överlåtelseskatt

I enlighet med riksdagens beslut

ändras i lagen om överlåtelseskatt (931/1996) 56 b § 2 mom., sådant det lyder i lag 622/2009, som följer:

56 b §

Elektronisk kommunikation och signering

— —

Deklarationer och andra handlingar som får lämnas in till skattemyndigheten på elektronisk väg och som ska signeras ska certifieras med en elektronisk underskrift eller på något annat godtagbart sätt.

— —

_____

Denna lag träder i kraft den 20 .

_____

10.

Lag

om ändring av 6 a § i lagen om förskottsuppbörd

I enlighet med riksdagens beslut

ändras i lagen om förskottsuppbörd (1118/1996) 6 a § 2 mom., sådant det lyder i lag 624/2009, som följer:

6 a §

Elektronisk kommunikation och signering

— —

Deklarationer och andra handlingar som får lämnas in till skattemyndigheten på elektronisk väg och som ska signeras ska certifieras med en elektronisk underskrift eller på något annat godtagbart sätt.

— —

———

Denna lag träder i kraft den 20 .

———

11.

Lag

om ändring av 11 § i blodtjänstlagen

I enlighet med riksdagens beslut
ändras i blodtjänstlagen (197/2005) 11 §, sådan den lyder i lag 777/2009, som följer:

11 §

Uppgifter som hänför sig till blodgivare

Den som ger blod och blodkomponenter ska före blodgivningen ges behövliga upplysningar som hänför sig till blodgivningen samt de uppgifter som avses i 24 § i personuppgiftslagen (523/1999). Blodgivaren ska informeras om sekretessen i fråga om uppgifterna. Av blodgivaren ska begäras identifieringsuppgifter, sådana uppgifter om hälsotillståndet som är nödvändiga när det gäller att bedöma blodgivarens lämplighet samt blodgivarens egenhändiga underskrift eller en sådan avancerad elektronisk underskrift som det föreskrivs om i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG. Säkerhets- och utvecklingscentret för läkemedelsområdet kan utfärda närmare föreskrifter om den information som ska ges till och inhämtas från blodgivare.

———

Denna lag träder i kraft den 20 .

———

12.

Lag

om ändring av 165 § i mervärdesskattelagen

I enlighet med riksdagens beslut

ändras i mervärdesskattelagen (1501/1993) 165 § 2 mom., sådant det lyder i lag 886/2009, som följer:

165 §

— —

Deklarationer enligt 162 e § och andra handlingar som får lämnas in till skattemyndigheten på elektronisk väg och som ska signeras ska certifieras med en elektronisk underskrift eller på något annat godtagbart sätt.

— —

———

Denna lag träder i kraft den 20 .

———

13.

Lag

om ändring av 7 § i skattekontolagen

I enlighet med riksdagens beslut
ändras i skattekontolagen (604/2009) 7 § 2 mom., sådant det lyder i lag 746/2009, som följer:

7 §

Inlämnande av periodskattedeklaration

— —

Den deklarationsskyldige ska underteckna periodskattedeklarationen. En periodskattedeklaration som lämnas in på elektronisk väg ska certifieras med en elektronisk underskrift eller på något annat godtagbart sätt. Skatteförvaltningen utfärdar närmare föreskrifter om med hjälp av vilka elektroniska förfaranden och certifierings- eller identifieringsmetoder periodskattedeklaration kan lämnas in på elektronisk väg.

— —

———

Denna lag träder i kraft den 20 .

———

14.

Lag

om ändring av 4 § i lagen om informationssystemet för byggnaders energicertifikat

I enlighet med riksdagens beslut

ändras i lagen om informationssystemet för byggnaders energicertifikat (147/2015) 4 § 1 mom. som följer:

4 §

Upprättande och signering av energicertifikat

Ett energicertifikat upprättas genom att upprättaren för in de uppgifter som behövs för upprättandet av energicertifikatet i registret över energicertifikat och signerar energicertifikatet med en sådan avancerad elektronisk underskrift som det föreskrivs om i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG. Energicertifikatet betraktas som inlämnat hos tillsynsmyndigheten när det är undertecknat på det sätt som anges ovan.

Denna lag träder i kraft den 20 .

15.

Lag

om ändring av 32 § i punktskattelagen

I enlighet med riksdagens beslut
ändras i punktskattelagen (182/2010) 32 § 3 mom., sådant det lyder i lag 495/2014, som följer:

32 §

Sätt att lämna in skattedeklaration

— —

En elektronisk skattedeklaration ska certifieras med en elektronisk underskrift eller på något annat godtagbart sätt. Den skattskyldige ska underteckna en skattedeklaration som lämnas in på en pappersblankett.

— —

———

Denna lag träder i kraft den 20 .

———

Helsingfors den 4 maj 2016

Statsminister

Juha Sipilä

Kommunikationsminister Anne Berner

Bilaga
Parallelltext

1.

Lag

om ändring av lagen om stark autentisering och elektroniska signaturer

I enlighet med riksdagens beslut

upphävs i lagen om stark autentisering och elektroniska signaturer (617/2009) 4 och 5,

ändras lagens rubrik, 1 och 2 §, rubriken för 2 §, 6 §, 7 § 1 mom., 8 §, 9 § 1 mom., 10 §, 13 § 1 mom., 14 §, rubriken för 15 §, det inledande stycket i 15 § 1 mom., 16 §, rubriken för 17 §, 17 § 1 och 2 mom., den svenska språkdräkten i 19 § 1 mom. 8 punkten, rubriken för 20 §, 20 § 3 mom., 21, 22 och 24 §, 25 § 1—3 mom., 26 §, rubriken för 4 kap., 28—42 §, 43 § 1 mom., 44 § 1 mom., 45 § 1 mom., 46, 47 och 49 §, av dem 2 och 6 § sådana de lyder delvis ändrade i lag 139/2015 samt 7 § 1 mom. och 17 § 1 och 2 mom. i lag 139/2015, och

fogas till lagen nya 7 a, 8 a och 17 a§, en ny kapitelrubrik före 39 § och till lagen nya 42 a—42 c, 45 a och 49 a § som följer:

Lag

om stark autentisering och betrodda elektroniska tjänster

Gällande lydelse	*Föreslagen lydelse*
1 §	1 §
Tillämpningsområde	*Tillämpningsområde*
I denna lag föreskrivs om stark autentisering och elektroniska signaturer samt om tillhandahållande av tjänster i anslutning till dem för tjänsteleverantörer som använder tjänsterna och för allmänheten.	*Denna lag innehåller bestämmelser om stark autentisering och om tillhandahållande av identifieringstjänster till tjänsteleverantörer, till allmänheten och till andra leverantörer av identifieringstjänster.*
Lagen tillämpas inte på tillhandahållande av tjänster avsedda för identifiering eller elektroniska signaturer internt inom en sammanslutning.	*Lagen innehåller bestämmelser om tillsynen över efterlevnaden av Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, nedan EU:s förordning om elektronisk identifiering, samt bestämmelser som kompletterar den förordningen. Dessutom innehåller lagen bestämmelser om*
Lagen tillämpas inte heller om en sammanslutning tillämpar en egen metod för identifiering för att i samband med sina egna tjänster identifiera sina egna kunder.	
Lagen tillämpas inte på tillverkning, import eller försäljning av identifieringsverktyg eller	

verktyg för elektroniska signaturer.

bedömning av överensstämmelsen med kraven när det gäller identifieringstjänster och betrodda tjänster.

På gränsöverskridande identifieringssystem som anmäls till Europeiska kommissionen tillämpas denna lag endast om inte något annat följer av EU:s förordning om elektronisk identifiering.

Lagen tillämpas inte på tillhandahållande av tjänster avsedda för identifiering internt inom en sammanslutning. Lagen tillämpas inte heller på en sammanslutning som använder en egen metod för identifiering av egna kunder i samband med egna tjänster.

2 §

Definitioner

I denna lag avses med

1) *stark autentisering* identifiering av en person och verifiering av identifikatorns autenticitet och riktighet genom tillämpning av en elektronisk metod där 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,

2) *identifieringsverktyg* föremål och specificerande uppgifter eller egenskaper som tillsammans utgör de identifikatorer, verktyg för identifiering och verktyg för verifiering som behövs för stark autentisering,

3) identifieringsmetod den helhet som bildas av identifieringsverktyget tillsammans med det system som behövs för att genomföra en enskild identifieringstransaktion baserad på stark autentisering,

4) *leverantör* av identifieringstjänster en tjänsteleverantör som tillhandahåller tjänster för stark autentisering till tjänsteleverantörer som använder sådana tjänster eller som ger ut identifieringsverktyg till allmänheten eller bådadera,

5) *innehavare av identifieringsverktyg* en fysisk person som på basis av avtal har fått

2 §

Definitioner

I denna lag avses med

1) stark autentisering identifiering av en person, av en juridisk person eller av en fysisk person som företräder en juridisk person och verifiering av identifikatorns autenticitet och riktighet genom tillämpning av en elektronisk metod som motsvarar tillitsnivån väsentlig enligt artikel 8.2 a i EU:s förordning om elektronisk identifiering eller tillitsnivån hög enligt artikel 8.2 c i den förordningen,

2) identifieringsverktyg ett sådant medel för elektronisk identifiering som avses i artikel 3.2 i EU:s förordning om elektronisk identifiering,

3) leverantör av identifieringstjänster en leverantör av tjänster för identifieringsförmedling eller en leverantör av identifieringsverktyg,

4) leverantör av identifieringsverktyg en tjänsteleverantör som tillhandahåller eller ger ut identifieringsverktyg för stark autentisering till allmänheten samt tillhandahåller sitt identifieringsverktyg till leverantörer av tjänster för identifieringsförmedling för förmedling i förtroendenätet,

5) leverantör av tjänster för identifieringsförmedling en tjänsteleverantör som förmedlar identifieringstransaktioner baserade på stark autentisering till en part som förlitar sig på en elektronisk identifiering,

6) innehavare av identifieringsverktyg en fysisk eller juridisk person som enligt avtal

ett identifieringsverktyg av en leverantör av identifieringstjänster,

6) *inledande identifiering* verifiering av identiteten hos den som ansöker om ett identifieringsverktyg, när verifieringen sker i samband med att verktyget skaffas,

7) *certifikat* ett intyg i elektronisk form som verifierar identiteten eller verifierar identiteten och kopplar ihop signaturverifieringsdata med en undertecknare och som kan användas vid stark autentisering och elektroniska signaturer,

8) *certifikatutfärdare* en fysisk eller juridisk person som tillhandahåller allmänheten certifikat,

9) *elektronisk signatur* data i elektronisk form som är fogade eller logiskt knutna till andra elektroniska data och som används som ett instrument för verifiering av undertecknarens identitet,

10) *avancerad elektronisk* signatur en elektronisk signatur som

a) entydigt är knuten till undertecknaren,

b) gör det möjligt att identifiera undertecknaren,

c) är skapad med en metod som endast undertecknaren kontrollerar, och

d) är knuten till andra elektroniska data på ett sådant sätt att eventuella senare förvanskningar av dessa data kan upptäckas,

11) *signaturframställningsdata* unika data, såsom koder eller privata nycklar, som undertecknaren använder för att skapa en elektronisk signatur,

12) *anordning för signaturframställning* programvara eller maskinvara för användning av signaturframställningsdata då en elektronisk signatur skapas, (20.2.2015/139)

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.

har fått ett identifieringsverktyg av en leverantör av identifieringstjänster,

7) inledande identifiering verifiering av identiteten hos den som ansöker om ett identifieringsverktyg, när verifieringen sker i samband med att verktyget skaffas,

8) certifikat ett intyg i elektronisk form som verifierar identiteten eller verifierar identiteten och kopplar ihop autentiseringsuppgifter för en betrodd tjänst med en användare av tjänsten och som kan användas vid stark autentisering och betrodda tjänster,

9) certifikatutfärdare en fysisk eller juridisk person som tillhandahåller allmänheten certifikat,

10) förtroendenätet de leverantörer av identifieringstjänster som har gjort en anmälan till Kommunikationsverket.

11) organ för bedömning av överensstämmelse ett av Kommunikationsverket godkänt organ enligt artikel 2.13 i Europaparlamentets och rådets förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93, som är ackrediterat i enlighet med den förordningen.

Termerna elektronisk underskrift, betrodd tjänst, avancerad elektronisk underskrift, system för elektronisk identifiering och förlitande part har i denna lag samma betydelse som i artikel 3 i EU:s förordning om elektronisk identifiering.

2 kap	2 kap.
Rättsverkningar och behandling av personuppgifter	***Lagens tvingande natur och behandling av personuppgifter***
4 §	Upphävs
Elektroniska signaturer som skapas med identifieringsverktyg	
Elektroniska signaturer och avancerade elektroniska signaturer kan skapas med identifieringsverktyg på det sätt som verktygens egenskaper tillåter, om inte något annat föreskrivs på något annat ställe i lag eller i 18 §.	
5 §	Upphävs
Rättshandlingar	
Identifieringsverktyg får användas vid rättshandlingar, om inte något annat föreskrivs på något annat ställe i lag eller i 18 §. *Om en rättshandling enligt lag kräver underskrift, uppfylls detta krav åtminstone genom en sådan avancerad elektronisk signatur som baserar sig på ett kvalificerat certifikat och har skapats med en säker anordning för signaturframställning. Elektroniska signaturer ska dock inte förvägras rättslig verkan enbart på den grunden att de har skapats på något annat sätt än vad som anges ovan.* *I fråga om användningen av elektroniska signaturer inom förvaltningen föreskrivs särskilt.*	
6 §	6 §
Behandling av personuppgifter	*Behandling av personuppgifter*
De personuppgifter som behövs när identifieringsverktyg ges ut och tjänster upprätthålls och för identifieringstransaktioner får leverantörer av identifieringstjänster behandla på de grunder som anges i 8 § 1 mom. 1 och 2 punkten i personuppgiftslagen (523/1999). På samma grunder får certifikatutfärdare som tillhandahåller elektroniska signaturer behandla de personuppgifter som	Leverantörer av identifieringstjänster får på de grunder som anges i 8 § 1 mom. 1 och 2 punkten i personuppgiftslagen (523/1999) behandla personuppgifter som behövs när identifieringsverktyg ges ut, tjänster upprätthålls och identifieringstransaktioner genomförs. På samma grunder får certifikatutfärdare som tillhandahåller *betrodda tjänster* behandla de personuppgifter som behövs vid

behövs vid utfärdandet och upprätthållandet av certifikat. I det syfte som anges ovan får leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller elektroniska signaturer dessutom inhämta personuppgifter från personen själv.	utfärdandet och upprätthållandet av certifikat samt inhämta personuppgifter från personen själv.
	En leverantör av tjänster för identifieringsförmedling har rätt att när en sådan tjänst tillhandahålls överlåta personuppgifter till en part som förlitar sig på en elektronisk identifiering, om den förlitande parten enligt lag har rätt att behandla personuppgifter.
Personuppgifter får behandlas i andra än i 1 mom. nämnda syften endast på de grunder som avses i 8 § 1 mom. 1 punkten i personuppgiftslagen.	Personuppgifter får behandlas i andra än i 1 mom. nämnda syften endast på de grunder som anges i 8 § 1 mom. 1 punkten i personuppgiftslagen.
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. (20.2.2015/139)	När leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller *betrodda tjänster* kontrollerar sökandens identitet ska de kräva att sökanden uppger sin personbeteckning. Leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller *betrodda tjänster* får behandla personbeteckningar i sina register i de syften som nämns i 1 mom. Identifieringsverktyg och certifikat får innehålla en 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.
I övrigt föreskrivs det om behandlingen av personuppgifter i 19, 24, 30, 37 och 38 § och i personuppgiftslagen.	Bestämmelser om behandlingen av personuppgifter finns dessutom i 19 och 24 och i personuppgiftslagen§.
7 §	7 §
Användning av uppgifter i befolkningsdatasystemet	*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.	Leverantörer av identifierings*verktyg* och certifikatutfärdare som tillhandahåller *betrodda tjänster* ska hämta och uppdatera de uppgifter som de behöver för tillhandahållandet av identifieringstjänster *för fysiska personer* med användning av befolkningsdatasystemet. Leverantörer av identifieringstjänster ska dessutom säkerställa att de uppgifter som de behöver för tillhandahållandet av identifieringstjänster är uppdaterade enligt uppgifterna i befolkningsdatasystemet.

