RP 36/2009 rd

Regeringens proposition till Riksdagen med förslag till lag om stark autentisering och elektroniska signaturer samt till vissa lagar som har samband med den

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås det att det stiftas en lag om stark autentisering och elektroniska signaturer. Samtidigt föreslås det att lagen om elektroniska signaturer upphävs.

I största delen av elektroniska tjänster behövs varken elektronisk identifiering eller elektroniska signaturer. I en del av elektroniska tjänster kan man ändå bl.a. företa olika rättshandlingar. Sådana elektroniska tjänster förutsätter att parterna har förtroende för varandra på ett helt annat sätt än när ärenden sköts genom fysisk närvaro. Den som använder tjänsterna ska bl.a. kunna lita på att tjänsteleverantören har byggt upp sin service så att kraven på informationssäkerhet och integritetsskydd har beaktats. Tjänsteleverantören ska å sin sida bl.a. kunna lita på att den som använder tjänsterna via en fjärranslutning är den som han eller hon ger sig ut för att vara. För att de elektroniska tjänsterna och den elektroniska kommunikationen ska kunna utvecklas förutsätts att det framöver finns välfungerande tjänster för elektronisk identifiering.

Syftet med bestämmelserna är att ge grundläggande förutsättningar för att tillhandahålla tjänster för stark autentisering i Finland. Ett annat syfte är att skapa en ram för en fungerande marknad för stark autentisering.

Den föreslagna lagen gäller stark autentisering. Svag autentisering omfattas således inte av bestämmelserna. Stark autentisering tillämpas vid identifiering av fysiska personer. Utanför regleringen faller metoder för sådan stark autentisering som används i slutna miljöer, såsom metoder för ett företags egna behov av identifiering.

Den föreslagna lagen innehåller bestämmelser om de krav som en elektronisk identifiering ska uppfylla för att vara stark autentisering. I lagen föreslås också bestämmelser om de krav som gäller leverantörer av tjänster för stark autentisering och leverantörernas tjänster. Tillhandahållandet av tjänster för stark autentisering övervakas av Kommunikationsverket.

Den föreslagna lagens bestämmelser om elektroniska signaturer motsvarar den gällande lagen om elektroniska signaturer.

Genom de övriga lagar som ingår i propositionen ändras hänvisningarna till lagen om elektroniska signaturer till hänvisningar till lag om stark autentisering och elektroniska signaturer. De föreslagna lagarna avses träda i kraft den 1 september 2009.

294504

INNEHÅLLSFÖRTECKNING

ALLMÄN MOTIVERING

1 Inledning

I Finland liksom även i det övriga Europa har utvecklingen av de elektroniska tjänsterna och den elektroniska kommunikationen varit långsammare än vad som förväntades i början av det nya årtusendet. Trots det börjar det finnas tillräckligt med erfarenheter för att efterfrågan på elektroniska tjänster nu kan börja öka markant. Den ökade efterfrågan beror på de fördelar som de elektroniska tjänsterna för med sig för användarna: ärendena kan skötas hemifrån, utan köer och öppettider.

Det bedöms att efterfrågan på elektroniska tjänster kommer att öka kraftigt under de närmaste åren och syftet är att stödja denna utveckling också genom det allmännas omfattande åtgärder. Enligt regeringsprogrammet främjar regeringen medborgarnas och företagens förtroende för vardagens informationssamhällstjänster. Ett sätt att främja detta förtroende är att revidera lagstiftningen om användarvänlig elektronisk identifiering.

Elektronisk identifiering möjliggör en mångsidig användning av elektroniska tjänster och elektronisk kommunikation. Det ökade antalet tjänster och särskilt deras mångfald kräver i framtiden allt oftare tillförlitlig elektronisk identifiering. För tillfället pågår några lagstiftningsprojekt, där planen är att tillförlitlig elektronisk identifiering ska vara en förutsättning för tjänster som erbjuds genom fjärranslutning. Denna typ av lagstiftning torde öka betydligt under de närmaste åren. För att systemet ska fungera måste det också finnas ett sådant regelverk som definierar tillförlitlig elektronisk identifiering och de grundläggande förutsättningarna för att tillhandahålla tjänster.

För att användningen av användarvänlig stark autentisering ska kunna öka i betydande mån i Finland måste förutsättningar för en fungerande marknad för tjänster för stark autentisering skapas i landet. Den föreslagna lagen, som reglerar de grundläggande principerna för tillhandahållande av tjänster, bidrar till att en sådan marknad kan växa fram.

2 Nuläge

2.1 Lagstiftning

I Finland finns ingen lag där tillämpningsområdet anges gälla elektronisk identifiering. Lagen om elektroniska signaturer gäller elektroniska signaturer och från lagens bestämmelser om certifikat har man försökt härleda bestämmelser som även gäller elektronisk identifiering som bygger på certifikat. Dessutom finns det många andra lagar som påverkar användningen av stark autentisering och elektroniska signaturer. Sådana lagar är i synnerhet lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003), lagstiftningen om befolkningsregistret och Befolkningsregistercentralens certifikattjänster och personuppgiftslagen (523/1999).

Lagen om elektroniska signaturer

Lagen om elektroniska signaturer grundar sig på Europaparlamentets och rådets direktiv om ett gemenskapsramverk för elektroniska signaturer. I enlighet med sitt tillämpningsområde gäller lagen endast elektroniska signaturer. Enligt 2 § 1 punkten i lagen avses med elektronisk signatur data i elektronisk form som är fogade till eller logiskt knutna till andra elektroniska data och som används som en metod för verifiering av undertecknarens identitet.

Enligt 2 punkten i samma paragraf avses med avancerad elektronisk signatur en elektronisk signatur som är knuten uteslutande till undertecknaren, gör det möjligt att identifiera undertecknaren, är skapad med medel som endast undertecknaren kontrollerar och är knuten till andra elektroniska data på ett sådant sätt att eventuella senare förvansk-

ningar av dessa data kan upptäckas. Enligt definitionen i lagen avses med certifikat ett intyg i elektronisk form som kopplar ihop signaturverifieringsdata med en undertecknare och bekräftar undertecknarens identitet.

Bestämmelserna i 5 § om säkra anordningar för signaturframställning gäller alla certifikat. Största delen av lagens bestämmelser gäller dock endast kvalificerade certifikat och certifikatutfärdare som tillhandahåller kvalificerade certifikat. Med kvalificerat certifikat avses ett certifikat som har utfärdats av en sådan certifikatutfärdare som avses i 10-15 §. Kännetecken på kvalificerade certifikat är också uppgift om att certifikatet är ett kvalificerat certifikat, uppgift om certifikatutfärdaren och dennes etableringsstat, undertecknarens namn eller pseudonym med uppgift om att det är en pseudonym, signaturverifieringsdata som motsvarar de signaturframställningsdata som undertecknaren innehar, det kvalificerade certifikatets giltighetstid, det kvalificerade certifikatets identifieringskod, certifikatutfärdarens avancerade elektroniska signatur, eventuella begränsningar i fråga om användningen av det kvalificerade certifikatet, samt särskilda uppgifter om undertecknaren, om de behövs med tanke på ändamålet med det kvalificerade certifikatet.

I lagens 18 § konstateras att om det beträffande en rättshandling i lag ställs krav på 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. På grund av ordalydelsen anges det inte entydigt i lagen att rättsverkan inte skulle kunna uppnås även med andra medel än med en avancerad elektronisk signatur som har skapats med ett kvalificerat certifikat. Genom paragrafen genomförs artikel 5 i direktivet om ett gemenskapsramverk för elektroniska signaturer. I artikel 5.2 i direktivet föreskrivs att en elektronisk signatur inte kan förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att signaturen är i elektronisk form, inte är baserad på ett kvalificerat certifikat eller inte är skapad av en säker anordning för skapande av signaturer.

Lagen om elektronisk kommunikation i myndigheternas verksamhet

Lagen om elektronisk kommunikation i myndigheternas verksamhet tillämpas när anhängiggörande och behandling av förvaltningsärenden, domstolsärenden, åtalsärenden och utsökningsärenden samt delgivning av beslut i nämnda ärenden sker på elektronisk väg. Lagen gäller i tillämpliga delar också annan myndighetsverksamhet. Enligt lagens 5 § ska en myndighet som har behövlig teknisk, ekonomisk och övrig beredskap inom ramen för den erbjuda var och en möjlighet att i syfte att anhängiggöra ärenden eller för behandlingen av dem sända meddelanden till en elektronisk adress eller specificerad anordning angivna av myndigheten. I nämnda fall ska dessutom var och en erbjudas möjlighet att i elektronisk form sända myndigheten anmälningar som den enligt gällande bestämmelser ska tillställas, utredningar och andra motsvarande handlingar som den begärt samt andra meddelanden.