7 a §

Användning av uppgifter i företags- och organisationsregister

Leverantörer av identifieringsverktyg och certifikatutfärdare som tillhandahåller betrodda tjänster ska hämta och uppdatera de uppgifter som de behöver för tillhandahållandet av identifieringstjänster för juridiska personer med användning av företags- och organisationsregistren. Leverantörer av identifieringstjänster ska dessutom säkerställa att de uppgifter som de behöver för tillhandahållandet av identifieringstjänster är uppdaterade enligt uppgifterna i företags- och organisationsregistren.

8 §

Krav som gäller identifieringsmetoden

Identifieringsmetoden ska uppfylla följande krav:

1) metoden ska grunda sig på en inledande identifiering enligt 17 § så att uppgifterna om den kan kontrolleras i efterskott i enlighet med 24 §,

2) metoden ska medge entydig identifiering av innehavaren av identifieringsverktyget,

3) det ska med tillräckligt hög tillförlitlighet gå att säkerställa att endast innehavaren av identifieringsverktyget kan använda verktyget, och

4) metoden ska vara tillräckligt säker och tillförlitlig med tanke på de informationssäkerhetsrisker som är förknippade med den teknik som används.

Bestämmelserna i 1 mom. hindrar inte att specifika tjänster tillhandahålls så att leverantören av identifieringstjänster meddelar den tjänsteleverantör som använder en identifieringstjänst den pseudonym som innehavaren av identifieringsverktyget använder eller endast ett begränsat antal personuppgifter.

Kommunikationsverket kan utfärda närmare tekniska föreskrifter om de krav som avses i 1 mom.

8 §

Krav på system för elektronisk identifiering

Ett system för elektronisk identifiering ska uppfylla följande krav:

1) identifieringsmetoden grundar sig på en identifiering enligt 17 och 17 a § så att uppgifterna om den kan kontrolleras i efterskott i enlighet med 24 §,

2) identifieringsmetoden medger entydig identifiering av innehavaren av identifieringsverktyget så att åtminstone de villkor uppfylls som gäller för tillitsnivån väsentlig enligt avsnitten 2.1.2, 2.1.3 och 2.1.4 i bilagan till kommissionens genomförandeförordning (EU) 2015/1502 om fastställande av tekniska minimispecifikationer och förfaranden för tillitsnivåer för medel för elektronisk identifiering i enlighet med artikel 8.3 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden, nedan förordningen om tillitsnivåer vid elektronisk identifiering,

3) med hjälp av identifieringsmetoden går det att säkerställa att endast innehavaren av identifieringsverktyget kan använda verktyget på ett sådant sätt att åtminstone de villkor uppfylls som gäller för tillitsnivån väsentlig enligt avsnitten 2.2.1 och 2.3 i bilagan till

förordningen om tillitsnivåer vid elektronisk identifiering,

4) identifieringssystemet är säkert och tillförlitligt på ett sådant sätt att åtminstone de villkor uppfylls som gäller för tillitsnivån väsentlig enligt avsnitten 2.2.1, 2.3.1 och 2.4.6 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering, med hänsyn till de informationssäkerhetsrisker som är förknippade med den teknik som används vid tidpunkten, och de lokaler som används för tillhandahållandet av identifieringstjänsten är säkra på det sätt som anges i avsnitt 2.4.5 i bilagan till den förordningen,

5) ledningen avseende informationssäkerheten sköts på ett sådant sätt att de villkor uppfylls som anges i i det inledande stycket i avsnitt 2.4 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering och åtminstone de villkor uppfylls som gäller för tillitsnivån väsentlig eller högre enligt avsnitt 2.4.3 och 2.4.7 i bilagan till den förordningen

Bestämmelserna i 1 mom. hindrar inte att specifika tjänster tillhandahålls så att leverantören av identifieringstjänster meddelar den tjänsteleverantör som använder en identifieringstjänst den pseudonym som innehavaren av identifieringsverktyget använder eller endast ett begränsat antal personuppgifter.

8 a §

Autentiseringsfaktorer som ska användas i identifieringsmetoden

I en identifieringsmetod ska minst två av följande autentiseringsfaktorer användas:

1) en kunskapsbaserad autentiseringsfaktor som personen måste kunna visa att den har kunskap om,

2) en innehavsbaserad autentiseringsfaktor som personen måste kunna visa att den innehar,

3) en egenskapsbaserad autentiseringsfaktor som utgår från en kroppslig egenskap hos en fysisk person.

I varje identifieringsmetod ska det i enlighet med avsnitt 2.3.1 i bilagan till förordningen om tillitsnivåer vid elektronisk identi-

fiering användas en sådan dynamisk autentisering som kan ändras vid varje ny autentisering mellan en person och det system som kontrollerar personens identitet.

9 §

Krav som gäller leverantörer av identifieringstjänster

Fysiska personer i egenskap av leverantörer av identifieringstjänster eller fysiska personer som handlar för deras räkning samt ledamöter eller suppleanter i styrelsen eller förvaltningsrådet för en sammanslutning eller stiftelse som är tjänsteleverantör, liksom dess verkställande direktör och ansvariga bolagsmän eller andra personer i motsvarande ställning ska uppfylla följande krav:

1) de ska ha uppnått myndighetsålder,

2) de får inte vara försatta i konkurs, och

3) de får inte ha begränsad handlingsbehörighet.

9 §

Krav som gäller leverantörer av identifieringstjänster

Juridiska personer som fungerar som leverantörer av identifieringstjänster och fysiska personer som handlar för deras räkning samt ledamöter eller ersättare i styrelsen eller förvaltningsrådet för en sammanslutning eller stiftelse som är tjänsteleverantör, liksom dess verkställande direktör och ansvariga bolagsmän andra personer i motsvarande ställning ska uppfylla följande krav:

1) de ska ha uppnått myndighetsålder,

2) de får inte vara försatta i konkurs,

3) de får inte ha begränsad handlingsbehörighet.

10 §

Skyldighet för leverantörer av identifieringstjänster att anmäla att verksamheten inleds

En leverantör av identifieringstjänster som är etablerad i Finland ska göra en skriftlig anmälan till Kommunikationsverket innan verksamheten inleds. Anmälan kan också göras av en sådan sammanslutning av tjänsteleverantörer som administrerar en tjänst som ska betraktas som en enda identifieringstjänst.

Anmälan ska innehålla

1) tjänsteleverantörens namn,

2) tjänsteleverantörens fullständiga kontaktuppgifter,

3) uppgifter om de tjänster som tillhandahålls,

4) uppgifter om de omständigheter som avses i 8, 9, 13 och 14 §, och

5) övriga uppgifter som behövs för tillsynen.

Leverantören av identifieringstjänster ska utan dröjsmål skriftligen underrätta Kommunikationsverket om förändringar av de upp-

10 §

Skyldighet för leverantörer av identifieringstjänster att anmäla att verksamheten inleds

En leverantör av identifieringstjänster som är etablerad i Finland ska göra en skriftlig anmälan till Kommunikationsverket innan verksamheten inleds. Anmälan kan också göras av en sådan sammanslutning av leverantörer av identifieringsverktyg som administrerar en tjänst som ska betraktas som en enda identifieringstjänst.

Anmälan ska innehålla

1) tjänsteleverantörens namn,

2) tjänsteleverantörens fullständiga kontaktuppgifter,

3) uppgifter om de tjänster som tillhandahålls,

4) utredning om att kraven i 8, 8 a, 9, 13 och 14 § uppfylls med avseende på sökanden och sökandens verksamhet,

5) en inspektionsberättelse om oberoende bedömning i enlighet med 29 § utarbetad av ett organ för bedömning av överensstämmelse, något annat utomstående bedöm-

gifter som avses i 2 mom. Anmälan ska också göras när verksamheten avslutas eller funktionerna överförs till en annan tjänsteleverantör.

Kommunikationsverket kan utfärda för tillsynen behövliga tekniska föreskrifter om det närmare innehållet i de uppgifter enligt denna paragraf som ska anmälas och om inlämnandet av dem till Kommunikationsverket.

13 §

Allmänna skyldigheter för leverantörer av identifieringstjänster

Leverantören av identifieringstjänster ska se till att de anställda har tillräcklig sakkunskap, erfarenhet och kompetens med tanke på verksamhetens omfattning.

— — — — — — — — — — — — — —

ningsorgan eller ett internt kontrollorgan,

6) övriga uppgifter som behövs för tillsynen.

Leverantören av identifieringstjänster ska utan dröjsmål skriftligen underrätta Kommunikationsverket om ändringar i de uppgifter som avses i 2 mom. Anmälan ska också göras när verksamheten avslutas eller funktionerna överförs till en annan tjänsteleverantör.

13 §

Allmänna skyldigheter för leverantörer av identifieringstjänster

Hos leverantörer av identifieringstjänster ska lagringen av uppgifter som sammanhänger med identifieringen, personalen och de tjänster som köps av underleverantörer uppfylla åtminstone kraven för tillitsnivån väsentlig enligt avsnitten 2.4.4 och 2.4.5 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering. Leverantörer av identifieringstjänster ska dessutom ha en omfattande plan för identifieringstjänstens upphörande.

— — — — — — — — — — — — — —

14 §

Principer för identifiering

Leverantören av identifieringstjänster ska ha principer för identifiering som närmare anger hur tjänsteleverantören uppfyller de skyldigheter som avses i denna lag. Det ska i synnerhet anges närmare hur leverantören utför den inledande identifieringen enligt 17 §.

Principerna för identifiering ska dessutom innehålla de viktigaste uppgifterna om

1) tjänsteleverantören,

2) de tjänster som tillhandahålls och priserna på dem,

3) tjänsteleverantörens viktigaste samarbetspartner,

4) de kontroller som har utförts av utomstående bedömningsorgan, och

5) andra omständigheter som är av betydelse för att tjänsteleverantörens verksamhet och tillförlitlighet ska kunna bedömas.

14 §

Principer för identifiering

Leverantörer av identifieringstjänster ska ha principer för identifiering som närmare anger hur tjänsteleverantören uppfyller de skyldigheter som anges i denna lag. Det ska i synnerhet anges närmare hur leverantören av identifieringsverktyg genomför den identifiering som avses i 17 och 17 a § när identifieringsverktyg beviljas.

Principerna för identifiering ska dessutom innehålla de viktigaste uppgifterna om

1) tjänsteleverantören,

2) de tjänster som tillhandahålls och priserna på dem,

3) samtliga villkor som tillämpas,

4) de principer för informationssäkerhet som tillämpas i tjänsten,

5) tjänsteleverantörens viktigaste samarbetspartner,

— — — — — — — — — — — — — — —

6) bedömningen av överensstämmelse enligt 29 §,

7) andra omständigheter som är av betydelse för att tjänsteleverantörens verksamhet och tillförlitlighet ska kunna bedömas.

Om elektroniska underskrifter eller avancerade elektroniska underskrifter kan skapas med ett identifieringsverktyg ska leverantören av identifieringstjänster också lämna uppgifter om hur och på vilken nivå de elektroniska underskrifterna tillhandahålls samt om säkerhetsfaktorerna i fråga om underskrifterna.

Leverantören av identifieringstjänster ska hålla principerna för identifiering allmänt tillgängliga och uppdaterade.

— — — — — — — — — — — — — — —

15 §

Skyldighet för leverantörer av identifieringstjänster att lämna uppgifter innan avtal ingås

Leverantören av identifieringstjänster ska innan ett avtal ingås informera den som ansöker om ett identifieringsverktyg om

— — — — — — — — — — — — — — —

15 §

Skyldighet för leverantörer av identifieringsverktyg att lämna uppgifter innan avtal ingås

En leverantör av identifierings*verktyg* ska innan ett avtal ingås informera den som ansöker om ett identifieringsverktyg om

— — — — — — — — — — — — — — —

16 §

Skyldighet för leverantörer av identifieringstjänster att anmäla hot och störningar som riktas mot informationssäkerheten eller skyddet av uppgifter

Leverantören av identifieringstjänster ska utan onödigt dröjsmål anmäla betydande hot och störningar som riktas mot tjänsternas informationssäkerhet till de tjänsteleverantörer som använder tjänsterna, innehavarna av identifieringsverktyg och Kommunikationsverket.

Om hotet eller störningen riktas mot det skydd av uppgifter som avses i 32 § i personuppgiftslagen, ska leverantören av identifieringstjänster förutom till de aktörer som avses i 1 mom. även anmäla saken till dataombudsmannen.

I anmälan ska också redogöras för de åtgärder som de olika aktörerna kan vidta för

16 §

Skyldighet för leverantörer av identifieringstjänster att anmäla hot och störningar som riktas mot verksamheten eller skyddet av uppgifter

En leverantör av identifieringstjänster ska utan ogrundat dröjsmål anmäla betydande hot och störningar som riktas mot tjänsternas funktion, informationssäkerheten eller användningen av en elektronisk identitet till de tjänsternas förlitande parter, till innehavarna av identifieringsverktyg, till övriga avtalsparter i förtroendenätet och till Kommunikationsverket. Kommunikationsverket får för anmälarens räkning på teknisk väg förmedla uppgifterna mellan parterna i förtroendenätet trots vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet (621/1999).

Om hotet eller störningen är riktat mot

att avvärja hoten eller störningarna, och för de beräknade kostnaderna för dessa åtgärder.

skydd av uppgifter som avses i 32 § i personuppgiftslagen, ska leverantören av identifieringstjänster även underrätta dataombudsmannen om saken.

I en anmälan enligt 1 mom. ska det redogöras för de åtgärder som olika aktörer har tillgång till för att avvärja hot eller störningar samt de beräknade kostnaderna för åtgärderna.

En leverantör av identifieringstjänster får använda sådana uppgifter om en annan leverantör av identifieringstjänster som den fått med stöd av denna paragraf endast för att skapa beredskap för de hot och störningar som avses i denna paragraf. Hos en leverantör av identifieringstjänster får uppgifterna behandlas endast av den personal som nödvändigt behöver uppgifterna i sitt arbete. Uppgifterna ska också annars behandlas så att affärshemligheter som tillhör en annan leverantör av identifieringstjänster inte röjs.

En leverantör av identifieringstjänster som genom att handla i strid med 4 mom. vållar en annan leverantör av identifieringstjänster skada är skyldig att ersätta för skadan.

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

17 §

Identifiering av en fysisk person som ansöker om ett identifieringsverktyg

Vid inledande identifiering ska identifieringen av en fysisk person göras personligen eller elektroniskt på ett sådant sätt att de krav uppfylls som gäller för tillitsnivån väsentlig eller hög enligt avsnitt 2.1.2 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering. Kontrollen av en persons identitet kan grunda sig på en identitetshandling som utfärdats av en myndighet eller ett sådant identifieringsverktyg för stark autentisering som avses i denna lag. Kontrollen av identiteten kan dessutom grunda sig på ett förfarande som en offentlig eller privat aktör tidigare och i annat syfte än för beviljande av ett identifieringsverktyg för stark autentisering har använt sig av och som Kommunikationsverket godkänner utifrån de bestämmelser som gäller förfarandet och utifrån myndighetstillsynen eller utifrån en bekräftelse av ett i 28 § 1 punkten avsett organ för bedömning av överensstämmelse.

annan stat.	*Dokument som godkänns vid inledande identifiering, när identifieringen endast sker utifrån en identitetshandling som utfärdats av en myndighet, är ett giltigt pass eller identitetskort som har utfärdats av en myndighet i en medlemsstat inom Europeiska ekonomiska samarbetsområdet, i Schweiz eller i San Marino. En leverantör av identifieringsverktyg som så önskar kan också vid kontrollen av identiteten använda ett giltigt pass som har utfärdats av en myndighet i någon annan stat.*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
	17 a §
	Identifiering av en juridisk person som ansöker om ett identifieringsverktyg
	Den identitet som uppgetts av en juridisk person ska kontrolleras med användning av företags- och organisationsregistren eller på ett sådant sätt att åtminstone de krav på styrkande och kontroll av juridiska personers identitet uppfylls som gäller för tillitsnivån väsentlig enligt avsnitt 2.1.3 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering.
19 §	19 §
Certifikatets innehåll	*Certifikatets innehåll*
Om identifieringsmetoden grundar sig på ett certifikat, ska certifikatet åtminstone innehålla	Om identifieringsmetoden grundar sig på ett certifikat, ska certifikatet åtminstone innehålla
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
8) certifikatutfärdarens avancerade elektroniska signatur.	8) certifikatutfärdarens avancerade elektroniska *underskrift*.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
20 §	20 §
Utgivning av identifieringsverktyg	*Beviljande av identifieringsverktyg*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Identifieringsverktyg tillhandahålls endast	*Identifieringsverktyg beviljas endast fysiska*

fysiska personer. Identifieringsverktyg ska vara personliga. Till ett verktyg kan vid behov fogas en uppgift om att en person i enskilda fall även kan företräda en annan fysisk person eller en juridisk person.

och juridiska personer. Bindningen mellan en fysisk persons och en juridisk persons identifieringsverktyg ska genomföras i enlighet med avsnitt 2.1.4 i förordningen om tillitsnivåer vid elektronisk identifiering. Ett identifieringsverktyg ska vara personligt. Till ett identifieringsverktyg kan det vid behov fogas en uppgift om att innehavaren av identifieringsverktyget i enskilda fall även får företräda en annan fysisk person eller en juridisk person.