Enligt regeringens proposition (RP 17/2002) ska myndigheternas skyldighet att anordna elektronisk service stå i proportion till det kunnande, den skicklighet och de ekonomiska resurser som myndigheten förfogar över. En ovillkorlig skyldighet att tillhandahålla elektronisk service ansågs inte kunna åläggas myndigheterna, eftersom lagens tillämpningsområde är vidsträckt och myndigheternas resurser varierar.

I lagens 9 § föreskrivs att 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 18 § i lagen om elektroniska signaturer. Ett elektroniskt dokument som inkommit 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. Enligt 16 § kan en beslutshandling signeras elektroniskt. En myndighets elektroniska signatur ska uppfylla kraven i 18 § lagen om elektroniska signaturer.

Befolkningsdatalagen

I 5 kap. i befolkningsdatalagen (507/1993) finns bestämmelser om tjänster som gäller certifierad elektronisk kommunikation. Enligt 19 § i lagen ska Befolkningsregistercentralen sörja för att parterna vid certifierad elektronisk kommunikation inom statsförvaltningen kan verifieras samt att handlingar och meddelanden inom förvaltningen vid behov kan undertecknas med elektronisk signatur och krypteras. Befolkningsregistercentralen kan tillhandahålla andra myndigheter, företag, sammanslutningar och enskilda personer motsvarande tjänster.

I 4 § i befolkningsdatalagen föreskrivs det om de uppgifter som registreras i befolkningsdatasystemet i fråga om finska medborgare. Enligt 1 punkten är sådana uppgifter bl.a. personbeteckning och den elektroniska kommunikationskod som ingår i medborgarcertifikatet. I lagens 21 § bestäms om den elektroniska kommunikationskoden och i 22 och 23 § om medborgarcertifikatet. Enligt 21 § 3 mom. ändras den tekniska identifieringsuppgiften till en elektronisk kommunikationskod för en person när ett certifikat utfärdas för honom eller henne.

I lagens 6 kap. bestäms om utlämnande av uppgifter som registrerats i befolkningsdatasystemet. Bestämmelserna innehåller inte några sådana begränsningar för utlämnande av uppgifter som gäller den elektroniska kommunikationskoden. Befolkningsregistercentralen har dock tolkat den gällande lagen så, att den inte har gått med på att lämna ut uppgifter om den elektroniska kommunikationskoden. Projektet för en totalreform av befolkningsdatalagen är under arbete. I samband med den avgörs bl.a. frågan om möjligheten att använda den elektroniska kommunikationskoden i andra än Befolkningsregistercentralens certifikat.

Personuppgiftslagen

Personuppgiftslagen tillämpas allmänt på all behandling av personuppgifter. Jämfört med regleringen enligt personuppgiftslagen innehåller den föreslagna lagen i viss mån preciseringar som gäller behandlingen av personuppgifter. I regel finns dock bestämmelserna om behandling av personuppgifter i den allmänna lagen.

Således ska bl.a. lagens bestämmelser om behandling av personuppgifter och om den registeransvariges skyldigheter iakttas även när tjänster för stark autentisering tillhandahålls. Med tanke på den föreslagna lagen är personuppgiftlagens bestämmelser om aktsamhetsplikt i 5 §, upplysningsplikt i 24 § och skydd av uppgifter i 32 § av särskild vikt.

Annan lagstiftning och anvisningar

Utöver den ovan nämnda lagstiftningen kan det finnas behov av att beakta även annan lagstiftning, såsom lagen om offentlighet i myndigheternas verksamhet (621/1999) och lagen om integritetsskydd i arbetslivet (759/2004).

Det finns inga allmänna bestämmelser om vilka tjänster som förutsätter stark autentisering. Sådana bestämmelser kan finnas i enstaka lagar och det verkar som om denna typ av bestämmelser håller på att öka i antal. I samband med kommunikationsministeriets tvååriga program ”Förtroende och informationssäkerhet i elektroniska tjänster”, dvs. LUOTI-programmet, ansågs stark autentisering allmänt taget komma i fråga i samband med ekonomiska eller rättsliga förbindelser och sådana elektroniska tjänster som förutsätter hantering av konfidentiella uppgifter, såsom känsliga personuppgifter enligt personuppgiftslagen eller en organisations sekretessbelagda uppgifter. Enligt finansministeriets anvisning 12/2006 behövs stark autentisering inom den offentliga sektorn i samband med konfidentiella interaktiva kommunikationstjänster och utbyte av information mellan datasystemen, dvs. i program-till-program-kommunikation.

2.2 Praxis

Elektronisk identifiering

Kommunikationsministeriet har tillsatt en utvecklingsgrupp för elektronisk identifiering, som lyder under delegationen för vardagens informationssamhälle. Utvecklingsgruppen utarbetade i september 2008 natio-

nella riktlinjer för stark autentisering. I riktlinjerna beskrivs den miljö som den fortsatta utvecklingen av stark autentisering i Finland förankras i. Riktlinjerna innehåller i sig ingenting nytt, utan de grundar sig på rådande praxis. Det viktiga är dock att alla infallsvinklar i ämnet presenteras i samma dokument. De nationella riktlinjerna för stark autentisering antogs i oktober 2008 av delegationen för vardagens informationssamhälle, i vilken ingår de aktörer inom den offentliga och privata sektorn som är de viktigaste med tanke på utvecklandet av elektronisk identifiering.

I den första punkten i riktlinjerna konstateras behovet av att skapa förutsättningar för en fungerande marknad för stark autentisering i Finland. Kännetecknande för en sådan marknad är identifieringsverktygens allmänna användbarhet och fri konkurrens.

I allmänhet anses en stark autentisering bestå av något som användaren vet, såsom användaridentifikation, något som användaren har, såsom en lösenordslista eller en dosa, ett certifikat eller annan utrustning som genererar engångskoder, eller något som användaren är, t.ex. fingeravtryck. För att en identifiering ska motsvara definitionen av stark autentisering ska minst två av dessa krav uppfyllas samtidigt.

I dagens läge tillhandahålls finländska konsumenter tjänster för stark autentisering av bankerna och Befolkningsregistercentralen. En av de klart mest använda metoderna för stark autentisering är bankernas identifieringskoder. På marknaden finns för närvarande mer än fyra miljoner bankkoder och ca 150 000 medborgarcertifikat som tillhandahålls av Befolkningsregistercentralen. Upp till 99 procent av identifieringstransaktionerna görs med bankkoder.

I den andra punkten i riktlinjerna anges det att en viktig förutsättning för att en marknad för stark autentisering ska växa fram och fungera är att parterna bedriver ett effektivt samarbete. Det behövs ett öppet samarbete som vid behov ska stödjas aktivt. Samtidigt ska man se till att samarbetsarrangemangen inte hindrar den fria konkurrensen.

I motiveringen till den andra punkten i riktlinjerna sägs det att internationella exempel från bl.a. Turkiet, Estland och Norge visar att det i de länder där elektronisk identifiering har framskridit bättre än i jämförelseländerna har funnits fungerande samarbetsarrangemang mellan två eller flera parter. Traditionen med samarbete mellan den privata och offentliga sektorn har av hävd varit Finlands starka sida. För att skapa en fungerande marknad behövs det samarbetsarrangemang som är öppna för alla aktörer. På marknaden uppstår också eventuellt några center för identifiering eller verifiering. På längre sikt kan dessa center eventuellt ha verksamhet på internationell nivå. Vid behov ska skapandet av denna typ av samarbetsarrangemang stödjas aktivt. Samtidigt ska man se till att samarbetsarrangemangen inte hindrar den fria konkurrensen.

I den tredje punkten i riktlinjerna konstateras det att man inom elektronisk identifiering skiljer på stark och svag autentisering. I lagstiftningen anges ramarna för regleringen av tillhandahållande av tjänster för stark autentisering. I motiveringen konstateras det att en fysisk person endast kan ha en faktisk identitet som är kopplad till personen som rättssubjekt. Vid svag autentisering kan en person själv skapa sig eller ges flera elektroniska s.k. identiteter, som också kan avvika från personens faktiska egenskaper. Personen kan uppge felaktiga uppgifter om t.ex. sin ålder eller sitt kön.

Kännetecknande för stark autentisering är däremot att identifieringsverktyget och användningen av det i sista hand alltid kan kopplas till en persons faktiska identitet. Detta är möjligt trots att en tjänsteleverantör som använder stark autentisering inte får information om de faktiska personuppgifterna i samband med användningen. Det är således fråga om s.k. anonym användning. Även vid stark autentisering kan en person ha flera roller som han eller hon använder och det är möjligt att koppla ett varierande antal uppgifter till personen i olika tjänster. En person kan dock endast ha en identitet, som i Finland skapas av staten.

Det förfarande som beskrivs i det föregående stycket kan i Finland göras ännu effektivare så att verktyg för stark autentisering innehåller en persons personbeteckning eller elektroniska kommunikationskod, som används som unika identifikatorer. I den total-

reform av befolkningsdatalagen som för närvarande är under behandling i riksdagen föreslås sådana ändringar som förändrar den nuvarande situationen och gör det möjligt för certifikatutfärdaren att använda elektroniska kommunikationskoder i certifikaten. Med hjälp av information, reglering och andra medel som behövs ska tjänsteleverantörer som tillhandahåller stark autentisering uppmuntras att använda personbeteckningar och elektroniska kommunikationskoder, med beaktande av bestämmelserna om personuppgifter.

Enligt den fjärde punkten i riktlinjerna grundar sig tillförlitligheten hos stark autentisering på den metod som används, säkra och reviderbara processer och genomförandesätt, lagstadgade grundläggande förutsättningar för tillhandahållande av tjänster för stark autentisering, förtroendenät som bildas av tjänsteleverantörer som tillhandahåller och använder tjänster för stark autentisering och på myndighetsövervakning. En stark autentisering som skapas på detta sätt lämpar sig i princip för all tillförlitlig elektronisk identifiering både inom den privata och inom den offentliga sektorn.

I motiveringen till den fjärde punkten konstateras det att i det finländska systemet ska marknaden, dvs. tjänsteleverantörer som tillhandahåller och använder tjänster för stark autentisering och slutanvändarna, själva besluta om en eventuell klassificering av metoderna och verktygen för stark autentisering och om användningen av klassificeringen. I den finländska lagstiftningen räcker det med indelningen i svag autentisering, som i praktiken är oreglerad, och stark autentisering, som ska börja regleras genom lagstiftning.

I den femte punkten i riktlinjerna konstateras det att användarnas förtroende för tjänster för stark autentisering också förutsätter att tjänsteleverantörer som tillhandahåller och använder stark autentisering ser till att bestämmelserna om konsumentskydd och integritetsskydd följs noggrant.

Enligt den sjätte punkten i riktlinjerna köper tjänsteleverantörerna inom den privata och offentliga sektorn de tjänster för elektronisk identifiering som de behöver på en fungerande marknad för stark autentisering. Tjänsteleverantörerna kan välja de tjänster för stark autentisering som de använder. Den offentliga makten begränsar inte denna valmöjlighet utom i vissa särskilda undantagsfall.

I motiveringen till den sjätte punkten konstateras det att tjänsteleverantörer såväl inom den offentliga som inom den privata sektorn ska ha valfrihet. Det väsentliga är att den offentliga makten inte begränsar denna möjlighet utom eventuellt i några mycket sällsynta undantagsfall. Även i dessa fall förutsätts alltid att undantagen är objektiva, tydliga, proportionella och icke-diskriminerande och endast gäller den berörda tjänstens särskilda egenskaper.

Inom den offentliga sektorn kan denna valmöjlighet i viss mån begränsas på grund av den gällande lagstiftningen. Beroende på ärendet kan beaktande av t.ex. konkurrenslagstiftningen eller lagstiftningen om offentlig upphandling eller elektronisk kommunikation i myndigheternas verksamhet komma i fråga. Dessutom bör det beaktas att finansministeriet styr de identifieringslösningar som används i den offentliga förvaltningens e-tjänster. Även ledningsgruppen för datasäkerheten inom statsförvaltningen VAHTI ger rekommendationer och anvisningar.

I vissa fall kan situationen vara den att en aktör behöver sådana metoder, verktyg eller tjänster för stark autentisering som inte finns på marknaden. Då kan aktören bli tvungen att utveckla det verktyg eller den tjänst som behövs.

I den sjunde punkten i riktlinjerna konstateras det att utbudet av tjänster för stark autentisering grundar sig på ett användarperspektiv. Alla användare kan själva välja den lämpligaste identifieringsmetoden av det utbud av metoder för stark autentisering som finns på marknaden. Målet är att var och en ska kunna använda den mest passande metoden för stark autentisering i så många som möjligt av de tjänster som kräver identifiering. Samtidigt ska dock den föregående riktlinjen beaktas.

Enligt motiveringen till den sjunde punkten bör användarperspektivet även i praktiken vara en av de grundläggande utgångspunkterna vid stark autentisering. Användarna måste kunna välja en sådan metod för stark autentisering som de själva tycker känns

bäst. Valet baserar sig ofta på användarens tidigare användarerfarenhet. Målet är en fungerande marknad som erbjuder några alternativa verktyg för stark autentisering, så att olika typer av användare kan hitta det verktyg som passar dem bäst.

En smidig användning av elektronisk identifiering förutsätter att användarna hela tiden får tillräckliga erfarenheter av användningen av en identifieringsmetod. Om det krävs att en användare i praktiken ska kunna hantera flera olika verktyg för elektronisk identifiering är användningen per verktyg inte tillräcklig för att garantera tillräcklig rutin och därmed en bekväm användning. En användare kan givetvis skaffa sig flera verktyg om han eller hon så önskar.

Stark autentisering är säkrare att använda än svag autentisering såväl för användaren som för tjänsteleverantören. Metoderna för stark autentisering är bättre än metoderna för svag autentisering t.ex. när det gäller att bekämpa identitetsstölder. Därför bör det slutliga målet vara att användarna kan använda en bekant och lättanvänd metod för stark autentisering även i samband med sådana tjänster som i sig inte nödvändigtvis kräver stark autentisering. För att uppnå detta mål måste kostnadsnivån för stark autentisering vara tillräckligt låg för alla aktörer. Ett av målen för en fungerande marknad är också en skälig prisnivå, som kan nås om det finns tillräckligt med alternativ på marknaden.

Även om målet är att alla användare ska kunna använda det verktyg för stark autentisering som de valt i samband med så många tjänster som möjligt, kan tjänsteleverantörerna dock inte tvingas godkänna ett visst verktyg eller en viss leverantör av tjänster för stark autentisering. Således ska det som konstateras i den föregående riktlinjen om tjänsteleverantörernas valmöjlighet beaktas. Sannolikt kommer det att finnas endast ett begränsat antal tjänsteleverantörer och verktyg för stark autentisering på den finländska marknaden. Därför torde det inte heller vara ett problem att samordna intressena hos de tjänsteleverantörer som använder stark autentisering och slutanvändarna.

I den åttonde punkten i riktlinjerna konstateras det faktiskt rådande rättsläget som innebär att en rättshandling kan utföras elektroniskt både genom elektroniska signaturer och genom verktyg för stark autentisering, om parterna så önskar.

I motiveringen konstateras det att man bör göra en tydlig begreppsmässig åtskillnad mellan stark autentisering, elektronisk signatur och utförande av en rättshandling elektroniskt. Vid stark autentisering bildar de tjänsteleverantörer som tillhandahåller och använder identifieringstjänster i allmänhet ett nätverk som regleras genom ett avtalsförhållande. I fråga om elektroniska signaturer är den grundläggande utgångspunkten däremot att leverantören av tjänster för elektroniska signaturer inte står i ett avtalsförhållande med den part som förlitar sig på signaturen. Definitionsmässigt innefattar en elektronisk signatur enligt direktivet om ett gemenskapsramverk för elektroniska signaturer alltid också ett identifieringselement. Enligt direktivet om ett gemenskapsramverk för elektroniska signaturer syftar definitionen av elektroniska signaturer till att vara tekniskt neutral, men i praktiken avser definitionen endast elektroniska signaturer som baseras på ett system med öppen nyckel.

Den viljeförklaring som ligger till grund för en rättshandling ska särskiljas från elektronisk signatur. Detta är särskilt viktigt i Finland, där mycket få rättshandlingar omfattas av vissa formkrav. Om en rättshandling bestrids har domstolarna i Finland fri bevisprövning. Den viljeförklaring som en rättshandling förutsätter kan i Finland avges genom att man använder elektronisk signatur eller metoder för stark autentisering, om parterna så önskar och det inte föreskrivs om några särskilda formkrav för rättshandlingen någon annanstans i lag. I Finland är det mycket sällsynt med sådana formkrav. Ingen part kan generellt eller i ett enskilt fall tvingas att utföra en rättshandling med verktyg för stark autentisering, men de som vill ha ett sådant alternativ ska ges en möjlighet till det. Det är viktigt att slutanvändarna och tjänsteleverantörerna är likställda. Tjänsteleverantören ska bl.a. se till att användaren faktiskt är medveten om att han eller hon utför en rättshandling och även känner till alla andra omständigheter som gäller en tjänst.