21 §

Överlåtelse av identifieringsverktyg till sökande

Leverantören av identifieringstjänster ska överlåta identifieringsverktyget till den sökande på det sätt som anges i avtalet. Leverantören ska på ett tillräckligt sätt säkerställa att verktyget inte obehörigt kommer i någon annans besittning vid överlåtelsen.

21 §

Överlåtelse av identifieringsverktyg till sökande

Leverantören av ett identifieringsverktyg ska överlåta identifieringsverktyget till sökanden på det sätt som anges i avtalet. Leverantören ska säkerställa att verktyget inte obehörigt kommer i någon annans besittning vid överlåtelsen, på ett sådant sätt att åtminstone de krav uppfylls som gäller för tillitsnivån väsentlig enligt avsnitt 2.2.2 i förordningen om tillitsnivåer vid elektronisk identifiering.

22 §

Förnyande av identifieringsverktyg

Leverantören av identifieringstjänster får leverera ett nytt verktyg till en innehavare av ett identifieringsverktyg utan en uttrycklig begäran endast om ett verktyg som tidigare har tillhandahållits ska ersättas med ett nytt. Vid leveransen ska bestämmelserna i 21 § iakttas.

22 §

Förnyande av identifieringsverktyg

En leverantör av identifieringsverktyg får leverera ett nytt verktyg till en innehavare av identifieringsverktyg utan en uttrycklig begäran om det endast om ett verktyg som tidigare har tillhandahållits ska ersättas med ett nytt. När identifieringsverktyg förnyas ska de krav uppfyllas som gäller för tillitsnivån väsentlig enligt avsnitt 2.2.4 i förordningen om tillitsnivåer vid elektronisk identifiering.

24 §

Registrering och användning av uppgifter om identifieringstransaktioner och identifieringsverktyg

Leverantörer av identifieringstjänster ska registrera

24 §

Registrering och användning av uppgifter om identifieringstransaktioner och identifieringsverktyg

Leverantörer av identifieringstjänster ska registrera

1) de uppgifter som behövs för att verifiera en enskild identifieringstransaktion och elektronisk signering,

2) de uppgifter som behövs om den inledande identifiering av en sökande som avses i 17 § och om den handling som anlitats för identifieringen,

3) uppgifter om sådana eventuella hinder och begränsningar för användningen av verktyget som avses i 18 §, och

4) i fråga om certifikat, uppgifter om certifikatets innehåll enligt 19 §.

De uppgifter som avses i 1 mom. 1 punkten ska förvaras i fem år från identifieringstransaktionen. De uppgifter som avses i 1 mom. 2–4 punkten ska förvaras i fem år från det att kundförhållandet mellan leverantören av identifieringstjänster och innehavaren av ett identifieringsverktyg upphörde.

De personuppgifter som har samlats in i samband med en identifieringstransaktion ska förstöras efter transaktionen, om det inte är nödvändigt att registrera dem för att verifiera en enskild identifieringstransaktion.

Leverantören av identifieringstjänster får behandla registrerade uppgifter endast för att tillhandahålla och upprätthålla tjänsterna, utföra fakturering och trygga sina rättigheter vid tvister samt på begäran av en tjänsteleverantör som använder identifieringstjänster eller en innehavare av ett identifieringsverktyg. Leverantören av identifieringstjänster ska registrera uppgifter om när och varför uppgifterna behandlats och vem som gjort det.

Vad som föreskrivs i 1 mom. 1 punkten och 3 mom. gäller inte tjänsteleverantörer som endast ger ut identifieringsverktyg. Den förvaringstid på fem år som avses i 2 mom. räknas då från det att identifieringsverktyget upphörde att gälla.

1) de uppgifter som behövs för att verifiera en enskild identifieringstransaktion eller elektronisk underskrift,

2) uppgifter om i 18 § avsedda hinder och begränsningar som gäller användningen av identifieringsverktyg,

3) i fråga om certifikat, uppgifter om certifikatets innehållet i certifikat enligt 19 §.

Leverantörer av identifieringsverktyg ska registrera behövliga uppgifter om den inledande identifiering av sökande som avses i 17 och 17 a § och om de handlingar eller den elektroniska identifiering som använts i den inledande identifieringen.

De uppgifter som avses i 1 mom. 1 punkten ska lagras i fem år från identifieringstransaktionen. De övriga uppgifter som avses i 1 och 2 mom. ska lagras i fem år från det att ett fast kundförhållande har upphört.

Personuppgifter som har uppkommit i samband med en identifieringstransaktion ska förstöras efter transaktionen, om det inte är nödvändigt att registrera dem för att verifiera en enskild identifieringstransaktion.

Leverantören av identifieringstjänster får behandla registrerade uppgifter endast för att tillhandahålla och upprätthålla tjänsterna, fakturera, trygga sina rättigheter vid tvister och utreda missbruk samt på begäran av en tjänsteleverantör som använder identifieringstjänster eller en innehavare av ett identifieringsverktyg. Leverantören av identifieringstjänster ska registrera uppgifter om när och varför uppgifterna behandlats och vem som gjort det.

Om en tjänsteleverantör endast ger ut identifieringsverktyg

1) tillämpas inte 1 mom. 1 punkten och 4 mom. på tjänsteleveratören,

2) räknas den registreringstid på fem år som avses i 3 mom. från det att identifieringsverktyget upphörde att gälla.

25 §

Anmälan om återkallande eller förhindrande av användning av identifieringsverktyg

Innehavaren av ett identifieringsverktyg ska anmäla till leverantören av identifieringstjänster eller någon annan aktör som denne har utsett att verktyget har försvunnit, obehö-

25 §

Anmälan om återkallande eller förhindrande av användning av identifieringsverktyg

Innehavaren av ett identifieringsverktyg ska utan obefogat dröjsmål göra en anmälan till leverantören av identifieringsverktyget, eller någon annan aktör som denne har utsett,

rigt har kommit i någon annans besittning eller obehörigt har använts. Anmälan ska göras utan obefogat dröjsmål efter det att saken har upptäckts.

Leverantören av identifieringstjänster ska se till att det är möjligt att när som helst göra en anmälan enligt 1 mom. Leverantören ska utan dröjsmål återkalla verktyget eller förhindra att det används efter det att anmälan har mottagits.

Leverantören av identifieringstjänster ska på lämpligt sätt och utan dröjsmål i systemet registrera uppgift om tidpunkten för återkallandet eller förhindrandet av användningen. Innehavaren av ett identifieringsverktyg har rätt att på begäran få ett intyg över att han eller hon har gjort anmälan enligt 1 mom. Intyget ska begäras inom 18 månader från anmälan.

— — — — — — — — — — — — — — —

om verktyget har förkommit, obehörigen har kommit i någon annans besittning eller obehörigen har använts. Anmälan ska göras utan obefogat dröjsmål efter det att saken har upptäckts.

Leverantören av identifierings*verktyg* ska se till att det är möjligt att när som helst göra en anmälan enligt 1 mom. Leverantören ska utan dröjsmål återkalla identifieringsverktyget eller förhindra dess användning efter det att anmälan har mottagits.

Leverantören av ett identifierings*verktyg* ska på lämpligt sätt och utan dröjsmål i systemet registrera uppgifter om tidpunkten för återkallandet eller förhindrandet av användningen. Innehavaren av identifieringsverktyget har rätt att på begäran få ett intyg över att innehavaren har gjort den anmälan som avses i 1 mom. Intyget ska begäras inom 18 månader från anmälan

— — — — — — — — — — — — — — —

26 §

Rätten för leverantörer av identifieringstjänster att återkalla eller förhindra användning av identifieringsverktyg

Utöver vad som föreskrivs i 25 § får leverantören av identifieringstjänster återkalla eller förhindra användningen av ett identifieringsverktyg, om

1) leverantören av identifieringstjänster har skäl att misstänka att verktyget används av någon annan än den som identifieringsverktyget har getts ut till,

2) verktyget innehåller ett uppenbart fel,

3) leverantören av identifieringstjänster har skäl att misstänka att säkerheten vid användningen av verktyget har äventyrats,

4) innehavaren av ett identifieringsverktyg använder verktyget på ett sätt som väsentligt strider mot avtalsvillkoren, eller

5) innehavaren av identifieringsverktyget har avlidit.

Leverantören av identifieringstjänster ska så snart som möjligt underrätta innehavaren om att identifieringsverktyget har återkallats eller användningen av det förhindrats och ange när och varför återkallandet eller förhindrandet skett.

Leverantören av identifieringstjänster ska erbjuda en ny möjlighet att använda identifie-

26 §

Rätten för leverantörer av identifieringsverktyg att återkalla eller förhindra användning av identifieringsverktyg

Utöver vad som föreskrivs i 25 § får leverantören av ett identifieringsverktyg återkalla eller förhindra användningen av identifieringsverktyget, om

1) leverantören har skäl att misstänka att identifieringsverktyget används av någon annan än den som det har beviljats till,

2) identifieringsverktyget innehåller ett uppenbart fel,

3) leverantören har skäl att misstänka att säkerheten vid användningen av identifieringsverktyget har äventyrats,

4) innehavaren av identifieringsverktyget använder det på ett sätt som väsentligt strider mot avtalsvillkoren,

5) innehavaren av identifieringsverktyget har avlidit.

Leverantören av identifieringsverktyget ska så snart som möjligt underrätta innehavaren av identifieringsverktyget om att identifieringsverktyget har återkallats eller användningen av det förhindrats samt om tidpunkten för och orsakerna till detta.

ringsverktyg eller tillhandahålla innehavaren ett nytt verktyg omedelbart efter det att en sådan orsak som avses 1 mom. 2 och 3 punkten inte längre föreligger.

Leverantören av identifieringsverktyget ska erbjuda en ny möjlighet att använda identifieringsverktyget eller tillhandahålla innehavaren ett nytt verktyg omedelbart efter det att en sådan orsak som avses 1 mom. 2 eller 3 punkten inte längre föreligger.

4 kap

Elektroniska signaturer

4 kap.

Bedömning av överensstämmelse

28 §

Säkra anordningar för signaturframställning

En säker anordning för signaturframställning ska på ett tillräckligt tillförlitligt sätt säkerställa att

1) signaturframställningsdata i praktiken kan förekomma endast en gång och att de förblir konfidentiella,

2) signaturframställningsdata inte kan härledas ur andra data,

3) signaturen är skyddad mot förfalskning,

4) undertecknaren kan skydda signaturframställningsdata så att andra inte kan använda dem, och

5) anordningen inte förändrar de uppgifter som ska signeras eller hindrar att de presenteras för undertecknaren före signeringen.

En anordning för signaturframställning anses alltid uppfylla kraven i 1 mom., om

1) den överensstämmer med de allmänt erkända standarder som Europeiska gemenskapernas kommission har fastställt och som har offentliggjorts i Europeiska unionens officiella tidning, eller

2) ett kontrollorgan, beläget i Finland eller i en annan stat inom Europeiska ekonomiska samarbetsområdet, som har utsetts för att bedöma om kraven uppfylls har godkänt anordningen.

28 §

Organ för bedömning av överensstämmelse

Överensstämmelsen hos en tjänst enligt detta kapitel kan bedömas av följande bedömningsorgan

1) ett organ för bedömning av överensstämmelse,

2) ett annat utomstående bedömningsorgan som är verksamt enligt en allmänt använd metod (annat utomstående bedömningsorgan), eller

3) ett oberoende bedömningsorgan inom tjänsteleverantörens organisation som uppfyller en allmänt använd standard (internt kontrollorgan).

29 §

Kontrollorgan

Kommunikationsverket kan utse kontrollorgan med uppgift att bedöma om anordningar för signaturframställning uppfyller

29 §

Bedömning av överensstämmelse hos en elektronisk identifieringstjänst

En leverantör av identifieringstjänster ska regelbundet låta ett sådant bedömningsorgan

kraven i 28 § 1 mom. Kontrollorganen kan vara privata eller offentliga inrättningar.

En inrättning kan utses till kontrollorgan under förutsättning att

1) den är oberoende i fråga om sin verksamhet och ekonomi,

2) dess verksamhet är tillförlitlig, ändamålsenlig och icke-diskriminerande,

3) den har tillräckliga ekonomiska resurser för att ordna verksamheten ändamålsenligt och täcka ett eventuellt ersättningsansvar,

4) den har tillgång till yrkeskunnig och opartisk personal i den omfattning som behövs, och

5) den har tillgång till sådana lokaler och sådan utrustning som verksamheten kräver.

Kommunikationsverket utser kontrollorganen på ansökan. Ansökan ska utöver sökandens kontaktuppgifter och handelsregisterutdrag eller motsvarande utredning innehålla uppgift om huruvida sökandens verksamhet uppfyller kraven i 2 mom. Kommunikationsverket meddelar vid behov anvisningar om de uppgifter som ska ingå i ansökan och om inlämnandet av dem till Kommunikationsverket.

Kommunikationsverket övervakar kontrollorganens verksamhet. Om ett kontrollorgan inte uppfyller fastställda krav eller om det bryter mot bestämmelserna, ska Kommunikationsverket återkalla beslutet genom vilket det utsett kontrollorganet. Kontrollorganen ska underrätta Kommunikationsverket om sådana ändringar i verksamheten som inverkar på förutsättningarna för att bli utsedd till kontrollorgan.

Vid bedömningen av anordningar kan kontrollorganet anlita utomstående personer. Kontrollorganet svarar också för det arbete som dessa utför.

som nämns i 28 § bedöma om identifieringstjänsten uppfyller kraven på interoperabilitet, informationssäkerhet, dataskydd och annan tillförlitlighet enligt denna lag.

Bestämmelser om bedömning av överensstämmelse hos system för elektronisk identifiering som ska anmälas till Europeiska kommissionen finns i EU:s förordning om elektronisk identifiering och i förordningen om tillitsnivåer vid elektronisk identifiering.

Bestämmelser om Kommunikationsverkets rätt att meddela närmare föreskrifter om bedömningsgrunderna vid bedömningen av överensstämmelsen hos en identifieringstjänst finns i 42 §. Som bedömningsgrund kan Kommunikationsverket utöver de författningar och rättsakter som avses i 1 och 2 mom. fastställa bestämmelser eller riktlinjer som antagits av Europeiska unionen eller något annat internationellt organ, publicerade och generellt eller regionalt tillämpade anvisningar för informationssäkerhet samt datasäkerhetsstandarder eller förfaranden som används allmänt.

30 §

Kvalificerade certifikat

Med kvalificerat certifikat avses ett certifikat som uppfyller kraven i 2 mom. och som har utfärdats av en certifikatutfärdare som uppfyller kraven i 33–38 §.

Ett kvalificerat certifikat ska innehålla

1) uppgift om att certifikatet är ett kvalificerat certifikat,

30 §

Bedömning av överensstämmelse hos den nationella noden för elektronisk identifiering

Överensstämmelse hos det nationella gränssnitt som hör till EU:s interoperabilitetsramverk för elektronisk identifiering (den nationella noden) ska påvisas genom en bedömning som görs av ett organ för bedömning av överensstämmelse eller ett annat ut-

2) uppgift om certifikatutfärdaren och dennes etableringsstat,
3) undertecknarens namn eller pseudonym med uppgift om att det är en pseudonym,
4) signaturverifieringsdata som motsvarar de signaturframställningsdata som undertecknaren innehar,
5) det kvalificerade certifikatets giltighetstid,
6) det kvalificerade certifikatets identifieringskod,
7) certifikatutfärdarens avancerade elektroniska signatur,
8) eventuella begränsningar av användningen av det kvalificerade certifikatet, och
9) särskilda uppgifter om undertecknaren, om de behövs med tanke på ändamålet med det kvalificerade certifikatet.

Om en certifikatutfärdare som tillhandahåller kvalificerade certifikat även tillhandahåller identifieringstjänster enligt 3 kap., anses kraven i 1 mom. alltid också uppfylla de krav på certifikatets innehåll som avses i 19 § 1 mom.

omstående bedömningsorgan.

Bestämmelser om kraven på den nationella noden finns i kommissionens genomförandeförordning (EU) 2015/1501 om interoperabilitetsramverket enligt artikel 12.8 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden. Bestämmelser om Kommunikationsverkets rätt att meddela närmare föreskrifter om bedömningsgrunderna vid bedömningen av överensstämmelse hos den nationella noden finns i 42 §.

31 §

Kvalificerade certifikat som tillhandahålls av en certifikatutfärdare som inte är etablerad i Finland

Ett certifikat som anges vara kvalificerat och som tillhandahålls av en certifikatutfärdare som inte är etablerad i Finland anses uppfylla kraven på kvalificerat certifikat i denna lag, om

1) certifikatutfärdaren är etablerad i en stat inom Europeiska ekonomiska samarbetsområdet och certifikatet uppfyller etableringsstatens krav på kvalificerat certifikat,
2) certifikatutfärdaren har anslutit sig till ett frivilligt ackrediteringssystem i en stat inom Europeiska ekonomiska samarbetsområdet och uppfyller de nationella krav som i denna stat föreskrivits för genomförande av Europaparlamentets och rådets direktiv 1999/93/EG om ett gemenskapsramverk för elektroniska signaturer, nedan direktivet om elektroniska signaturer,
3) certifikatet garanteras av en certifikatutfärdare som är etablerad i en stat inom Europeiska ekonomiska samarbetsområdet och uppfyller de nationella krav som i denna stat

31 §

Inspektionsberättelse

En leverantör av identifieringstjänster och Befolkningsregistercentralen ska över bedömningen av överensstämmelse låta utarbeta en inspektionsberättelse som lämnas in till Kommunikationsverket.

Inspektionsberättelsen är i kraft den tid som anges i den standard som användes vid bedömningen, dock högst i 2 år.

föreskrivits för genomförande av direktivet om elektroniska signaturer, eller

4) certifikatet eller certifikatutfärdaren har erkänts enligt ett bilateralt eller multilateralt avtal mellan Europeiska gemenskapen och ett eller flera tredjeländer eller internationella organisationer.

32 §

Anmälan om inledande av verksamhet

En certifikatutfärdare som tillhandahåller kvalificerade certifikat ska göra en skriftlig anmälan till Kommunikationsverket innan verksamheten inleds. Anmälan ska innehålla certifikatutfärdarens namn och kontaktuppgifter samt de uppgifter som behövs för att säkerställa att kraven i 30 och 33–38 § uppfylls. Kommunikationsverket kan utfärda föreskrifter om det närmare innehållet i de uppgifter som ska lämnas och om inlämnandet av dem till Kommunikationsverket.

Kommunikationsverket ska utan dröjsmål efter det att anmälan inkommit förbjuda certifikatutfärdaren att tillhandahålla sina certifikat som kvalificerade certifikat, om certifikaten inte uppfyller kraven i 30 § 2 mom. eller om certifikatutfärdaren inte uppfyller kraven i 33–38 §.

Certifikatutfärdaren ska utan dröjsmål skriftligen underrätta Kommunikationsverket, om de uppgifter som avses i 1 mom. har förändrats.

Kommunikationsverket för ett offentligt register över certifikatutfärdare som utfärdar kvalificerade certifikat.

Certifikatutfärdare som tillhandahåller kvalificerade certifikat kan också göra en anmälan enligt 10 §, om de utöver kvalificerade certifikat även vill tillhandahålla identifieringstjänster.

32 §

Fastställande av överensstämmelse hos betrodda tjänster

Ett organ för bedömning av överensstämmelse ska inspektera en kvalificerad tillhandahållare av betrodda tjänster och överensstämmelsen hos en kvalificerad betrodd tjänst med iakttagande av bestämmelserna i EU:s förordning om elektronisk identifiering.

Bestämmelser om Kommunikationsverkets rätt att meddela närmare föreskrifter om bedömningsgrunderna vid bedömningen av överensstämmelse finns i 42 §. Som bedömningsgrund kan Kommunikationsverket fastställa bestämmelser eller riktlinjer som antagits av Europeiska unionen eller något annat internationellt organ, publicerade och generellt eller regionalt tillämpade anvisningar för informationssäkerhet samt datasäkerhetsstandarder eller förfaranden som används allmänt.

33 §

Allmänna skyldigheter för certifikatutfärdare som tillhandahåller kvalificerade certifikat

Certifikatutfärdaren ska ha tillräckliga tekniska kunskaper och ekonomiska resurser med tanke på verksamhetens omfattning. Certifikatutfärdaren svarar för alla delområden av certifikatverksamheten, även för att

33 §

Allmänna krav på bedömningsorgan

De bedömningsorgan som nämns i 28 § omfattas av följande kompetenskrav:

1) organet ska vara funktionellt och ekonomiskt oberoende av bedömningsobjektet,

2) organets personal ska ha god teknisk och yrkesinriktad utbildning samt tillräckligt

tjänster och produkter som produceras av personer som certifikatutfärdaren eventuellt anlitar är tillförlitliga och fungerar.

Certifikatutfärdaren ska

1) säkerställa att personalen har tillräcklig sakkunskap, erfarenhet och kompetens,

2) förfoga över tillräckliga ekonomiska resurser för att ordna verksamheten och täcka ett eventuellt skadeståndsansvar,

3) hålla sådana uppgifter om certifikaten och certifikatverksamheten allmänt tillgängliga som behövs för bedömande av certifikatutfärdarens verksamhet och tillförlitlighet, och

4) sörja för att signaturframställningsdata är konfidentiella då certifikatutfärdaren själv framställer dem.

Certifikatutfärdaren får inte lagra eller kopiera de signaturframställningsdata som överlåtits till en undertecknare.

omfattande erfarenhet av de uppgifter som ingår i bedömningsverksamheten,

3) organet ska förfoga över den utrustning och de lokaler, redskap och system som behövs för bedömningsverksamheten,

4) organet ska ha ändamålsenliga riktlinjer för verksamheten och uppföljningen av den.

Bestämmelser om Kommunikationsverkets rätt att meddela närmare föreskrifter om de krav som anges i 1 mom. finns i 42 §.

Ett organ för bedömning av överensstämmelse ska visa att kraven i 1 mom. 1–3 punkten är uppfyllda genom en ackreditering beviljad av den nationella ackrediteringsenheten med iakttagande av bestämmelserna i Europaparlamentets och rådets förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 och i lagen om konstaterande av tillförlitligheten hos tjänster för bedömning av överensstämmelse med kraven (920/2005).

En leverantör av identifieringstjänster ska i den anmälan som avses i 1 mom. lämna en redogörelse för att ett annat utomstående bedömningsorgan eller ett internt kontrollorgan som bedömt dess överensstämmelse uppfyller kraven enligt 1 mom. Att kraven i 1 mom. 1–3 punkten är uppfyllda ska visas genom en ackreditering enligt 2 mom. eller genom ett annat oberoende förfarande som grundar sig på en allmänt använd standard.

En ackreditering som beviljas av en utländsk ackrediteringsenhet motsvarar ett ackrediteringsbeslut enligt 3 och 4 mom.

34 §

Tillförlitlig maskinvara och programvara

En certifikatutfärdare som tillhandahåller kvalificerade certifikat ska se till att de system samt den maskinvara och programvara som används är tillräckligt säkra och tillförlitliga samt skyddade mot ändringar och mot förfalskning.

Maskinvara eller programvara avsedd för elektroniska signaturer anses alltid uppfylla kraven i 1 mom., om den överensstämmer med de allmänt erkända standarder som Europeiska gemenskapernas kommission har

34 §

Godkännande av organ för bedömning av överensstämmelse

Organ för bedömning av överensstämmelse godkänns av Kommunikationsverket. Ett organ kan godkännas för viss tid, om det finns särskilda skäl till detta. Kommunikationsverket kan förena ett beslut om godkännande med begränsningar och villkor rörande organets kompetensområde, tillsynen över organet och organets verksamhet.

fastställt och som har offentliggjorts i Europeiska unionens officiella tidning.

35 §

Utgivning av kvalificerade certifikat

En certifikatutfärdare som tillhandahåller kvalificerade certifikat ska omsorgsfullt och på ett tillförlitligt sätt kontrollera identiteten hos den som ansöker om kvalificerat certifikat och andra uppgifter som gäller sökandens person och som är relevanta för utfärdandet och upprätthållandet av det kvalificerade certifikatet. Certifikatutfärdare som tillhandahåller kvalificerade certifikat ska identifiera sökanden personligen. Utfärdaren ska bemöta sin kunder på ett icke-diskriminerande sätt och de som ansöker om certifikat jämlikt när avtalet ingås.

En certifikatutfärdare som tillhandahåller kvalificerade certifikat ska innan ett avtal ingås informera sökanden om villkoren för användning av det kvalificerade certifikatet, inbegripet eventuella begränsningar av användningen, om frivilliga ackrediteringssystem, myndighetstillsynen över verksamheten samt förfarandena för klagomål och avgörande av tvister. Informationen ska ges skriftligen i sådan form att sökanden kan förstå den utan svårighet.

36 §

Återkallande av kvalificerade certifikat

Undertecknaren ska utan dröjsmål begära att den certifikatutfärdare som utfärdat ett kvalificerat certifikat ska återkalla det, om undertecknaren har grundad anledning att anta att signaturframställningsdata används på obehörigt sätt.

En certifikatutfärdare som tillhandahåller kvalificerade certifikat ska utan dröjsmål återkalla ett kvalificerat certifikat, om undertecknaren begär det. Begäran om återkallande av ett kvalificerat certifikat anses ha inkommit till certifikatutfärdaren då den har stått till utfärdarens förfogande så att begäran kan behandlas.

Ett kvalificerat certifikat kan återkallas

35 §

Ansökan om att bli organ för bedömning av överensstämmelse

Organ för bedömning av överensstämmelse godkänns efter ansökan. Ansökan ska innehålla sådana uppgifter om sökanden och sökandens verksamhet utifrån vilka det kan avgöras om kraven i 33 § är uppfyllda.

När Kommunikationsverket behandlar en ansökan kan verket skaffa utlåtanden samt anlita utomstående experter för att bedöma ansökan och de uppgifter som ges i ansökan.

36 §

Certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter eller kvalificerade elektroniska stämplar

Kommunikationsverket får efter ansökan utse offentliga eller privata certifieringsorgan enligt artiklarna 30 och 39.2 i EU:s förordning om elektronisk identifiering som har i uppgift att certifiera anordningar för skapande av kvalificerade elektroniska underskrifter eller kvalificerade elektroniska stämplar. Certifieringsorganet kan utses för viss tid. I sin ansökan ska certifieringsorganet ange de uppgifter som Kommunikationsverket begär och som behövs för behandlingen av ansökan.

Certifieringsorganet ska vara funktionellt

också om det annars finns särskild anledning till det. Undertecknaren ska alltid underrättas om att det kvalificerade certifikatet har återkallats och om tidpunkten för återkallandet.

och ekonomiskt oberoende av tillverkarna av anordningar för skapande av elektroniska underskrifter eller elektroniska stämplar. Organet ska ha en ansvarsförsäkring som är tillräcklig med hänsyn till verksamhetens omfattning, eller något annat motsvarande arrangemang, och det ska ha tillgång till en tillräckligt stor yrkeskunnig personal och de system, den utrustning och de redskap som behövs för verksamheten.

37 §

Register som ska föras av certifikatutfärdare som tillhandahåller kvalificerade certifikat

En certifikatutfärdare som tillhandahåller kvalificerade certifikat ska föra register över utfärdade kvalificerade certifikat (certifikatregister). I registret ska införas

1) de uppgifter som det kvalificerade certifikatet ska innehålla enligt 30 § 2 mom.,

2) de uppgifter som gäller sökandens person och som avses i 35 § 1 mom., inbegripet uppgift om det förfarande för identifiering av sökanden som använts då det kvalificerade certifikatet utfärdades och behövliga uppgifter om den handling som eventuellt anlitats för identifieringen, och

3) de uppgifter som avses i 39 § om kontroll av ett certifikats giltighet som gjorts på spärrlistan, om en certifikatutfärdare som tillhandahåller kvalificerade certifikat utnyttjar rätten att registrera uppgifter enligt 39 §.

En certifikatutfärdare som tillhandahåller kvalificerade certifikat ska säkerställa att den som förlitar sig på en avancerad elektronisk signatur som är baserad på ett kvalificerat certifikat har tillgång till certifikatets i 30 § 2 mom. definierade innehåll. De uppgifter som avses ovan i 1 mom. 3 punkten behöver dock inte införas i certifikatregistret, om certifikatutfärdaren på annat sätt ser till att den som förlitar sig på certifikatet kan visa upp tillförlitligt bevis på behörig kontroll av spärrlistan.

Certifikatutfärdaren ska också föra ett register över återkallade kvalificerade certifikat (spärrlista) som ska vara tillgängligt för dem som förlitar sig på kvalificerade certifikat. På

37 §

Allmänna skyldigheter för certifieringsorgan och organ för bedömning av överensstämmelse

Ett organ för bedömning av överensstämmelse och ett certifieringsorgan får i sitt uppdrag anlita biträde av personer som inte hör till organisationen. Organen ansvarar också för det arbete som utförts av personer de anlitat.

Bestämmelser om de principer för god förvaltning som organ för bedömning av överensstämmelse och certifieringsorgan ska följa när de utför offentliga förvaltningsuppgifter som avses i denna lag finns i förvaltningslagen (434/2003), lagen om offentlighet i myndigheternas verksamhet, lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003), språklagen (423/2003) och samiska språklagen (1086/2003). På personalen vid organ för bedömning av överensstämmelse och vid certifieringsorgan och vid dotterbolag och underentreprenörer som anlitas av sådana organ tillämpas bestämmelserna om straffrättsligt tjänsteansvar när den sköter uppgifter som avses i denna paragraf,. Bestämmelser om skadeståndsansvar finns i skadeståndslagen (412/1974).

Organ för bedömning av överensstämmelse och certifieringsorgan ska underrätta Kommunikationsverket om varje ändring som har betydelse för uppfyllandet av villkoren för att godkännas eller utses.

spärrlistan ska utan dröjsmål införas uppgift om att ett kvalificerat certifikat har återkallats och exakt tidpunkt för återkallandet.

De uppgifter som nämns i 2 och 3 mom. ska vara tillgängliga dygnet runt.

38 §

Förvaring av uppgifterna i certifikatregistret

Certifikatutfärdare som tillhandahåller kvalificerade certifikat ska på ett tillförlitligt och ändamålsenligt sätt förvara uppgifterna i certifikatregistret i 10 år från det att certifikatet upphörde att gälla.

Certifikatutfärdare som utöver kvalificerade certifikat också tillhandahåller tjänster för stark autentisering får oberoende av vad som föreskrivs i 24 § till alla delar förvara uppgifterna på det sätt som avses i 1 mom.

38 §

Återkallande av godkännande som organ för bedömning av överensstämmelse eller utseende till certifieringsorgan

Om Kommunikationsverket konstaterar att ett organ för bedömning av överensstämmelse eller ett certifieringsorgan inte uppfyller föreskrivna villkor eller att organet i väsentlig grad handlar i strid med gällande bestämmelser, ska Kommunikationsverket sätta ut en tillräcklig tidsfrist inom vilken saken ska rättas till.