I den nionde punkten i riktlinjerna konstateras det att elektronisk identifiering inte är

själva syftet utan gör tillförlitlig elektronisk kommunikation möjlig. Det finns även tjänster där identifiering inte alls behövs. Tjänsteleverantörer som använder stark autentisering ska särskilja de tjänster som kräver identifiering.

I motiveringen till den nämnda punkten konstateras det att en stor del av de elektroniska tjänsterna är sådana som inte alls kräver elektronisk identifiering. I viss mån har det förekommit överdrifter och man har krävt identifiering även i samband med tjänster där det inte är nödvändigt.

Tjänsteleverantörerna inom den privata sektorn har också skäl att överväga om det är möjligt att minska på användningen av svag autentisering även på så sätt att fler tjänster skulle vara öppna för användarna. På grund av sina särdrag måste den offentliga sektorn särskilja de tjänster som kan förutsätta identifiering.

Enligt den sista, dvs. tionde, punkten i riktlinjerna ska Finland sträva efter att aktivt främja dessa principer även inom EU och på det internationella planet.

Statsrådets principbeslut om elektronisk identifiering

Statsrådet godkände den 5 mars 2009 ett principbeslut om elektronisk identifiering. Syfte med beslutet är att komma överens om den interna arbetsfördelningen inom statsrådet på området för elektronisk identifiering när det gäller de nödvändiga åtgärder som för närvarande är i sikte.

Med tanke på den fortsatta utvecklingen av elektronisk identifiering anses det aktuella lagförslaget vara viktigt, liksom även det att utvecklingsgruppen för elektronisk identifiering år 2009 utarbetar en handlingsmodell för användning och hantering av elektronisk identifiering, som baserar sig på internationella öppna standarder. Utifrån resultaten av det projekt för omorganisering av statens certifikatproduktion som finansministeriet ansvarar för kommer den fortsatta utvecklingen av tjänsterna att inledas i slutet av 2009.

I fråga om styrning och samverkan inom den offentliga sektorn är avsikten att finansministeriet under 2009 ska inleda ett lagstiftningsarbete i syfte att utarbeta ny bindande reglering om styrningen av elektroniska tjänster inom den offentliga sektorn. Under år 2009 ska finansministeriet dessutom göra upp en plan om byggande av en gemensam förmedlingstjänst för den offentliga sektorn och bereda de anskaffningar som hör till planen.

Med tanke på helheten är det ytterst viktigt att lösningarna för identifiering av företag och andra organisationer vidareutvecklas. I anslutning till det kommer finansministeriet, arbets- och näringsministeriet och kommunikationsministeriet att inleda ett projekt för att utvärdera fortsättningen av Skatteförvaltningens Katso-system och för att utarbeta en plan för utvidgningen av användningen av Patent- och registerstyrelsens rollinformationstjänst. I projektet ska det också utvärderas hur andra aktörer kan utnyttja Patent- och registerstyrelsens uppgifter i sina egna tjänster.

I fråga om identifieringen av tjänstemän fortsätter Kommunförbundet och finansministeriet VIRTU-projekten och ser till att verksamheten inleds. Utifrån resultaten av projektet för omorganisering av statens certifikatproduktion tillsätter finansministeriet dessutom ett projekt för identifieringslösningar, t.ex. införande av ett tjänstekort, och har hand om de nödvändiga anvisningarna.

Enligt principbeslutet är målet också att social- och hälsovårdsministeriet omvärderar Tillstånds- och tillsynsverket för social- och hälsovårdens (Valviras) roll som producent av certifikattjänster så snabbt som möjligt efter det att finansministeriet har slutfört projektet för omorganisering av statens certifikatproduktion.

I fråga om identitetsstölder granskas stöld av en persons identifieringsuppgifter och användningen av falsk identitet som fenomen inom programmet för den inre säkerheten och identitetsprogrammet. Programmen leds av inrikesministeriet. I projekten redogörs det bl.a. för i vilka former dessa fenomen kan uppträda och vilket hot de utgör mot medborgarna nu och i framtiden. Dessutom redogörs det för hur den nuvarande lagstiftningen, speciellt strafflagen, bemöter dessa problem och om det finns behov av ytterligare reglering.

Justitieministeriet kommer för sin del att år 2009 tillsätta en arbetsgrupp med uppgift att utreda användningen av biometriska känne-

tecken vid elektronisk identifiering. I arbetsgruppen finns åtminstone kommunikationsministeriet, inrikesministeriet och finansministeriet representerade.

Elektroniska signaturer

Med elektronisk signatur avses data i elektronisk form som är fogade till eller logiskt knutna till andra elektroniska data och som används som en metod för verifiering av undertecknarens identitet utanför det ramverk för elektronisk identifiering som tjänsteleverantörerna bildar. Certifikatutfärdaren spelar en viktig roll vid elektronisk signering. Tillförlitligheten hos en elektronisk signatur bygger på att någon aktör, i allmänhet en certifikatutfärdare, försäkrar sig om undertecknarens identitet. Den part som förlitar sig på den elektroniska signaturen kan identifiera undertecknaren med hjälp av det certifikat som certifikatutfärdaren utfärdat för undertecknaren.

Den teknik som för närvarande används mest vid elektronisk signering bygger på en metod med öppna nycklar. Underskriften, certifikatet och certifikatutfärdaren bildar tillsammans den öppna nyckelns infrastruktur. Nedan ges en beskrivning av metoden med öppna nycklar i syfte att klarlägga certifikatutfärdarens ställning i användningen av elektroniska signaturer.

Metoden med öppna nycklar använder sig av s.k. nycklar, dvs. bitsträngar, där den ena nyckeln är privat och den andra är öppen. I systemet förlitar man sig på certifikatutfärdaren, som i certifikatet kopplar en viss person till en öppen nyckel. I praktiken har användaren alltså två nycklar, en privat och en öppen. Dessa nycklar samverkar så att information som krypterats med hjälp av den öppna nyckeln kan öppnas med den privata nyckeln i nyckelparet och tvärtom. Den öppna nyckeln är som namnet anger tillgänglig för alla, t.ex. i en katalog som certifikatutfärdaren upprätthåller. Den privata nyckeln innehas av undertecknaren. Den öppna och den privata nyckeln är kopplade till varandra genom en komplicerad matematisk ekvation på ett sådant sätt att det i praktiken inte går att härleda den privata nyckeln ur den öppna nyckeln eller tvärtom. Ju längre nyckelserier som används desto säkrare är systemet. Kryptering som bygger på öppna och privata nycklar kallas asymmetrisk kryptering och möjliggör inte bara kryptering utan också framställning av elektroniska signaturer.

Elektroniska signaturer bygger inte bara på metoden med öppna nycklar utan också på en s.k. hashfunktion. Detta innebär att information av godtycklig längd omskapas till en bestämd längd, ett hashvärde. Den elektroniska signeringen genomförs så att den person som ska underteckna informationen kondenserar datamängden och krypterar denna med hjälp av sin privata nyckel. Informationen och det krypterade hashvärdet skickas till mottagaren som dekrypterar hashvärdet med sin öppna nyckel och bearbetar den mottagna informationen, dvs. skapar ett hashvärde med hjälp av sin egen programvara för verifiering av signaturen. Genom att jämföra dessa två hashvärden med varandra kan mottagaren vara säker på informationens integritet, dvs. att den inte förvanskats.

Att det krypterade hashvärdet kan öppnas med undertecknarens öppna nyckel visar att undertecknaren förfogar över den privata nyckel som hör samman med den öppna nyckeln. Eftersom den öppna nyckeln är certifierad, dvs. en tredje part har utfärdat ett certifikat för undertecknaren och verifierat att den öppna nyckeln i fråga motsvaras endast och uteslutande av den privata nyckel som undertecknaren har använt, kan mottagaren vara säker på att informationen har signerats av den person som uppges i certifikatet. Certifikatet och den öppna nyckeln kan t.ex. skickas antingen tillsammans med informationen eller den kan hämtas av mottagaren i certifikatutfärdarens katalogtjänst.

Elektroniska signaturer används i en teknisk användarmiljö. Själva åtgärderna, undertecknandet och verifieringen samt t.ex. användningen av katalogtjänsterna är främst normal användning av programvara för användaren. Själva undertecknandet går till t.ex. så att undertecknaren klickar på alternativet "underteckna" i menyn till det program som används.

Det väsentliga med tanke på elektroniska signaturers tillförlitlighet är att den privata nyckeln förblir privat. Den privata nyckeln finns i allmänhet på något slags plattform,

t.ex. ett smartkort, som skyddats med t.ex. en PIN-kod eller ett lösenord på samma sätt som i fråga om bankkort. I framtiden kan biometriska kännetecken, t.ex. fingeravtryck, delvis komma att ersätta användningen av lösenord, som baserar sig på användarens minne. Den privata nyckeln kan t.ex. också finnas på mobiltelefonens SIM-kort eller som program i den anordning som undertecknaren använder, t.ex. hans eller hennes persondator.