Kommunikationsverket kan återkalla ett beslut att godkänna ett bedömningsorgan eller utse ett certifieringsorgan om organet inte har korrigerat sin verksamhet inom den tid som satts ut enligt 1 mom. och det är fråga om en väsentlig förseelse eller försummelse.

39 §

Registrering av uppgift om kontroll av certifikats giltighet

Certifikatutfärdare som tillhandahåller kvalificerade certifikat får registrera uppgifter om kontroll av certifikatens giltighet som gjorts på spärrlistan. De registrerade uppgifterna får användas endast för fakturering av användningen av certifikat och för verifiering av rättshandlingar som företagits med hjälp av elektroniska signaturer som är baserade på certifikat.

4 a kap.

Betrodda tjänster

39 §

Återkallande av certifikat

En undertecknare eller en innehavare av en elektronisk stämpel ska utan dröjsmål begära att den certifikatutfärdare som har utfärdat ett kvalificerat certifikat ska återkalla det, om undertecknaren har grundad anledning att misstänka att framställningsdata för undertecknigen eller den elektroniska stämpeln används på obehörigt sätt.

En certifikatutfärdare som tillhandahåller kvalificerade certifikat ska utan dröjsmål återkalla ett kvalificerat certifikat, om undertecknaren eller innehavaren av den elektro-

niska stämpeln begär det. En begäran om återkallande av ett certifikat anses ha kommit in till certifikatutfärdaren när den har stått till utfärdarens förfogande så att begäran har kunnat behandlas.

40 §

Ansvar för obehörig användning av signaturframställningsdata

Undertecknaren ansvarar för skada som orsakats av obehörig användning av signaturframställningsdata för en avancerad elektronisk signatur som är baserad på ett kvalificerat certifikat tills en begäran om återkallande av certifikatet har inkommit till certifikatutfärdaren så som anges i 36 § 2 mom.

En konsument har dock ansvar enligt 1 mom. endast om

1) konsumenten har överlåtit signaturframställningsdata till någon annan,

2) någon som är obehörig att använda signaturframställningsdata kommit åt dem på grund av att konsumenten varit vårdslös på ett sätt som inte är lindrigt, eller

3) konsumenten på annat sätt än det som nämns i 2 punkten har förlorat besittningen till signaturframställningsdata och därefter har underlåtit att begära att det kvalificerade certifikatet ska återkallas så som anges i 36 § 1 mom.

40 §

Ansvar för obehörig användning av framställningsdata för en underteckning eller elektronisk stämpel

En undertecknare och en innehavare av en elektronisk stämpel ansvarar för skada som orsakats av obehörig användning av framställningsdata för en avancerad elektronisk underskrift eller elektronisk stämpel som är baserad på ett kvalificerat certifikat tills en begäran om återkallande av certifikatet har kommit in till certifikatutfärdaren så som anges i 39 § 2 mom.

En konsument har dock ansvar enligt 1 mom. endast om

1) konsumenten har överlåtit framställningsdata till någon annan,

2) någon som är obehörig att använda framställningsdata kommit åt dem på grund av att konsumenten varit vårdslös på ett sätt som inte är lindrigt, eller

3) konsumenten på annat sätt än det som nämns i 2 punkten har förlorat besittningen till framställningsdata och därefter har underlåtit att begära att det certifikatet ska återkallas så som anges i 39 § 1 mom.

41 §

Skadeståndsansvar för certifikatutfärdare som tillhandahåller kvalificerade certifikat

En certifikatutfärdare som tillhandahåller kvalificerade certifikat är ansvarig för skada som orsakats den som förlitat sig på ett kvalificerat certifikat, om skadan uppkommit genom att

1) de uppgifter som antecknats i det kvalificerade certifikatet var felaktiga vid den tidpunkt då certifikatet utfärdades,

2) det kvalificerade certifikatet inte innehåller de uppgifter som nämns i 30 § 2 mom.,

41 §

Det ansvar som vilar på tillhandahållare av betrodda tjänster

Bestämmelser om det ansvar som vilar på tillhandahållare av betrodda tjänster finns i artikel 13 i EU:s förordning om elektronisk identifiering.

Den certifikatutfärdare som tillhandahållit ett kvalificerat certifikat är ansvarig för skada som den som förlitat sig på det kvalificerade certifikatet orsakats genom att certifikatutfärdaren eller en person som denne anlitat inte har återkallat certifikatet på det sätt

3) den person som anges i det kvalificerade certifikatet inte vid den tidpunkt då certifikatet utfärdades var i besittning av de signaturframställningsdata som motsvarar de signaturverifieringsdata som anges eller definieras i certifikatet,

4) de signaturframställningsdata och signaturverifieringsdata som framställts av certifikatutfärdaren eller en person som denne anlitat inte kan användas som komplement till varandra, eller

5) certifikatutfärdaren eller en person som denne anlitat inte har återkallat det kvalificerade certifikatet på det sätt som anges i 36 §.

Certifikatutfärdaren är fri från ansvar enligt 1 mom., om utfärdaren visar att skadan inte har orsakats av vårdslöshet hos utfärdaren själv eller någon som denne har anlitat.

En certifikatutfärdare ansvarar inte för skada som orsakats av att ett kvalificerat certifikat har använts i strid med de begränsningar av användningen som ingår i det.

I fråga om skadeståndsansvaret för certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat föreskrivs i övrigt i skadeståndslagen (412/1974).

Vad som föreskrivs i denna paragraf tillämpas också på en certifikatutfärdare som för allmänheten garanterar att ett certifikat är ett kvalificerat certifikat.

som anges i 39 §. Certifikatutfärdaren är fri från ansvar, om den visar att skadan inte har berott på oaktsamhet hos certifikatutfärdaren eller en person som denne anlitat.

42 §

Allmän styrning och tillsyn

Kommunikationsministeriet svarar för den allmänna styrningen och utvecklingen av stark autentisering och elektroniska signaturer.

Kommunikationsverket har tillsyn över efterlevnaden av denna lag med undantag av 1 § 3 mom. Kommunikationsverket utfärdar vid behov tekniska föreskrifter om kraven på tillförlitlighet och informationssäkerhet i verksamhet som bedrivs av leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller kvalificerade certifikat.

Dataombudsmannen ska övervaka att bestämmelserna om personuppgifter i denna lag följs.

42 §

Allmän styrning och Kommunikationsverkets föreskrifter

Kommunikationsministeriet svarar för den allmänna styrningen och utvecklingen av stark autentisering och *betrodda tjänster*.

Kommunikationsverket får meddela närmare föreskrifter om

1) kraven enligt 8 § 1 mom. 4 och 5 punkten på säkerhet och tillförlitlighet hos identifieringssystemet,

2) innehållet i de uppgifter som ska anmälas enligt 10 § och inlämnandet av dem till Kommunikationsverket,

3) egenskaperna enligt 12 a § 2 mom. hos förtroendenätets gränssnitt,

4) när störningar som avses i 16 § är bety-

dande och innehållet i anmälningar enligt 16 § 1 mom. samt anmälningarnas form och inlämnandet av dem,

5) grunderna för bedömningen enligt 29, 30 och 32 § av överensstämmelsen hos en identifieringstjänst, en betrodd tjänst och den nationella noden,

6) kompetenskraven enligt 33 § för organ för bedömning av överensstämmelse med beaktande av vad som föreskrivs i EU:s förordning om elektronisk identifiering,

7) de uppgifter som ska ingå i en ansökan enligt 35 § och inlämnandet av dem till Kommunikationsverket,

8) de krav som ställs på certifieringsorgan som avses i 36 §, förfarandet vid certifiering och kraven på anordningar för skapande av underskrifter och stämplar med beaktande av vad som föreskrivs i EU:s förordning om elektronisk identifiering.

42 a §

Kommunikationsverkets uppgifter

Kommunikationsverket ska utöva tillsyn över efterlevnaden av denna lag, om inte något annat föreskrivs i denna lag.

Kommunikationsverket ska i enlighet med EU:s förordning om elektronisk identifiering

1) delta i samarbetet mellan Europeiska unionens medlemsstater i det interoperabilitetsramverk för elektronisk identifiering som avses i artikel 12 i förordningen och i det samarbetsnätverk som upprättats för detta ändamål,

2) anmäla system för elektronisk identifiering till Europeiska kommissionen i enlighet med artiklarna 7—10 i förordningen,

3) vara tillsynsorgan enligt artikel 17 i förordningen och sköta tillsynsorganets uppgifter enligt förordningen,

4) i enlighet med artikel 22 i förordningen föra och publicera förteckningar över kvalificerade tillhandahållare av betrodda tjänster i Finland och över de kvalificerade betrodda tjänster som dessa tillhandahåller.

Kommunikationsverkets beslutanderätt omfattar inte avtalsförhållanden mellan parter eller frågor om ersättningsskyldighet.

42 b §

Dataombudsmannens uppgifter

Dataombudsmannen ska övervaka att bestämmelserna om personuppgifter i denna lag iakttas.

42 c §

Befolkningsregistercentralens uppgifter

Befolkningsregistercentralen ska upprätthålla den nationella nod som avses i 30 §.

43 §

Rätt till information

Trots bestämmelserna om sekretess har Kommunikationsverket rätt att av leverantörer av identifieringstjänster, certifikatutfärdare som tillhandahåller kvalificerade certifikat och kontrollorgan som avses i 29 § samt av personer som dessa anlitar få den information som behövs för att fullgöra de uppgifter som anges i 42 §.

— — — — — — — — — — — — — — —

43 §

Rätt till information

När Kommunikationsverket fullgör sina uppgifter enligt denna lag har verket trots sekretessbestämmelserna rätt att få den information som behövs för skötseln av uppgifterna av dem vars rättigheter och skyldigheter denna lag gäller och av dem som handlar för dessas räkning.

— — — — — — — — — — — — — — —

44 §

Myndighetssamarbete och rätt att lämna information

Utöver vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet (621/1999) har Kommunikationsverket och dataombudsmannen trots sekretessbestämmelserna rätt att till Finansinspektionen lämna den information som den behöver för att fullgöra sina uppgifter. Finansinspektionen har motsvarande rätt att trots sekretessbestämmelserna till Kommunikationsverket och dataombudsmannen lämna de uppgifter som de behöver för att fullgöra sina uppgifter enligt denna lag.

— — — — — — — — — — — — — — —

44 §

Myndighetssamarbete och rätt att lämna information

Utöver vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet har Kommunikationsverket och dataombudsmannen trots sekretessbestämmelserna *och andra begränsningar som gäller utlämnande av uppgifter* rätt att lämna Finansinspektionen *och Konkurrens- och konsumentverket* den information som de behöver för skötseln av sina uppgifter. Finansinspektionen *och Konkurrens- och konsumentverket* har motsvarande rätt att trots sekretessbestämmelserna lämna Kommunikationsverket och dataombudsmannen de uppgifter som behövs för skötseln av deras uppgifter enligt denna lag.

— — — — — — — — — — — — — — —

45 §

Administrativa tvångsmedel

Om någon 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. Bestämmelser om vite, hot om avbrytande och hot om tvångsutförande finns i viteslagen (1113/1990).

— — — — — — — — — — — — — — —

45 §

Administrativa tvångsmedel

Kommunikationsverket kan ge en anmärkning till den som bryter mot denna lag eller bestämmelser som utfärdats eller föreskrifter eller beslut som har meddelats med stöd av den, eller mot EU:s förordning om elektronisk identifiering eller bestämmelser som har utfärdats med stöd av den, samt ålägga denne att avhjälpa felet eller försummelsen inom skälig tid. 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. Bestämmelser om vite, hot om avbrytande och hot om tvångsutförande finns i viteslagen (1113/1990).

— — — — — — — — — — — — — — —

45 a §

Interimistiska beslut

Om ett fel eller en försummelse som gäller EU:s förordning om elektronisk identifiering, denna lag eller bestämmelser som utfärdats eller föreskrifter som meddelats med stöd av dem, eller en störning i datasäkerheten, omedelbart och i väsentlig grad äventyrar tillförlitligheten hos en identifieringstjänst eller betrodd tjänst, får Kommunikationsverket omgående besluta om behövliga interimistiska åtgärder oberoende av den tidsfrist som avses i 45 §.

Kommunikationsverket ska innan det beslutar om interimistiska åtgärder ge den som är föremål för beslutet tillfälle att bli hörd, utom när detta inte kan ordnas så snabbt som ärendets brådskande natur nödvändigtvis kräver.

Som interimistisk åtgärd kan Kommunikationsverket förbjuda eller avbryta

1) tillhandahållandet av en identifieringsmetod som stark autentisering,

2) tillhandahållandet av en sådan kvalifice-

rad betrodd tjänst som avses i artikel 3.17 i EU:s förordning om elektronisk identifiering,

3) tillhandahållandet av ett system för elektronisk identifiering som anmälts enligt artikel 9.1 i EU:s förordning om elektronisk identifiering,

4) tillhandahållandet av autentisering enligt artikel 7 f i EU:s förordning om elektronisk identifiering.

De interimistiska åtgärderna kan vara i kraft i högst tre månader. Beslut om interimistiska åtgärder får överklagas separat, på samma sätt som beslut som avses i 45 § 1 mom.

46 §

Inspektionsrätt

Kommunikationsverket har rätt att utföra inspektioner av leverantörer av identifieringstjänster och av leverantörernas tjänster, kontrollorgan som avses i 29 § och av deras verksamhet och certifikatutfärdare som tillhandahåller kvalificerade certifikat och av deras tjänster, om det finns skäl att misstänka att de på ett väsentligt sätt har brutit mot denna lag eller mot föreskrifter som har utfärdats med stöd av den.

Kommunikationsverket ska årligen utföra inspektioner av certifikatutfärdare som tillhandahåller kvalificerade certifikat och av deras tjänster.

Kommunikationsverket förordnar en inspektör att utföra de inspektioner som avses i 1 och 2 mom. Den som utför inspektionen har rätt att hos en leverantör av identifieringstjänster och hos en certifikatutfärdare som tillhandahåller kvalificerade certifikat samt hos personer som dessa anlitar undersöka sådan maskinvara och programvara som kan vara av betydelse vid tillsynen över att denna lag och de föreskrifter som utfärdats med stöd av den efterlevs.

Leverantörer av identifieringstjänster, certifikatutfärdare som tillhandahåller kvalificerade certifikat och de personer som dessa anlitar ska för inspektionen ge en inspektör som avses i 3 mom. tillträde till sådana produktions- och affärslokaler samt lagerutrymmen som inte omfattas av hemfriden.

Kommunikationsverket har rätt att få

46 §

Inspektionsrätt

Kommunikationsverket har rätt att utföra inspektioner av leverantörer av identifieringstjänster och av leverantörernas tjänster, *av organ för bedömning av överensstämmelse som avses i 28 §, av certifieringsorgan enligt 36 § för anordningar för skapande av kvalificerade elektroniska underskrifter och elektroniska stämplar och dessa organs verksamhet, av certifikatutfärdare som tillhandahåller kvalificerade certifikat samt av tillhandahållare av betrodda tjänster och deras tjänster. En inspektion kan genomföras för att övervaka fullgörandet av skyldigheter enligt denna lag och EU:s förordning om elektronisk identifiering samt bestämmelser som utfärdats och föreskrifter och beslut som har meddelats med stöd av dem. Bestämmelser om inspektioner finns i 39 § i förvaltningslagen.*

Kommunikationsverket förordnar en inspektör att utföra de inspektioner som avses i 1 mom. Den som utför inspektionen har rätt att hos en leverantör av identifieringstjänster, hos en certifikatutfärdare som tillhandahåller kvalificerade certifikat och hos en tillhandahållare av betrodda tjänster samt hos personer som dessa anlitar granska sådan maskinvara och programvara som kan vara av betydelse vid tillsynen över efterlevnaden av denna lag och de bestämmelser utfärdats och föreskrifter som meddelats med stöd av den.

Leverantörer av identifieringstjänster, cer-

handräckning av polisen för att utföra inspektioner enligt denna paragraf.

Vid fullgörandet av sina uppgifter har dataombudsmannen den rätt att utöva tillsyn som anges i personuppgiftslagen.

tifikatutfärdare som tillhandahåller kvalificerade certifikat, tillhandahållare av betrodda tjänster och de personer som dessa anlitar ska för inspektionen ge en inspektör som avses i 2 mom. tillträde till alla andra utrymmen än sådana som används för boende av permanent natur.

Kommunikationsverket har rätt att få handräckning av polisen för att utföra inspektioner enligt denna paragraf.

Dataombudsmannen har vid fullgörandet av sina uppgifter den rätt att utföra inspektioner som anges i personuppgiftslagen.

47 §

Avgifter som ska betalas till Kommunikationsverket

En leverantör av identifieringstjänster och en sammanslutning av tjänsteleverantörer som har gjort en anmälan enligt 10 § ska betala en registreringsavgift på 5 000 euro till Kommunikationsverket. Leverantören av identifieringstjänster och sammanslutningen ska dessutom årligen betala en tillsynsavgift på 12 000 euro till Kommunikationsverket.

Certifikatutfärdare som tillhandahåller kvalificerade certifikat och som gjort en anmälan enligt 32 § ska betala en registreringsavgift på 5 000 euro till Kommunikationsverket. Dessutom ska en sådan certifikatutfärdare årligen betala en tillsynsavgift på 40 000 euro till Kommunikationsverket. Om en certifikatutfärdare som tillhandahåller kvalificerade certifikat även gör en anmälan enligt 10 §, ska certifikatutfärdaren betala den registreringsavgift som avses i 1 mom.

Kontrollorgan som har utsetts enligt 29 § ska betala en utnämningsavgift på 10 000 euro till Kommunikationsverket. Dessutom ska kontrollorganet årligen betala en tillsynsavgift på 15 000 euro till Kommunikationsverket.

Registreringsavgiften, utnämningsavgiften och tillsynsavgiften motsvarar Kommunikationsverkets kostnader för att utföra uppgifterna enligt denna lag, med undantag för de uppgifter som avses i 46 § 1 mom. Tillsynsavgiften ska betalas till fullt belopp också under det första verksamhetsåret, även om verksamheten inleds under året. Tillsynsav-

47 §

Avgifter till Kommunikationsverket

En leverantör av identifieringstjänster och en sammanslutning av tjänsteleverantörer som har gjort en anmälan enligt 10 § ska betala Kommunikationsverket en registreringsavgift på 5 000 euro. Leverantören av identifieringstjänster och sammanslutningen ska dessutom betala Kommunikationsverket en årlig tillsynsavgift på 14 000 euro.

En kvalificerad tillhandahållare av betrodda tjänster som gjort en anmälan enligt artikel 21 i EU:s förordning om elektronisk identifiering och en certifikatutfärdare som tillhandahåller kvalificerade betrodda tjänster ska betala Kommunikationsverket en registreringsavgift på 5 000 euro för varje betrodd tjänst de tillhandahåller. Dessutom ska de betala Kommunikationsverket en årlig tillsynsavgift på 14 000 euro för den första kvalificerade betrodda tjänst som de tillhandahåller och en årlig tillsynsavgift på 9 000 euro för varje därpå följande kvalificerade betrodda tjänst som de tillhandahåller. Om en certifikatutfärdare som tillhandahåller betrodda tjänster även gör en anmälan enligt 10 §, ska certifikatutfärdaren dessutom betala den registreringsavgift som anges i 1 mom.

Ett organ för bedömning av överensstämmelse som godkänts enligt 34 § ska betala Kommunikationsverket en utnämningsavgift på 10 000 euro. Dessutom ska organet betala Kommunikationsverket en årlig tillsynsavgift på 15 000 euro.

Ett certifieringsorgan som utsetts enligt 36

giften återbetalas inte även om tjänsteleverantören upphör med sin verksamhet under året.

Registreringsavgiften, utnämningsavgiften och tillsynsavgiften påförs av Kommunikationsverket. Kommunikationsverkets beslut om att påföra avgift får överklagas i enlighet med 49 § 1 mom. Närmare bestämmelser om verkställigheten av avgifterna kan utfärdas genom förordning av kommunikationsministeriet.

Registreringsavgiften, utnämningsavgiften och tillsynsavgiften får drivas in utan dom eller beslut på det sätt som föreskrivs i lagen om verkställighet av skatter och avgifter. Om avgifterna inte betalas senast på förfallodagen, tas en årlig dröjsmålsränta ut på det obetalda beloppet enligt den räntefot som avses i 4 § 1 mom. i räntelagen (633/1982). I stället för dröjsmålsränta kan myndigheten ta ut en dröjsmålsavgift på fem euro i sådana fall då dröjsmålsräntan understiger detta belopp.

Om den verksamhet som bedrivs av en leverantör av identifieringstjänster ska inspekteras med stöd av 46 § 1 mom., tas kostnaderna för inspektionen ut av leverantören av identifieringstjänster enligt lagen om grunderna för avgifter till staten.

§ ska betala Kommunikationsverket en utnämningsavgift på 10 000 euro. Dessutom ska organet betala Kommunikationsverket en årlig tillsynsavgift på 15 000 euro.

Registreringsavgiften, utnämningsavgiften och tillsynsavgiften täcker Kommunikationsverkets kostnader för att utföra uppgifterna enligt denna lag, med undantag för de uppgifter som avses i 46 § 1 mom. Tillsynsavgiften ska betalas till fullt belopp också under det första verksamhetsåret, även om verksamheten inleds under året. Tillsynsavgiften återbetalas inte, även om tjänsteleverantören upphör med sin verksamhet under året.

Registreringsavgiften, utnämningsavgiften och tillsynsavgiften påförs av Kommunikationsverket och avgifterna är direkt utsökbara. I kommunikationsverkets beslut om påförande av avgift får ändring sökas i enlighet med 49 § 1 mom. Närmare bestämmelser om verkställigheten av avgifterna får utfärdas genom förordning av kommunikationsministeriet.

Bestämmelser om indrivning av registreringsavgiften, utnämningsavgiften och tillsynsavgiften finns i lagen om verkställighet av skatter och avgifter. Om avgifterna inte betalas senast på förfallodagen, tas årlig dröjsmålsränta ut på det obetalda beloppet enligt den räntesats som avses i 4 § i räntelagen (633/1982). I stället för dröjsmålsränta kan myndigheten ta ut en dröjsmålsavgift på fem euro om dröjsmålsräntan är mindre än detta belopp.

För en inspektion som avses i 46 § 1 mom. tas kostnaderna för inspektionen ut av föremålet för inspektionen med iakttagande av lagen om grunderna för avgifter till staten.

49 §

Ändringssökande

Beslut av Kommunikationsverket får överklagas genom besvär hos förvaltningsdomstolen på det sätt som anges i förvaltningsprocesslagen (586/1996).

Förvaltningsdomstolens beslut i ett ärende som gäller återkallande av ett beslut att utse ett kontrollorgan får överklagas genom besvär på det sätt som anges i förvaltningspro-

49 §

Sökande av ändring i myndighetsbeslut

Omprövning av ett beslut som fattats av Kommunikationsverket om en avgift som ska betalas till Kommunikationsverket enligt 47 § får begäras på det sätt som anges i 7 a kap. i förvaltningslagen.

Beslut som Kommunikationsverket fattat med anledning av en begäran om omprövning samt andra beslut av Kommunikations-

cesslagen. Andra beslut av förvaltningsdomstolen får överklagas genom besvär endast om högsta förvaltningsdomstolen beviljar besvärstillstånd.

Kommunikationsverket får i sina beslut bestämma att beslutet ska iakttas innan det har vunnit laga kraft. Besvärsmyndigheten kan dock förbjuda verkställigheten av beslutet tills besvären har avgjorts.

Bestämmelser om sökande av ändring i ett beslut av dataombudsmannen finns i personuppgiftslagen.

verket än sådana som avses i 1 mom. får överklagas genom besvär hos förvaltningsdomstolen på det sätt som anges i förvaltningsprocesslagen (586/1996).

Förvaltningsdomstolens beslut i ett ärende som gäller återkallande av ett beslut om att godkänna ett organ för bedömning av överensstämmelse eller om att utse ett certifieringsorgan får överklagas genom besvär på det sätt som anges i förvaltningsprocesslagen. Över andra beslut av förvaltningsdomstolen får besvär anföras endast om högsta förvaltningsdomstolen beviljar besvärstillstånd.

Kommunikationsverket får i sina beslut bestämma att beslutet ska iakttas innan det har vunnit laga kraft. Besvärsmyndigheten kan dock förbjuda verkställigheten av beslutet tills besvären har avgjorts.

Bestämmelser om sökande av ändring i ett beslut av dataombudsmannen finns i personuppgiftslagen.

49 a §

Sökande av ändring i beslut av organ för bedömning av överensstämmelse och beslut av certifieringsorgan

Omprövning av ett beslut som fattats av ett organ för bedömning av överensstämmelse eller av ett certifieringsorgan med stöd av denna lag får begäras hos Kommunikationsverket på det sätt som anges i 7 a kap. i förvaltningslagen.

Beslut som fattats med anledning av en begäran om omprövning får överklagas genom besvär hos förvaltningsdomstolen på det sätt som anges förvaltningsprocesslagen. Över förvaltningsdomstolens beslut får besvär anföras endast om högsta förvaltningsdomstolen beviljar besvärstillstånd.

Beslut av organ för bedömning av överensstämmelse och beslut av certifieringsorgan ska iakttas oberoende av ändringssökande, om inte den myndighet där ändring sökts bestämmer något annat.

Denna lag träder i kraft den 20 .

En leverantör av identifieringsverktyg får till och med den 31 december 2018 som ett i

17 § 2 mom. i denna lag avsett godkänt dokument också använda ett giltigt körkort som har beviljats efter den 1 oktober 1990 av en myndighet i en medlemsstat i Europeiska ekonomiska samarbetsområdet.

De av Kommunikationsverket meddelade föreskrifter som gäller vid ikraftträdandet av denna lag förblir i kraft.

En leverantör av identifieringstjänster som är införd i det register som avses i 12 § ska senast två månader från ikraftträdandet av denna lag lämna Kommunikationsverket en ändringsanmälan enligt 10 § 3 mom., om leverantören vill fortsätta vara verksam som leverantör av identifieringstjänster för stark autentisering. De uppgifter som krävs enligt 10 § i denna lag ska lämnas in till Kommunikationsverket senast den 31 januari 2017.

Kommunikationsverket ska behandla en ändringsanmälan enligt 3 mom. från en leverantör av identifieringstjänster och göra de anteckningar som föranleds av anmälan i det register som avses i 12 § senast tre månader efter att ha mottagit ändringsanmälan och övriga uppgifter enligt 3 mom.

Ett identifieringsverktyg för stark autentisering som har beviljats enligt de bestämmelser som gällde vid ikraftträdandet av denna lag ska betraktas som ett identifieringsverktyg för stark autentisering för åtminstone tillitsnivån väsentlig i två månader från ikraftträdandet av denna lag. Om inte något annat följer av 7 mom. och om leverantören av identifieringstjänster lämnar en ändringsanmälan enligt 3 mom. inom utsatt tid, ska ett identifieringsverktyg leverantören beviljat före eller efter ikraftträdandet av denna lag betraktas som ett identifieringsverktyg för stark autentisering för åtminstone tillitsnivån väsentlig tills Kommunikationsverket har gjort en anteckning om identifieringstjänsten i det register som avses i 12 § utifrån uppgifterna i ändringsanmälan.

Ett elektroniskt identifieringsverktyg som har beviljats enligt 17 § i denna lag på grundval av ett elektroniskt identifieringsverktyg som sökanden tidigare innehaft ska betraktas som ett identifieringsverktyg för stark autentisering, om

1) identifieringsverktyget har beviljats senast två månader från ikraftträdandet av denna lag, eller

2) identifieringsverktyget har beviljats efter

det att två månader förflutit från ikraftträdandet av denna lag på grundval av ett sådant annat identifieringsverktyg för stark autentisering som beviljats av en leverantör av identifieringstjänster som gjort en ändringsanmälan enligt 3 mom.

Ett elektroniskt identifieringsverktyg betraktas inte längre som ett identifieringsverktyg för stark autentisering, om leverantören av identifieringstjänster inte har lämnat en ändringsanmälan enligt 3 mom. inom utsatt tid. Kommunikationsverket ska då avföra leverantören av identifieringstjänster ur det register som avses i 12 § och underrätta leverantören om detta.

———

2.

Lag

om ändring av lagen om elektronisk kommunikation i myndigheternas verksamhet

I enlighet med riksdagens beslut

ändras i lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003) 3, 9, 16 och 18 §, sådana de lyder, 3 och 9 § delvis ändrade i lag 618/2009, 16 § i lag 618/2009 och 18 § i lag 924/2010, som följer:

Gällande lydelse	*Föreslagen lydelse*
3 §	3 §
Annan lagstiftning	*Annan lagstiftning*
Vid uträttande och behandling av ärenden hos myndigheter tillämpas i övrigt vad som föreskrivs om anhängiggörande av ärenden, delgivning av beslut, offentlighet i myndigheternas verksamhet, behandling av personuppgifter, arkivering av handlingar, det språk som används vid behandling av ärenden och om hur ärenden behandlas. *Bestämmelser om elektroniska signaturer och om tillhandahållande av identifieringstjänster och kvalificerade certifikat i anslutning till dem finns i lagen om stark autentisering och elektroniska signaturer (617/2009*).	*Vid uträttande och behandling av ärenden hos myndigheter tillämpas i övrigt vad som föreskrivs om anhängiggörande av ärenden, delgivning av beslut, offentlighet i myndigheternas verksamhet, behandling av personuppgifter, arkivering av handlingar, det språk som används vid behandling av ärenden och om hur ärenden behandlas.*
9 §	9 §
Krav på skriftlig form och underskrift	*Krav på skriftlig form*
Vid anhängiggörande och behandling av ärenden uppfyller också elektroniska dokument som sänts till en myndighet kravet på skriftlig form. *Om det vid anhängiggörande eller behandling av ett ärende krävs en undertecknad handling, uppfylls kravet på underskrift också genom en sådan elektronisk signatur som avses i 5 § 2 mom. i lagen om stark autentisering och elektroniska signaturer*. Ett elektroniskt dokument som inkommit till en myndighet behöver inte kompletteras	*Vid anhängiggörande och behandling av ärenden uppfyller också elektroniska dokument som sänts till en myndighet kravet på skriftlig form.* *Ett elektroniskt dokument som kommit in till en myndighet behöver inte kompletteras med en underskrift, om dokumentet innehåller uppgifter om avsändaren och om det inte finns anledning att betvivla dokumentets autenticitet och integritet. Om ett elektroniskt dokument som sänts till en myndighet inne-*

med en underskrift, om dokumentet innehåller uppgifter om avsändaren och om det inte finns anledning att betvivla dokumentets autenticitet och integritet. Om ett elektroniskt dokument som sänts till en myndighet innehåller utredning om ett ombuds behörighet, behöver ombudet inte lämna in fullmakt. Myndigheten kan dock förordna att en fullmakt skall lämnas in, om den har anledning att betvivla ombudets behörighet eller behörighetens omfattning.

håller utredning om ett ombuds behörighet, behöver ombudet inte lämna in fullmakt. Myndigheten kan dock förordna att en fullmakt skall lämnas in, om den har anledning att betvivla ombudets behörighet eller behörighetens omfattning.

16 §

Elektronisk signering av beslutshandlingar

En beslutshandling kan signeras elektroniskt. Myndigheten ska signera dokumentet på det sätt som anges i 5 § 2 mom. i lagen om stark autentisering och elektroniska signaturer.

16 §

Elektronisk signering av beslutshandlingar

En beslutshandling får signeras elektroniskt. Myndigheten ska signera handlingen med en avancerad elektronisk underskrift som uppfyller kraven enligt artikel 26 i Europaparlamentets och rådets förordning (EU) Nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG eller annars på ett sådant sätt att man kan försäkra sig om handlingens autenticitet och integritet.

18 §

Bevislig elektronisk delgivning

En handling som enligt lag ska sändas med post mot mottagningsbevis eller delges bevisligen på annat sätt får med partens samtycke delges också som ett elektroniskt meddelande, dock inte per telefax eller på därmed jämförbart sätt. Myndigheten ska då meddela att parten eller dennes företrädare kan hämta handlingen från en av myndigheten anvisad server, databas eller någon annan fil.