Elektronisk signering omfattar inte bara själva undertecknandet utan också verifieringen av underskriften. Anordningarna för signaturframställning, dvs. programvara och maskinvara, motsvaras av anordningar för signaturverifiering, dvs. programvara och maskinvara som möjliggör signaturverifiering. Det är viktigt att märka att en certifikatutfärdare i sista hand inte på något sätt kan försäkra sig om att den som verifierar en signatur har tillgång till lämpliga, kompatibla och säkra program och maskiner för detta. Certifikatutfärdaren tillhandahåller en katalogtjänst och en spärrlista, och det är den tredje part som förlitar sig på ett certifikat som själv ska försäkra sig om certifikatets giltighet med hjälp av dessa. Den som verifierar elektroniska signaturer bör skaffa lämpliga och säkra verifieringsverktyg och använda certifikaten för att identifiera undertecknarna och försäkra sig om att informationen är oförvanskad.

Förtroende utgör en väsentlig del av konceptet med öppen nyckel. För att två parter som inte känner varandra från förut ska kunna kommunicera konfidentiellt behövs det en tredje part som säkerställer parternas identitet. I konceptet med öppen nyckel grundar sig förtroendet på den tredje parten, dvs. en certifikatutfärdare, som båda parterna litar på. Certifikatutfärdaren kopplar den öppna nyckeln till dess innehavare i certifikatet. På så sätt är det möjligt att skapa konfidentiell kommunikation och digitala signaturer, även om parterna inte känner varandra från förut.

Finland har ett starkt kunnande och flera företag som tillverkar certifikat för att användas som tekniskt verktyg. Sådana företag är bl.a. Valimo Wireless Oy, F-Secure Oyj, SSH Communications Security Oy, Tietoenator Abp och Nixu Oy. Lagen om elektroniska signaturer gäller inte dessa aktörer, eftersom lagens tillämpningsområde inte omfattar ren tillverkning, import och försäljning av verktyg. Det aktuella lagförslaget innehåller också en motsvarande begränsning av tillämpningsområdet. I Finland är det för närvarande endast Befolkningsregistercentralen som tillhandahåller tjänster för elektroniska signaturer på basis av certifikat som baserar sig på teknologi med öppna nycklar.

Terminologin

Certifikaten baserar sig på ett system med öppna nycklar (på engelska public key infrastructure, PKI), som fungerar på det sätt som förklaras ovan. Ofta talar man också om PKI-certifikat. När prefixet PKI, som högst syftar på tekniken, fogas till certifikat, talar man om certifikat i allmänhet. Certifikat har i regel använts vid elektroniska signaturer men de kan också användas vid elektronisk identifiering. Antalet certifikat för elektronisk identifiering förväntas öka betydligt.

Den finska termen ”laatuvermenne” (kvalificerat certifikat) motsvarar begreppet ”hyväksytty varmenne”, som används i EU:s direktiv om ett gemenskapsramverk för elektroniska signaturer. Det är fråga om EU:s interna reglering, man känner inte till en sådan certifikatkategori på internationell nivå. På svenska används termen kvalificerat certifikat även i direktivet. Med kvalificerat certifikat avses att det ställs mycket höga kvalitetskrav och andra krav på certifikatet och certifikatutfärdaren. För närvarande är det endast Befolkningsregistercentralen som tillhandahåller kvalificerade certifikat i Finland, men lagstiftningen hindrar inte att också andra tjänsteleverantörer kommer ut på marknaden.

Medborgarcertifikaten är certifikat som endast tillhandahålls och får tillhandahållas av Befolkningsregistercentralen. Utfärdandet av dessa certifikat omfattas också av en egen lag, befolkningsdatalagen. Medborgarcertifikaten grundar sig inte på EU-lagstiftning. Enligt Befolkningsregistercentralen uppfyller medborgarcertifikaten kraven i direktivet om ett gemenskapsramverk för elektroniska signaturer och i lagen om elektroniska signaturer och de är således även kvalificerade certifikat. Medborgarcertifikat finns huvudsakli-

gen på identitetskort eller pass som har utfärdats av polisen.

2.3 Den internationella utvecklingen samt lagstiftningen i utlandet och i EU

Direktivet om ett gemenskapsramverk för elektroniska signaturer

Europaparlamentets och rådets direktiv om ett gemenskapsramverk för elektroniska signaturer utfärdades den 30 november 1999 och det trädde i kraft den 19 januari 2000.

Utgångspunkten i direktivet är att tillhandahållande av certifikattjänster är en fri näring. Det är dock endast certifikat som uppfyller de höga, i direktivet definierade kvalitetskraven som kan betraktas som sådana kvalificerade certifikat som garanterar att avancerade elektroniska signaturer som framställts med säkra anordningar för signaturframställning åtminstone kan jämställas med traditionella egenhändiga namnunderskrifter. Regleringen i direktivet fokuserar uttryckligen på kvalificerade certifikat och på certifikatutfärdare som tillhandahåller sådana certifikat. I den föreslagna lagen används termen kvalificerat certifikat, liksom också i lagen om elektroniska signaturer.

Enligt tillämpningsområdet i artikel 1 är syftet att underlätta användningen av elektroniska signaturer och bidra till deras rättsliga erkännande. Direktivet strävar efter att fastställa ett rättsligt ramverk för elektroniska signaturer och vissa certifikattjänster för att säkerställa en väl fungerande inre marknad.

Direktivet omfattar inte frågor som avser ingående eller giltighet av avtal eller andra rättsliga förpliktelser, om den nationella lagstiftningen eller gemenskapslagstiftningen föreskriver vissa formkrav, och inte heller bestämmelser som reglerar användningen av dokument.

I artikel 2 ingår definitioner. I artikeln ingår en förteckning med 13 punkter som definierar begrepp som är av central betydelse för direktivet. I artikeln definieras bl.a. elektronisk signatur, flera delfunktioner som behövs vid elektronisk signering, certifikat och tillhandahållare av certifikattjänster.

I artikel 3 föreskrivs om marknadstillträde. Tillhandahållandet av certifikattjänster får inte vara beroende av förhandstillstånd. Medlemsstaterna får dock införa eller behålla frivilliga ackrediteringssystem. Ackrediteringssystemen ska vara objektiva, tydliga, proportionella och icke- diskriminerande.

Medlemsstaterna ska på ett lämpligt sätt införa övervakning av de tillhandahållare av certifikattjänster som är etablerade på deras territorium och som utfärdar kvalificerade certifikat till allmänheten.

Medlemsstaterna får utse offentliga eller privata organ som ska avgöra om säkra anordningar för skapande av signaturer överensstämmer med kraven i bilaga III. Ett beslut som fattas av ett sådant organ ska erkännas av samtliga medlemsstater.

Sådana produkter för elektroniska signaturer som är förenliga med allmänt erkända standarder ska erkännas i enlighet med direktivets krav. Kommissionen får offentliggöra referensnummer till dessa standarder i Europeiska gemenskapernas officiella tidning.

Medlemsstaterna får förena användningen av elektroniska signaturer i den offentliga sektorn med ytterligare krav. Sådana krav ska vara objektiva, tydliga, proportionella och icke-diskriminerande. Dessutom ska de endast gälla de särskilda egenskaperna för tillämpningen i fråga. Dessa krav får inte utgöra ett hinder för gränsöverskridande tjänster för medborgaren.

Enligt principerna för den inre marknaden i artikel 4 ska varje medlemsstat tillämpa de nationella bestämmelser som den antar enligt direktivet på samtliga tillhandahållare av certifikattjänster vilka är etablerade på dess territorium och på de tjänster som dessa tillhandahåller. Medlemsstaterna får inte heller begränsa tillhandahållandet av certifikattjänster med ursprung i andra medlemsstater genom nationella bestämmelser. Dessutom ska medlemsstaterna säkerställa att produkter för elektroniska signaturer har fri rörlighet på den inre marknaden.

I artikel 5 föreskrivs om rättslig verkan för elektroniska signaturer. Medlemsstaterna ska säkerställa att avancerade elektroniska signaturer som baseras på ett kvalificerat certifikat och som skapas av en säker anordning för skapande av signaturer har samma rättsliga

verkan som en handskriven signatur och godtas som bevis vid rättsliga förfaranden. Medlemsstaterna ska också säkerställa att en elektronisk signatur inte förvägras rättslig verkan eller giltighet som bevis enbart på grund av att signaturen inte uppfyller de ovan angivna kvalitetskraven.

I artikel 6 i direktivet bestäms om skadeståndsansvaret för den som tillhandahåller kvalificerade certifikat för allmänheten, om skadan orsakats någon som har rimlig anledning att förlita sig på ett certifikat. Skadeståndsskyldighet uppkommer i vissa fall om tillhandahållaren av certifikattjänster inte kan visa att han inte har handlat försumligt.

Enligt direktivet är certifikatutfärdaren ansvarig åtminstone för att all information i det kvalificerade certifikatet är korrekt vid tidpunkten för utfärdandet och för att certifikatet innehåller alla de uppgifter som föreskrivs för ett kvalificerat certifikat. Vidare ansvarar certifikatutfärdaren för att signeringsnyckeln överlämnas uttryckligen till certifikatinnehavaren och för att uppgifterna för skapande av signaturer och uppgifterna för signaturverifiering kan användas som komplement till varandra om certifikatutfärdaren framställer båda dessa. Certifikatutfärdaren ansvarar också för underlåtenhet att registrera återkallande av certifikat.

Certifikatutfärdaren ska ha rätt att i ett kvalificerat certifikat ange begränsningar i certifikatets användningsområde. Begränsningen får också gälla värdet av de transaktioner för vilka certifikatet kan användas. Begränsningen ska vara identifierbar för tredje man och den får inte vara oskälig. Certifikatutfärdaren är inte ansvarig för användningen av kvalificerade certifikat som inte motsvarar begränsningarna.

Artikel 7 innehåller bestämmelser om hur certifikat som utfärdas som kvalificerade certifikat till allmänheten av sådana tillhandahållare av certifikattjänster som är etablerade i ett tredje land betraktas som rättsligt likvärdiga med certifikat som utfärdas inom Europeiska gemenskaperna. Detta kan ske om certifikatutfärdaren uppfyller kraven i direktivet och har ackrediterats enligt ett frivilligt ackrediteringssystem enligt direktivet eller om en tillhandahållare av certifikattjänster som är etablerad inom gemenskapen garanterar certifikatet eller om certifikatet eller certifikatutfärdaren har erkänts enligt ett avtal mellan gemenskapen och ett tredje land eller internationella organisationer. Kommissionen kan överlämna förslag till rådet om lämpliga mandat för att förhandla om dessa internationella avtal. Besluten fattas med kvalificerad majoritet.

Enligt bestämmelserna om dataskydd i artikel 8 ska medlemsstaterna säkerställa att certifikatutfärdare, ackrediteringssystem och övervakande myndigheter uppfyller kraven i direktivet om allmänt dataskydd. En certifikatutfärdare får endast inhämta personuppgifter direkt från den berörda personen eller med dennes uttryckliga medgivande. Utan uttryckligt medgivande från personen i fråga får uppgifterna inte heller samlas in eller behandlas för andra ändamål än för utfärdande och bibehållande av certifikat. En pseudonym får anges i stället för undertecknarens namn i certifikatet. Detta får dock inte påverka den rättsliga verkan som enligt nationell lagstiftning ges pseudonymer.

I artiklarna 9 och 10 bestäms om den kommitté för elektroniska signaturer som ska biträda kommissionen och om kommitténs uppgifter. I artiklarna 11 och 12 bestäms också om medlemsstaternas anmälningsskyldighet och om översynen av hur direktivet fungerar.

I artiklarna 13–15 ingår de sedvanliga slutbestämmelserna.

I bilaga I anges kraven på kvalificerade certifikat. Ett kvalificerat certifikat ska bl.a. innehålla uppgifter om den som tillhandahåller certifikattjänster, undertecknarens namn, eventuella särskilda attribut för undertecknaren, uppgifter för signaturverifiering, certifikatets giltighetstid och avancerad elektronisk signering av den som tillhandahåller certifikattjänster.

I bilaga II anges kraven på tillhandahållare av certifikattjänster som utfärdar kvalificerade certifikat. De krav som ställs gäller bl.a. att kunna påvisa den pålitlighet som krävs för tillhandahållande av certifikattjänster. Vidare krävs ett snabbt och säkert system för registrering och för säkert och omedelbart återkallande, säker kontroll av identiteten hos den person till vilken certifikat utfärdas, kompetent personal, säkra system, tillräckli-

ga medel och lämpliga försäkringar, förbud att lagra signeringsnyckeln, arkiveringsskyldighet och skyldighet att informera användarna när certifikat utfärdas.

I bilaga III anges kraven på säkra anordningar för skapande av signaturer. Anordningarna ska säkerställa att uppgifterna som används för skapande av signaturer praktiskt taget är unika och att de inte kan härledas och att sekretessen är säkerställd inom rimliga gränser samt att signaturen är skyddad mot förfalskning. Det ska också vara möjligt för undertecknaren att skydda uppgifterna så att andra inte kan använda dem. Anordningarna för skapande av signaturer får inte förändra de uppgifter som ska signeras och inte heller förhindra att dessa uppgifter presenteras för undertecknaren före undertecknandet.

Bilaga IV innehåller rekommendationer för säker signaturverifiering. Enligt rekommendationerna ska processen bl.a. med rimlig säkerhet garantera att de uppgifter som används för att utföra signaturverifiering överensstämmer med de uppgifter som visas för den som utför verifieringen, att signaturen kontrolleras på ett tillförlitligt sätt, att den som utför verifieringen vid behov kan fastställa innehållet i de signerade uppgifterna och att certifikatets autencitet och giltighet kan kontrolleras på ett tillfredsställande sätt.

Europeiska kommissionen har låtit göra en undersökning (The Legal And Market Aspects Of Eletronic Signatures) av hur genomförandet av direktivet om elektroniska signaturer har lyckats i olika länder både ur juridisk och ur praktisk synvinkel. Enligt undersökningen har medlemsstaterna nog genomfört direktivet på ett berömvärt sätt, men andemeningen eller ordalydelsen i direktivet har ofta misstolkats.

Av undersökningen framgår att man i samband med offentliga tjänster onödigt ofta kräver att kvalificerade certifikat ska användas, vilket i många fall försvårar medborgarnas elektroniska kommunikation. Enligt undersökningen har man inte heller alltid förstått diskrimineringsförbudet i artikel 5.2, utan felaktigt tolkat det så att endast en viss teknik uppfyller kraven i lagen. I undersökningen rekommenderas därför att kommissionen ska vidta aktiva åtgärder för att informera alla intressegrupper och öka deras kännedom om artikeln i fråga. I undersökningen betonas att ett kvalificerat certifikat inte är samma sak som en juridiskt godkänd signatur, utan endast en teknik för att skapa en elektronisk signatur som kan godkännas juridiskt. För att främja den elektroniska kommunikationen och betona lagens anda, dvs. teknikneutralitet, rekommenderar arbetsgruppen att termen kvalificerat certifikat ska få minskad betydelse.

I undersökningen konstateras också att det inte ännu finns en naturlig efterfrågan på kvalificerade certifikat på marknaden. Man tror också att situationen kommer att vara densamma ännu en lång tid framöver. På marknaden råder ofta den felaktiga uppfattningen att vissa tillämpningar eller tjänster kräver att underskriften görs med ett kvalificerat certifikat, vilket orsakar tjänsteleverantörerna onödiga kostnader och problem när de utvecklar tjänsterna.

I sin lista över alternativa signeringssätt lyfter arbetsgruppen fram bankernas system med lösenordslistor som byts ut. Man önskar att bankkoder ska användas i stor utsträckning i olika nättjänster, vilket förutsätter samarbete från bankernas sida. Detta är redan fallet i Finland, eftersom bankerna har tagit fram Tupas-standarden och den offentliga förvaltningen har gett sina rekommendationer för användningen av Tupas. I Europa har man bl.a. under ledning av VISA börjat utreda möjligheten att utnyttja bankernas identifieringsmetoder i större utsträckning i samband med nättjänster.

EU:s program och projekt

Inom Europeiska unionen pågår ett flertal program som syftar till att främja eller använda elektronisk identifiering och elektroniska signaturer liksom även till att främja accepterandet av dem i gränsöverskridande verksamhet.