Parten eller dennes företrädare ska identifiera sig när handlingen hämtas. Vid identifieringen används ett identifieringsverktyg eller ett kvalificerat certifikat som avses i lagen om stark autentisering och elektroniska signaturer eller någon annan motsvarande identifieringsteknik som är datatekniskt tillförlitlig och bevislig.

En handling anses ha delgivits när den har hämtats från den länk som myndigheten an-

18 §

Bevislig elektronisk delgivning

En handling som enligt lag ska sändas med post mot mottagningsbevis eller delges bevisligen på annat sätt får med partens samtycke delges också som ett elektroniskt meddelande, dock inte per telefax eller på därmed jämförbart sätt. Myndigheten ska då meddela att parten eller dennes företrädare kan hämta handlingen från en av myndigheten anvisad server, databas eller någon annan fil.

Parten eller dennes företrädare ska identifiera sig när handlingen hämtas. Vid identifieringen ska då användas en identifieringsteknik som är datatekniskt tillförlitlig och bevislig.

En handling anses ha delgivits när den har hämtats från den länk som myndigheten anvisat enligt 1 mom. Om handlingen inte har hämtats inom sju dagar från myndighetens

visat enligt 1 mom. Om handlingen inte har hämtats inom sju dagar från myndighetens meddelande, iakttas vid delgivningen vad som annanstans i lag föreskrivs om delgivning.

meddelande, iakttas vid delgivningen vad som annanstans i lag föreskrivs om delgivning.

Denna lag träder i kraft den 20 .

3.

Lag

om ändring av 2 § i lagen om kommunikationsförvaltningen

I enlighet med riksdagens beslut
ändras i lagen om kommunikationsförvaltningen (625/2001) 2 § 1 punkten, sådan den lyder i lag 730/2014, som följer:

Gällande lydelse	*Föreslagen lydelse*
2 §	2 §
Kommunikationsverkets uppgifter	*Kommunikationsverkets uppgifter*
Kommunikationsverket har till uppgift att 1) sköta de uppgifter som enligt kommunikationsmarknadslagen (393/2003), lagen om radiofrekvenser och teleutrustningar (1015/2001), postlagen (415/2011), lagen om televisions- och radioverksamhet (744/1998), lagen om statens televisions- och radiofond (745/1998), lagen om dataskydd vid elektronisk kommunikation (516/2004), lagen om förbud mot vissa avkodningssystem (1117/2001), lagen om stark autentisering och elektroniska signaturer (617/2009), lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004), säkerhetsutredningslagen (726/2014), lagen om bedömningsorgan för informationssystem (1405/2011), lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation (1406/2011) samt lagen om domännamn (228/2003) ankommer på Kommunikationsverket,	Kommunikationsverket har till uppgift att 1) sköta de uppgifter som enligt *informationssamhällsbalken (917/2014), postlagen (415/2011), lagen om statens televisions- och radiofond (745/1998), lagen om stark autentisering och betrodda elektroniska tjänster (617/2009), lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004), säkerhetsutredningslagen (726/2014), lagen om bedömningsorgan för informationssäkerhet (1405/2011) och lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation ankommer på Kommunikationsverket*,
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —

Denna lag träder i kraft den 20 .

4.

Lag

om ändring av 9 a kap. 1 § i jordabalken

I enlighet med riksdagens beslut
ändras i jordabalken (540/1995) 9 a kap. 1 § 1 mom., sådant det lyder i lag 96/2011, som följer:

Gällande lydelse	*Föreslagen lydelse*
1 §	1 §
Användning av ärendehanteringssystem och elektronisk identifiering i ett ärendehanteringssystem	*Användning av ärendehanteringssystem och elektronisk identifiering i ett ärendehanteringssystem*
En förutsättning för att upprätta och godkänna elektroniska dokument i ett ärendehanteringssystem samt för att i övrigt använda ärendehanteringssystemet är att användaren identifieras på ett tillförlitligt sätt med hjälp av en sådan identifieringsmetod, tillhandahållen av en leverantör av tjänster för stark autentisering, eller ett sådant kvalificerat certifikat som avses i lagen om stark autentisering och elektroniska signaturer (617/2009), eller med hjälp av någon annan identifieringsteknik som är datatekniskt tillförlitlig och bevislig.	En förutsättning för att upprätta och godkänna elektroniska dokument i ett ärendehanteringssystem samt för att i övrigt använda ärendehanteringssystemet är att användaren identifieras på ett tillförlitligt sätt med hjälp av en sådan identifieringsmetod, tillhandahållen av en leverantör av tjänster för stark autentisering, *som avses i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009), eller ett sådant kvalificerat certifikat för elektronisk underskrift som föreskrivs i artikel 28 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG,* eller med hjälp av någon annan identifieringsteknik som är datatekniskt tillförlitlig och bevislig.
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —

Denna lag träder i kraft den 20 .

5.

Lag

om ändring av 18 § i lagen om förhindrande och utredning av penningtvätt och av finansiering av terrorism

I enlighet med riksdagens beslut

ändras i lagen om förhindrande och utredning av penningtvätt och av finansiering av terrorism (503/2008) 18 § 3 punkten, sådan den lyder i lag 621/2009, som följer:

Gällande lydelse	*Föreslagen lydelse*
18 § *Skärpta krav på kontroll vid identifiering på distans*	18 § Skärpta krav på kontroll vid identifiering på distans
Om kunden inte är närvarande vid identifieringen och styrkandet av identiteten (identifiering på distans), ska den rapporteringsskyldiga vidta följande åtgärder för att minska risken för penningtvätt och finansiering av terrorism:	Om kunden inte är närvarande vid identifieringen och styrkandet av identiteten (identifiering på distans), ska den rapporteringsskyldiga vidta följande åtgärder för att minska risken för penningtvätt och finansiering av terrorism:
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
3) kontrollera kundens identitet med ett identifieringsverktyg eller ett kvalificerat certifikat som avses i lagen om stark autentisering och elektroniska signaturer (617/2009) eller med hjälp av någon annan teknik för elektronisk identifiering som är informationssäker och bevislig.	3) kontrollera kundens identitet med ett identifieringsverktyg *som avses i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) eller med ett kvalificerat certifikat för elektronisk underskrift som föreskrivs i artikel 28 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG,* eller med hjälp av någon annan teknik för elektronisk identifiering som är datatekniskt tillförlitlig och bevislig.

Denna lag träder i kraft den 20 .

6.

Lag

om ändring av lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster

I enlighet med riksdagens beslut

ändras i lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009) 2 § 2 mom. 2 punkten, 6 § 2 mom., 43 § 2 mom. 2 punkten, 61 § 3 mom., 62 §, 66 § 3 mom., 67 § 1 mom. och 68 § 1 mom., sådana de lyder i lag 983/2010, som följer:

Gällande lydelse	*Föreslagen lydelse*
2 §	2 §
Lagens tillämpningsområde	*Lagens tillämpningsområde*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
Om inte något annat bestäms i denna lag, ska följande lagar tillämpas:	Om inte något annat bestäms i denna lag, ska följande lagar tillämpas:
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
2) i fråga om certifierad elektronisk kommunikation och behandlingen av uppgifter i det certifikatregister som avses i denna lag lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003) och lagen om stark autentisering och elektroniska signaturer (617/2009).	2) i fråga om certifierad elektronisk kommunikation och behandlingen av uppgifter i det certifikatregister som avses i denna lag, lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003) och lagen om stark autentisering och *betrodda elektroniska tjänster* (617/2009).
6 §	6 §
Befolkningsregistercentralens certifierade elektroniska kommunikation och dess syfte	*Befolkningsregistercentralens certifierade elektroniska kommunikation och dess syfte*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
Befolkningsregistercentralen för ett sådant certifikatregister över utfärdade personcertifikat som avses i lagen om stark autentisering och elektroniska signaturer. Befolkningsregistercentralen är registeransvarig för registret.	Befolkningsregistercentralen för ett sådant certifikatregister över utfärdade personcertifikat som *det föreskrivs om i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, nedan EU:s förordning om elektronisk identifiering*). Befolkningsregistercentralen är registeransvarig för certifikatregistret.
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —

43 §	43 §
Utlämnande av identifieringsuppgifter	*Utlämnande av identifieringsuppgifter*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Elektroniska kommunikationskoder som registrerats i befolkningsdatasystemet får lämnas ut endast om	Elektroniska kommunikationskoder som registrerats i befolkningsdatasystemet får lämnas ut endast om
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
2) en annan i Finland etablerad certifikatutfärdare använder koden som en uppgift som identifierar innehavaren av certifikatet i certifikat som avses i lagen om stark autentisering och elektroniska signaturer eller i motsvarande certifikat som används i identifieringssyfte.	2) en annan i Finland etablerad certifikatutfärdare använder koden som en uppgift som identifierar innehavaren av certifikatet i certifikat som avses i lagen om stark autentisering och *betrodda elektroniska tjänster* eller i motsvarande certifikat som används i identifieringssyfte.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
61 §	61 §
Tjänster som tillhandahålls vid certifierad elektronisk kommunikation	*Tjänster som tillhandahålls vid certifierad elektronisk kommunikation*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Med medborgarcertifikat avses ett certifikat som utfärdats av Befolkningsregistercentralen för en fysisk person och som ingår i ett i lagen om identitetskort (829/1999) avsett identitetskort eller i en därmed jämförbar myndighetshandling eller ett tekniskt underlag och som används för verifiering av personen, för elektroniska signaturer och för kryptering av handlingar och meddelanden. Med medborgarcertifikat avses också ett av Befolkningsregistercentralen utfärdat certifikat som ingår i en annan myndighetshandling eller ett tekniskt underlag och som används i ovan nämnda syfte och som uppfyller kraven i 30 § i lagen om stark autentisering och elektroniska signaturer.	Med medborgarcertifikat avses ett certifikat som utfärdats av Befolkningsregistercentralen för en fysisk person och som ingår i ett i lagen om identitetskort (829/1999) avsett identitetskort eller i en därmed jämförbar myndighetshandling eller ett tekniskt underlag och som används för verifiering av personen, för elektroniska underskrifter och för kryptering av handlingar och meddelanden. Med medborgarcertifikat avses också ett av Befolkningsregistercentralen utfärdat certifikat som ingår i en annan myndighetshandling eller ett tekniskt underlag och som används i ovan nämnda syfte och uppfyller kraven *i EU:s förordning om elektronisk identifiering*.
62 §	62 §
Uppgifter som ska ingå i certifikat för certifierad elektronisk kommunikation	*Uppgifter som ska ingå i certifikat för certifierad elektronisk kommunikation*
Bestämmelser om vilka uppgifter som ska ingå i medborgarcertifikat och andra certifikat som Befolkningsregistercentralen utfärdar för fysiska personer finns i lagen om	*Bestämmelser om vilka uppgifter som ska ingå i medborgarcertifikat och andra certifikat som Befolkningsregistercentralen utfärdar för fysiska personer finns i lagen om*

stark autentisering och elektroniska signaturer. Medborgarcertifikat ska innehålla en elektronisk kommunikationskod som identifierar innehavaren av certifikatet. Andra certifikat som Befolkningsregistercentralen utfärdar för fysiska personer ska innehålla en elektronisk kommunikationskod som identifierar innehavaren av certifikatet eller någon annan identifikationsuppgift som identifierar personen och som inte innehåller information om personen. Även andra tekniska uppgifter som är nödvändiga vid användningen av ett certifikat kan ingå i medborgarcertifikat och andra certifikat som Befolkningsregistercentralen utfärdar för fysiska personer. Befolkningsregistercentralen beslutar om dessa uppgifter.

En elektronisk kommunikationskod kan också ingå i andra i lagen om stark autentisering och elektroniska signaturer avsedda certifikat för fysiska personer som en uppgift som identifierar innehavaren av certifikatet.

stark autentisering och betrodda elektroniska tjänster och i EU:s förordning om elektronisk identifiering. Medborgarcertifikat ska innehålla en elektronisk kommunikationskod som identifierar innehavaren av certifikatet. Andra certifikat som Befolkningsregistercentralen utfärdar för fysiska personer ska innehålla en elektronisk kommunikationskod som identifierar innehavaren av certifikatet eller någon annan identifieringsuppgift som identifierar personen och som inte innehåller information om personen. Även andra tekniska uppgifter som är nödvändiga vid användningen av ett certifikat kan ingå i medborgarcertifikat och andra certifikat som Befolkningsregister-centralen utfärdar för fysiska personer. Befolkningsregistercentralen beslutar om dessa uppgifter.

En elektronisk kommunikationskod kan också ingå i andra i lagen om stark autentisering och betrodda elektroniska tjänster avsedda certifikat för fysiska personer som en uppgift som identifierar innehavaren av certifikatet.

66 §

Ansökan om och utfärdande av medborgarcertifikat

— — — — — — — — — — — — — — — —

Den som tar emot ansökan ska iaktta de krav i personuppgiftslagen som gäller behandlingen av personuppgifter och de krav i lagen om stark autentisering och elektroniska signaturer som gäller utfärdande av certifikat.

66 §

Ansökan om och utfärdande av medborgarcertifikat

— — — — — — — — — — — — — — — —

Den som tar emot ansökan ska iaktta de krav i personuppgiftslagen som gäller behandlingen av personuppgifter och de krav i lagen om stark autentisering och *betrodda elektroniska tjänster och i EU:s förordning om elektronisk identifiering* som gäller utfärdande av certifikat.

67 §

Ansökan om och utfärdande av andra certifikat

Andra certifikat för fysiska personer som Befolkningsregistercentralen producerar och som inte är medborgarcertifikat kan utfärdas endast för finska medborgare samt för utlänningar som enligt lagen om hemkommun är stadigvarande bosatta i Finland och vars

67 §

Ansökan om och utfärdande av andra certifikat

Andra certifikat för fysiska personer som Befolkningsregistercentralen producerar och som inte är medborgarcertifikat kan utfärdas endast för finska medborgare samt för utlänningar som enligt lagen om hemkommun är stadigvarande bosatta i Finland och vars

uppgifter har registrerats i befolkningsdatasystemet och vars identitet har kunnat konstateras på ett tillförlitligt sätt. Andra certifikat än medborgarcertifikat som Befolkningsregistercentralen producerar för fysiska personer kan av särskilda och motiverade skäl också beviljas personer vars identitet har kunnat konstateras tillförlitligt även om de inte uppfyller övriga ovan nämnda villkor för att få certifikat. Sådana certifikat kan på sökandens begäran ingå i handlingar, kort och tekniska underlag som används vid elektronisk kommunikation och som utfärdas av en myndighet, ett företag eller en organisation. Befolkningsregistercentralen kan komma överens med en myndighet, ett företag eller en organisation som utfärdar handlingar eller tekniska underlag om att ansökningar om certifikat personligen kan lämnas in till myndigheten, företaget eller organisationen för vidarebefordran till Befolkningsregistercentralen. Befolkningsregistercentralen ska då se till att den som tar emot ansökan iakttar de krav i personuppgiftslagen som gäller behandlingen av personuppgifter och de krav i lagen om stark autentisering och elektroniska signaturer som gäller utfärdande av certifikat.	uppgifter har registrerats i befolkningsdatasystemet och vars identitet har kunnat konstateras på ett tillförlitligt sätt. Andra certifikat än medborgarcertifikat som Befolkningsregistercentralen producerar för fysiska personer kan av särskilda och motiverade skäl också beviljas personer vars identitet har kunnat konstateras tillförlitligt även om de inte uppfyller övriga ovan nämnda villkor för att få certifikat. Sådana certifikat kan på sökandens begäran ingå i handlingar, kort och tekniska underlag som används vid elektronisk kommunikation och som utfärdas av en myndighet, ett företag eller en organisation. Befolkningsregistercentralen kan komma överens med en myndighet, ett företag eller en organisation som utfärdar handlingar eller tekniska underlag om att ansökningar om certifikat personligen kan lämnas in till myndigheten, företaget eller organisationen för vidarebefordran till Befolkningsregistercentralen. Befolkningsregistercentralen ska då se till att den som tar emot ansökan iakttar de bestämmelser i personuppgiftslagen som gäller behandlingen av personuppgifter och de bestämmelser i *EU:s förordning om elektronisk identifiering som gäller utfärdande av certifikat*.
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
68 §	68 §
Ansökan om och utfärdande av certifikat i vissa fall	*Ansökan om och utfärdande av certifikat i vissa fall*
I stället för genom ett personligt besök kan ansökan om förnyande av ett medborgarcertifikat även göras elektroniskt och undertecknas med hjälp av ett medborgarcertifikat som sökanden använder och ansökan om förnyande av ett annat certifikat som Befolkningsregistercentralen producerar undertecknas med hjälp av ett certifikat enligt 30 § i lagen om stark autentisering och elektroniska signaturer som sökanden använder, om en sådan tjänst är i bruk. Vid behandlingen av ansökan iakttas i övrigt i tillämpliga delar de krav i fråga om utfärdande av certifikat som ställs i lagen om stark autentisering och elektroniska signaturer.	I stället för genom ett personligt besök kan ansökan om förnyande av ett medborgarcertifikat även göras elektroniskt och undertecknas med hjälp av ett medborgarcertifikat som sökanden använder, och ansökan om förnyande av ett annat certifikat som Befolkningsregistercentralen producerar undertecknas med hjälp av ett sådant kvalificerat certifikat enligt *EU:s förordning om elektronisk identifiering* som sökanden använder, om en sådan tjänst är i bruk. Vid behandlingen av ansökan iakttas bestämmelserna om utfärdande av certifikat i *EU:s förordning om elektronisk identifiering*.
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —

Denna lag träder i kraft den 20 .