IDABC (Interchange of Data Between Administrations) är ett gemenskapsprogram som stöder genomförandet av EU-lagstiftningen genom att förbättra det elektroniska informationsutbytet mellan medlemsstaterna. Programmet startade redan i mitten av 1990-talet och den aktuella fasen av programmet grundar sig på Europaparla-

mentets och rådets beslut 2004/387/EG av den 21 april 2004 om interoperabelt tillhandahållande av alleuropeiska e-förvaltningstjänster för offentliga förvaltningar, företag och medborgare (IDABC). Programmet, som är kopplat till eEuropa och indirekt till Lissabonstrategin, är indelat i projekt (Projects of Common Interest) och horisontella åtgärder (Horizontal Actions and Measures). Inom ramen för programmet har man gjort en undersökning om medlemsstaternas ömsesidiga erkännande av elektroniska signaturer med tanke på den elektroniska förvaltningens behov. I undersökningen, vars preliminära resultat är klara, har man jämfört likheter och olikheter i användningen av elektroniska signaturer både ur juridisk och teknisk synvinkel i samband med elektronisk kommunikation hos myndigheterna i olika medlemsstater och i vissa andra stater. I undersökningen klarläggs hur likheterna och olikheterna påverkar interoperabiliteten. Samtidigt ger man också rekommendationer. Undersökningen fokuserar inte uttryckligen på frågor som gäller elektronisk identifiering.

STORK (Secure identity across borders linked) är ett pilotprojekt som kommissionen inledde i maj 2008. Syftet med projektet är att underlätta användningen av offentliga tjänster i 13 medlemsstater. Målet är att skapa en modell för kompatibel elektronisk identifiering, som erkänns ömsesidigt av medlemsstaterna men ger dem en möjlighet att bevara sina nuvarande system och förfaranden. I projektet deltar Europeiska kommissionen, Belgien, Frankrike, Förenade kungariket, Italien, Luxemburg, Nederländerna, Portugal, Slovenien, Spanien, Sverige, Tyskland och Österrike. Av länderna inom Europeiska ekonomiska samarbetsområdet deltar Island. Projektet är en del av EU:s ramprogram för konkurrenskraft och innovation (CIP).

Projektet syftar till att företag, privatpersoner och anställda inom den offentliga förvaltningen ska kunna använda sina elektroniska identiteter i vilken medlemsstat som helst. Avsikten är att systemet ska grunda sig på att informations- och kommunikationstekniska lösningar som redan är i bruk på ett nationellt, regionalt och lokalt plan ska användas över landsgränserna. Några av de mest användbara elektroniska identifieringstjänsterna kommer att testas genom att det definieras ett antal gemensamma specifikationer som möjliggör ömsesidigt erkännande av olika nationella identifikatorer mellan deltagarna, och som kommer att vara tillgängliga för andra länder. De länder som deltar i projektet uppmuntras också att erkänna varandras elektroniska identifikatorer.

Systemet gör det möjligt att verifiera identiteten elektroniskt på ett säkert sätt och att kontakta den offentliga förvaltningen t.ex. från en dator eller t.o.m. från en mobiltelefon. Avsikten är inte att systemet ska ersätta de nationella systemen, och även de stater som inte deltar i pilotprojektet ska kunna dra nytta av dess resultat.

PEPPOL (Pan European Public Procurement Online) är ett annat centralt projekt med tanke på identifiering. Projektet anknyter till EU:s ramprogram för konkurrenskraft och innovation (CIP) och inriktas på gränsöverskridande förfaranden i samband med den offentliga upphandlingsprocessen. Europeiska kommissionen samarbetar med EU-länderna Danmark, Finland, Frankrike, Italien, Tyskland, Ungern och Österrike samt med Norge, som hör till Europeiska ekonomiska samarbetsområdet. Avsikten är att göra det lättare för företag att ge anbud vid offentlig upphandling utanför det egna landets gränser. I projektet ersätts inte befintliga nationella system för elektronisk upphandling, utan de byggs på så att de kan kommunicera med varandra.

Flera EU-länder har tagit i bruk system för elektronisk offentlig upphandling. De krav som gäller elektroniska signaturer i upphandlingsdokument varierar mellan medlemsländerna, men anbudsgivare som deltar i upphandlingsförfaranden har i princip rätt att i sina anbud använda sådana elektroniska signaturer som uppfyller kraven i den egna medlemsstaten. Signaturkraven grundar sig i allmänhet inte på signaturernas traditionella uppgift att uttrycka en viljeförklaring, utan på avsikten att identifiera avsändaren för olika myndighetsändamål.

Kommissionens meddelande om att förenkla tillhandahållandet av gränsöverskridande offentliga tjänster

Kommissionen lade den 28 november 2008 fram ett meddelande till rådet, Europaparlamentet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén om en handlingsplan för bättre e-signaturer och e-legitimation för att förenkla tillhandahållandet av gränsöverskridande offentliga tjänster på den inre marknaden (KOM(2008) 798 slutlig). Syftet med handlingsplanen är att hjälpa medlemsstaterna att införa ömsesidigt godkända och kompatibla system för e-signaturer och e-legitimation (elektronisk identifiering) i syfte att göra det lättare att tillhandahålla elektroniska offentliga tjänster över gränserna. Handlingsplanen inriktas huvudsakligen på e-förvaltningstillämpningar, men de föreslagna åtgärderna kan också vara till nytta för företagstillämpningar.

Meddelandet gäller åtgärder för elektroniska signaturer och åtgärder för elektronisk legitimering. Fokus ligger tydligt på elektroniska signaturer. I fråga om dem är åtgärderna indelade i två grupper. Den första gruppen gäller gränsöverskridande användning av kvalificerade elektroniska signaturer (KES) och avancerade elektroniska signaturer som baseras på ett kvalificerat certifikat (AES som baseras på KS). Enligt kommissionen är det möjligt att relativt snabbt förbättra detta område, eftersom båda dessa typer av signaturer har en tydlig rättslig status enligt direktivet om elektroniska signaturer. Dessutom har det redan gjorts mycket för att standardisera de båda typerna av signaturer.

Kommissionen konstaterar att det främsta hindret för gränsöverskridande användning av elektroniska signaturer i praktiken är bristande förtroende för signaturer från andra medlemsstater och de svårigheter som förknippas med valideringen av signaturerna. Enligt kommissionen bör för det första den mottagande parten ges möjlighet att kontrollera status för de tillhandahållare av certifikattjänster som utfärdar kvalificerade certifikat i andra medlemsstater. För det andra bör den mottagande parten ges möjlighet att kontrollera kvaliteten på signaturen. Detta innebär att den mottagande parten måste kunna kontrollera om en signatur är en avancerad elektronisk signatur och om den baseras på ett kvalificerat certifikat som har utfärdats av en tillhandahållare av certifikattjänster som står under övervakning. När det gäller kvalificerade elektroniska signaturer måste mottagaren också kunna kontrollera om signaturen har skapats med hjälp av en säker anordning för skapande av signaturer. Kommissionen konstaterar att denna information i princip kan inhämtas från själva signaturen och från innehållet i det kvalificerade certifikatet. Det är emellertid i nuläget svårt att inhämta informationen på grund av de skillnader som finns när det gäller hur man använder befintliga standarder och förfaranden.

Kommissionens slutsats är att valideringen av elektroniska signaturer skulle kunna förenklas genom att den mottagande parten ges nödvändig information om de tillhandahållare av certifikattjänster som är godkända och föremål för tillsyn på nationell nivå och genom att det utfärdas riktlinjer för hur de befintliga standarderna och förfarandena ska användas för att vara driftskompatibla.

Kommissionen föreslår fyra åtgärder för att förbättra situationen. Senast andra kvartalet 2009 sammanställs en tillförlitlig förteckning över tillhandhållare av kvalificerade certifikat som är föremål för tillsyn (Trusted List of Supervised Qualified Certification Service Providers) på EU-nivå. Avsikten är att förteckningen ska innehålla all nödvändig information om befintliga tillhandhållare av kvalificerade certifikat som är föremål för tillsyn. Arbetet pågår redan i kommissionens arbetsgrupp som bereder genomförandet av tjänstedirektivet.

Kommissionens mål är också att senast tredje kvartalet 2009 aktualisera beslut 2003/511/EG, som innehåller en förteckning över allmänt erkända standarder för produkter för elektroniska signaturer, och undersöka om det finns möjlighet att utvidga beslutets tillämpningsområde till andra e-signaturprodukter. Ett annat mål är att senast tredje kvartalet 2009 ta fram riktlinjer avseende de gemensamma kraven för att hjälpa aktörerna att genomföra kvalificerade elektroniska signaturer och avancerade elektroniska signaturer som är baserade på ett kvalificerat certifikat på ett kompatibelt sätt. Som

pågående åtgärder nämns att medlemsstaterna uppmanas att regelbundet lämna in den information som kommissionen behöver och vid behov vidta de åtgärder som följer av den ovan nämnda åtgärdsplanen.