7.

Lag

om ändring av lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården

I enlighet med riksdagens beslut

ändras i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) 2 § 3 mom., 9 § och 14 § 3 mom., sådana de lyder, 2 § 3 mom. i lag 250/2014, 9 § i lag 619/2009 och 14 § 3 mom. i lag 255/2015, som följer:

Gällande lydelse	*Föreslagen lydelse*
2 §	2 §
Tillämpningsområde	*Tillämpningsområde*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Om inte något annat följer av denna eller någon annan lag tillämpas på behandlingen av klientuppgifter vad som bestäms i lagen om patientens ställning och rättigheter (785/1992), nedan patientlagen, lagen om klientens ställning och rättigheter inom socialvården (812/2000), nedan klientlagen, personuppgiftslagen (523/1999), lagen om offentlighet i myndigheternas verksamhet (621/1999), lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003), lagen om stark autentisering och elektroniska signaturer (617/2009), lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009) och arkivlagen (831/1994) eller i bestämmelser som utfärdats med stöd av dem. Vid behandlingen av klientuppgifter och ordnande av tjänster och funktioner enligt denna lag ska dessutom iakttas vad som föreskrivs i språklagen (423/2003) och med stöd av den. Om det informationssystem där hälso- och sjukvårdens klient- och patientuppgifter behandlas är en sådan utrustning för hälso- och sjukvård som avses i lagen om produkter och utrustning för hälso- och sjukvård (629/2010) tilllämpas på informationssystemet även den lagen och kraven i enlighet med den.	Om inte något annat följer av denna eller någon annan lag tillämpas på behandlingen av klientuppgifter vad som föreskrivs i lagen om patientens ställning och rättigheter (785/1992), nedan patientlagen, lagen om klientens ställning och rättigheter inom socialvården (812/2000), nedan klientlagen, personuppgiftslagen (523/1999), lagen om offentlighet i myndigheternas verksamhet (621/1999), lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003), lagen om stark autentisering och *betrodda elektroniska tjänster* (617/2009), lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009) och arkivlagen (831/1994) eller i bestämmelser som utfärdats med stöd av dem. Vid behandlingen av kli-entuppgifter och ordnande av tjänster och funktioner enligt denna lag ska dessutom iakttas vad som föreskrivs i språklagen (423/2003) och med stöd av den. Om det informationssystem där hälso- och sjukvårdens klient- och patientuppgifter behandlas utgör sådan utrustning för hälso- och sjukvård som avses i lagen om produkter och utrustning för hälso- och sjukvård (629/2010) tillämpas på informationssystemet även den lagen och kraven i enlighet

med den.

9 §	9 §
Elektronisk signering av handlingar	*Elektronisk signering av handlingar*
Klientuppgifternas integritet, oförvanskade form och oavvislighet ska säkerställas med en elektronisk signatur vid elektronisk behandling, överföring och förvaring av uppgifterna. Vid elektronisk signering som görs av en fysisk person ska användas en avancerad elektronisk signatur enligt lagen om stark autentisering och elektroniska signaturer. Vid signering som görs av en organisation och datatekniska enheter ska användas en elektronisk signatur av motsvarande tillförlitlighet.	*Klientuppgifternas integritet, oförvanskade form och oavvislighet ska säkerställas med en elektronisk underskrift vid elektronisk behandling, överföring och förvaring av uppgifterna. Vid elektronisk signering som görs av en fysisk person ska det användas en sådan avancerad elektronisk underskrift som det föreskrivs om i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, nedan EU:s förordning om elektronisk identifiering. Vid signering som görs av en organisation och datatekniska enheter ska det användas en elektronisk underskrift av motsvarande tillförlitlighet.*
14 §	14 §
Riksomfattande informationssystemtjänster	*Riksomfattande informationssystemtjänster*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
Befolkningsregistercentralen är certifikatutfärdare enligt lagen om stark autentisering och elektroniska signaturer för yrkesutbildade personer inom social- och hälsovården och annan personal inom social- och hälsovården, tillhandahållare av social- och hälsovårdstjänster samt organisationer som deltar i tillhandahållandet av dessa tjänster, deras personal och datatekniska enheter. Befolkningsregistercentralen har rätt att för skötseln av dessa uppgifter av Tillstånds- och tillsynsverket för social- och hälsovården få den information som behövs för utfärdande och återkallande av certifikat, för certifikat, för det tekniska underlaget för certifikat och för sändande av certifikat, ur centralregistret över yrkesutbildade personer inom hälso- och sjukvården som verket upprätthåller. Tillstånds- och tillsynsverket för social- och hälsovården har på motsvarande sätt rätt att för	Befolkningsregistercentralen är certifikatutfärdare enligt lagen om stark autentisering och *betrodda elektroniska tjänster* för yrkesutbildade personer inom social- och hälsovården och annan personal inom social- och hälsovården, tillhandahållare av social- och hälsovårdstjänster samt organisationer som deltar i tillhandahållandet av dessa tjänster, deras personal och datatekniska enheter. Befolkningsregistercentralen har rätt att för skötseln av dessa uppgifter av Tillstånds- och tillsynsverket för social- och hälsovården få den information som behövs för utfärdande och återkallande av certifikat, för certifikat, för det tekniska underlaget för certifikat och för sändande av certifikat, ur centralregistret över yrkesutbildade personer inom hälso- och sjukvården som verket upprätthåller. Tillstånds- och tillsynsverket för social- och hälsovården har på motsvarande sätt rätt att för

skötseln av sina lagstadgade uppgifter av Befolkningsregistercentralen få information om de certifikat som centralen utfärdat på ovannämnda grunder. Informationen kan överlämnas med hjälp av en teknisk anslutning.	skötseln av sina lagstadgade uppgifter av Befolkningsregistercentralen få information om de certifikat som centralen utfärdat på ovannämnda grunder. Informationen kan överlämnas med hjälp av en teknisk anslutning.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —

———

Denna lag träder i kraft den 20 .

———

8.

Lag

om ändring av 93 a § i lagen om beskattningsförfarande

I enlighet med riksdagens beslut
ändras i lagen om beskattningsförfarande (1558/1995) 93 a § 2 mom., sådant det lyder i lag 623/2009, som följer:

Gällande lydelse	*Föreslagen lydelse*
93 a §	93 a §
Elektronisk kommunikation och signering	*Elektronisk kommunikation och signering*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Deklarationer och andra handlingar som får lämnas in till skattemyndigheten på elektronisk väg och som ska signeras ska certifieras med en avancerad elektronisk signatur som avses i lagen om stark autentisering och elektroniska signaturer (617/2009) eller på något annat godtagbart sätt.	Deklarationer och andra handlingar som får lämnas in till skattemyndigheten på elektronisk väg och som ska signeras ska certifieras med *en elektronisk underskrift* eller på något annat godtagbart sätt.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —

———

Denna lag träder i kraft den 20 .

———

9.

Lag

om ändring av 56 b § i lagen om överlåtelseskatt

I enlighet med riksdagens beslut
ändras i lagen om överlåtelseskatt (931/1996) 56 b § 2 mom., sådant det lyder i lag 622/2009, som följer:

Gällande lydelse	*Föreslagen lydelse*
56 b §	56 b §
Elektronisk kommunikation och signering	*Elektronisk kommunikation och signering*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
Deklarationer och andra handlingar som får lämnas in till skattemyndigheten på elektronisk väg och som ska signeras ska certifieras med en avancerad elektronisk signatur som avses i lagen om stark autentisering och elektroniska signaturer (617/2009) eller på något annat godtagbart sätt.	Deklarationer och andra handlingar som får lämnas in till skattemyndigheten på elektronisk väg och som ska signeras ska certifieras med *en elektronisk underskrift eller på något annat godtagbart sätt.*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —

———

Denna lag träder i kraft den 20 .

———

10.

Lag

om ändring av 6 a § i lagen om förskottsuppbörd

I enlighet med riksdagens beslut
ändras i lagen om förskottsuppbörd (1118/1996) 6 a § 2 mom., sådant det lyder i lag 624/2009, som följer:

Gällande lydelse	*Föreslagen lydelse*
6 a §	6 a §
Elektronisk kommunikation och signering	*Elektronisk kommunikation och signering*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Deklarationer och andra handlingar som får lämnas in till skattemyndigheten på elektronisk väg och som ska signeras ska certifieras med en avancerad elektronisk signatur som avses i lagen om stark autentisering och elektroniska signaturer (617/2009) eller på något annat godtagbart sätt.	Deklarationer och andra handlingar som får lämnas in till skattemyndigheten på elektronisk väg och som ska signeras ska certifieras med *en elektronisk underskrift eller på något annat godtagbart sätt.*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —

Denna lag träder i kraft den 20 .

11.

Lag

om ändring av 11 § i blodtjänstlagen

I enlighet med riksdagens beslut
ändras i blodtjänstlagen (197/2005) 11 §, sådan den lyder i lag 777/2009, som följer:

Gällande lydelse	*Föreslagen lydelse*
11 §	11 §
Uppgifter som hänför sig till blodgivare	*Uppgifter som hänför sig till blodgivare*
Den som ger blod och blodkomponenter ska före blodgivningen ges behövliga upplysningar som hänför sig till blodgivningen samt de uppgifter som avses i 24 § i personuppgiftslagen (523/1999). Blodgivaren ska informeras om sekretessen i fråga om uppgifterna. Av blodgivaren ska begäras identifieringsuppgifter, sådana uppgifter om hälsotillståndet som är nödvändiga när det gäller att bedöma blodgivarens lämplighet samt blodgivarens egenhändiga underskrift eller en avancerad elektronisk signatur enligt lagen om stark autentisering och elektroniska signaturer (617/2009). Säkerhets- och utvecklingscentret för läkemedelsområdet kan utfärda närmare föreskrifter om den information som ska ges till och inhämtas från blodgivare.	*Den som ger blod och blodkomponenter ska före blodgivningen ges behövliga upplysningar som hänför sig till blodgivningen samt de uppgifter som avses i 24 § i personuppgiftslagen (523/1999). Blodgivaren ska informeras om sekretessen i fråga om uppgifterna. Av blodgivaren ska begäras identifieringsuppgifter, sådana uppgifter om hälsotillståndet som är nödvändiga när det gäller att bedöma blodgivarens lämplighet samt blodgivarens egenhändiga underskrift eller en sådan avancerad elektronisk underskrift som det föreskrivs om i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG. Säkerhets- och utvecklingscentret för läkemedelsområdet kan utfärda närmare föreskrifter om den information som ska ges till och inhämtas från blodgivare.*

Denna lag träder i kraft den 20 .

12.

Lag

om ändring av 165 § i mervärdesskattelagen

I enlighet med riksdagens beslut
ändras i mervärdesskattelagen (1501/1993) 165 § 2 mom., sådant det lyder i lag 886/2009, som följer:

Gällande lydelse	*Föreslagen lydelse*
165 §	165 §
— — — — — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — — — — —
Deklarationer enligt 162 e § och andra handlingar som får lämnas in till skattemyndigheten på elektronisk väg och som ska signeras ska certifieras på det sätt som anges i lagen om stark autentisering och elektroniska signaturer (617/2009) med avancerad elektronisk signatur eller på något annat godtagbart sätt.	Deklarationer enligt 162 e § och andra handlingar som får lämnas in till skattemyndigheten på elektronisk väg och som ska signeras ska certifieras med *en elektronisk underskrift eller på något annat godtagbart sätt.*
— — — — — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — — — — —

———

Denna lag träder i kraft den 20 .

———

13.

Lag

om ändring av 7 § i skattekontolagen

I enlighet med riksdagens beslut

ändras i skattekontolagen (604/2009) 7 § 2 mom., sådant det lyder i lag 746/2009, som följer:

Gällande lydelse	*Föreslagen lydelse*
7 §	7 §
Inlämnande av periodskattedeklaration	*Inlämnande av periodskattedeklaration*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Den deklarationsskyldige ska underteckna periodskattedeklarationen. En periodskattedeklaration som lämnas in på elektronisk väg ska certifieras på det sätt som anges i lagen om stark autentisering och elektroniska signaturer (617/2009) med avancerad elektronisk signatur eller på något annat godtagbart sätt. Skatteförvaltningen utfärdar närmare föreskrifter om med hjälp av vilka elektroniska förfaranden och certifierings- eller identifieringsmetoder periodskattedeklaration kan lämnas in på elektronisk väg.	Den deklarationsskyldige ska underteckna periodskattedeklarationen. En periodskattedeklaration som lämnas in på elektronisk väg ska certifieras med *en elektronisk underskrift eller på något annat godtagbart sätt*. Skatteförvaltningen utfärdar närmare föreskrifter om med hjälp av vilka elektroniska förfaranden och certifierings- eller identifieringsmetoder periodskattedeklaration kan lämnas in på elektronisk väg.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
	Denna lag träder i kraft den 20 .

— — — — — — — — — — — — — — — — —

14.

Lag

om ändring av 4 § i lagen om informationssystemet för byggnaders energicertifikat

I enlighet med riksdagens beslut
ändras i lagen om informationssystemet för byggnaders energicertifikat (147/2015) 4 § 1 mom. som följer:

Gällande lydelse	*Föreslagen lydelse*
4 §	4 §
Upprättande och signering av energicertifikat	*Upprättande och signering av energicertifikat*
Ett energicertifikat upprättas genom att upprättaren för in de uppgifter som behövs för upprättandet av energicertifikatet i registret över energicertifikat och signerar energicertifikatet med en avancerad elektronisk signatur som avses i 5 § 2 mom. i lagen om stark autentisering och elektroniska signaturer (617/2009). Energicertifikatet betraktas som inlämnat hos tillsynsmyndigheten när det är undertecknat på det sätt som anges ovan.	Ett energicertifikat upprättas genom att upprättaren för in de uppgifter som behövs för upprättandet av energicertifikatet i registret över energicertifikat och signerar energicertifikatet med en sådan avancerad elektronisk *underskrift som det föreskrivs om i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG*. Energicertifikatet betraktas som inlämnat hos tillsynsmyndigheten när det är undertecknat på det sätt som anges ovan.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —

Denna lag träder i kraft den 20 .

15.

Lag

om ändring av 32 § i punktskattelagen

I enlighet med riksdagens beslut
ändras i punktskattelagen (182/2010) 32 § 3 mom., sådant det lyder i lag 495/2014, som följer:

Gällande lydelse	*Föreslagen lydelse*
32 §	32 §
Sätt att lämna in skattedeklaration	*Sätt att lämna in skattedeklaration*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
En elektronisk skattedeklaration ska certifieras *enligt 5 § 2 mom. i lagen om stark autentisering och elektroniska signaturer (617/2009)* eller på något annat godtagbart sätt. Den skattskyldige ska underteckna en skattedeklaration som lämnas in på en pappersblankett.	En elektronisk skattedeklaration ska certifieras *med en elektronisk* underskrift eller på något annat godtagbart sätt. Den skattskyldige ska underteckna en skattedeklaration som lämnas in på en pappersblankett.
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —

Denna lag träder i kraft den 20 .