Enligt kommissionens indelning är avancerade elektroniska signaturer (AES) en annan grupp av elektroniska signaturer. I fråga om dem uppstår ungefär samma kompatibilitetsproblem som har diskuterats ovan när det gäller kvalificerade elektroniska signaturer och avancerade elektroniska signaturer som baseras på ett kvalificerat certifikat. I praktiken är emellertid situationen mer komplicerad när det gäller avancerade elektroniska signaturer, eftersom det för närvarande finns flera juridiska, tekniska och organisatoriska svårigheter när det gäller dem.

I artikel 2.2 i direktivet om elektroniska signaturer ges en mycket allmän definition av begreppet avancerad elektronisk signatur. Detta har gjort att medlemsstaterna använder sig av många olika tekniska lösningar med olika grader av säkerhet. Medlemsstaterna får också införa specifika nationella lösningar för specifika tillämpningar, vilket skapar ytterligare hinder för gränsöverskridande användning av avancerade elektroniska signaturer. Både valideringen av en avancerad elektronisk signatur och bedömningen av dess juridiska status eller dess säkerhetsnivå i en viss tillämpning är svåra uppgifter för den mottagande parten. För närvarande krävs det ofta att det görs en separat bedömning och hantering av den mottagna signaturen i varje enskilt fall.

Kommissionen konstaterar att för att förenkla gränsöverskridande användning av avancerade elektroniska signaturer bör det skapas förutsättningar som gör att den mottagande parten kan lita på en avancerad elektronisk signatur från en annan medlemsstat. Kommissionens slutsats är att det inom ramen för handlingsplanen i praktiken är omöjligt att ta fram en gemensam strategi och gemensamma kriterier för avancerade elektroniska signaturer. En lösning kunde dock vara att delegera verifieringen och valideringen till en central eller decentraliserad valideringstjänst. Härigenom skulle det vara möjligt att stegvis undanröja det främsta hindret för driftskompatibla avancerade elektroniska signaturer. Kommissionen meddelar att den under det andra kvartalet 2009 kommer att göra en genomförbarhetsundersökning för att se om det är möjligt att införa en sådan valideringstjänst på EU-nivå.

Kommissionen kommer också senast andra kvartalet 2009 att aktualisera landsprofilerna i den undersökning om ömsesidigt erkännande av e-signaturer för e-förvaltningstillämpningar som har tagits fram inom IDABC. Kommissionen kommer senast 2010 att rapportera om vilka åtgärder som behövs för att främja gränsöverskridande användning av elektroniska signaturer. Kommissionen kommer att basera sitt arbete på resultaten av det pågående arbetet. Medlemsstaterna uppmanas att lämna in all relevant information till kommissionen och att sörja för det samarbete som krävs för åtgärderna, särskilt de åtgärder som är nödvändiga för inrättandet av valideringstjänsten. Medlemsstaterna uppmanas också att testa valideringstjänsten inom ramen för pilotprojektet PEPPOL.

I fråga om e-legitimering konstaterar kommissionen att det för att vidareutveckla de gränsöverskridande offentliga e-tjänsterna emellertid krävs att systemen för e-legitimering är kompatibla. Hittills har medlemsstaterna infört olika system för e-legitimering utan någon samordning. Om det inte införs ett kompatibelt system för e-legitimering inom unionen kommer det i praktiken att uppstå nya hinder, som inte är förenliga med instrumenten för den inre marknaden.

Vissa gemensamma åtgärder har vidtagits för att försöka finna ett system för gränsöverskridande e-legitimering som kan bygga på befintliga identifieringssystem. På samma sätt som när det gäller elektroniska signaturer söker man finna en övergripande lösning som fungerar för sektorstillämpningarna och som bygger på ömsesidigt erkännande av motpartens system för e-legitimering. Ett antal frågor behöver emellertid fortfarande lösas.

Ett första steg är pilotprojektet STORK. Senast i slutet av 2009 kommer kommissionen i samarbete med medlemsstaterna att göra specifika undersökningar om användningen av e-legitimation i medlemsstaterna, dels som ett komplement till STORK-

projektet och dels till stöd för projektet. När projektet har presenterat sina resultat kommer kommissionen att avgöra om det behövs fler åtgärder för att säkra effektiv användning av e-legitimation i hela EU, och i så fall vilka. Medlemsstaterna uppmanas också att senast 2012 inom ramen för STORK-projektet lägga fram lösningar för gränsöverskridande e-legitimering.

Lagstiftningen i andra länder

Sverige

Sveriges lag om elektroniska signaturer (Lag [2000:832] om kvalificerade elektroniska signaturer) innehåller reglering för utfärdare av kvalificerade certifikat som är etablerade i Sverige. Lagen som sådan har dock hamnat i skymundan eftersom det hittills inte har kommit in utfärdare av kvalificerade certifikat på den svenska marknaden. Den svenska lagen avviker något från direktivet genom att den allmänna definitionen av elektronisk signatur inte bara gäller identifiering av undertecknaren, utan även inbegriper ett krav om att innehållet i signaturen inte får ha förvanskats.

Post- och telestyrelsen för en förteckning över dem som utfärdar kvalificerade certifikat och övervakar deras verksamhet. I en förordning om finansiering som gäller Post- och telestyrelsen föreskrivs det om årsavgifter för utfärdare av kvalificerade certifikat och förordningen kompletteras av Post- och telestyrelsens egna föreskrifter om avgifter (PTSFS 2007:8).

I Sverige utfärdas elektroniska identitetshandlingar av ett flertal kommersiella aktörer, som utses genom offentlig upphandling. De som utfärdar elektroniska identitetshandlingar kan använda sig av uppgifter i befolkningsregistret och personbeteckningar. Identifieringen regleras dock inte genom lag och det har inte heller fastställts hur elektroniska identitetshandlingar ska skapas. I allmänhet anses det dock att de metoder som använts för att skapa elektroniska identitetshandlingar inte uppfyller de krav som ställs på kvalificerade certifikat. Elektroniska identitetshandlingar kan laddas ner på datorns hårdskiva, men smartkort eller aktiveringskoder ska hämtas på posten, där man personligen ska legitimera sig. I fråga om de elektroniska signaturer som avses i lagen konstateras det att certifikatutfärdaren ska ha säkra rutiner för identitetskontroll av dem som certifikaten utfärdas till.

Norge

Norges lag om elektroniska signaturer (Lov om elektronisk signatur) är från 2001. Lagen bygger på EU-direktivet och använder därför samma begreppsapparat som direktivet. I Norge finns det dock inte utfärdare av kvalificerade certifikat, så lagen har tills vidare varit ganska betydelselös.

Det har inte gjorts upp några allmänna bestämmelser i lag om elektronisk identifiering. För skapandet av elektroniska identitetshandlingar används smartkort som utfärdas av många olika aktörer, t.ex. banker och penningspelinrättningar, och ett nationellt system håller på att utvecklas. Några slutliga avgöranden om genomförande, tillsyn och lagstiftning har dock inte träffats. De befintliga lösningarna är kommersiella och de allmänna civilrättsliga reglerna styr ansvarsfrågorna.

Danmark

I Danmark har man i likhet med de övriga EU-länderna genomfört direktivet om elektroniska signaturer, men det har i praktiken inte haft någon betydelse, eftersom det inte finns utfärdare av kvalificerade certifikat i landet som certifierar kvalificerade elektroniska signaturer. Danmark har ingen särskild lagstiftning om elektronisk identifiering.

Lagen om elektroniska signaturer kräver att de som ansöker om kvalificerade elektroniska signaturer ska legitimera sig personligen. Av denna anledning skapade den danska regeringen en enklare typ av elektronisk signatur som bygger på en viss standard, OCES, och vid ansökan om en sådan signatur behöver man inte legitimera sig personligen. OCES-signaturen är en avancerad elektronisk signatur som bygger på servercertifikat. OCES-certifikat för signaturer kan utfärdas för privatpersoner, företag och anställda. Utfärdandet av certifikat är i princip öppet för

olika kommersiella aktörer, men systemet övervakas av landets kommunikationsverk, med vilket certifikatutfärdaren (CA) ingår ett ramavtal enligt vilket certifikatutfärdaren förbinder sig att följa kommunikationsverkets certifikatpolitik och att årligen lämna in en redogörelse över sin verksamhet till verket och att tillåta kontroll av verksamheten. Det har länge funnits ett avtalsarrangemang med landets största teleoperatör, men man håller som bäst på att omarbeta systemet. Många tillämpningar inom den elektroniska förvaltningen godkänner OCES-signaturen. Systemet känner till att den part som förlitar sig på tjänsten deltar i finansieringen av certifikatet.

Eftersom OCES-signaturen inte är en sådan kvalificerad elektronisk signatur som avses i direktivet, har man kunnat avvika från direktivets ansvarsbestämmelser så att certifikatutfärdaren har rätt att begränsa sitt ansvar i sitt avtalsförhållande till företag och offentliga organ, men inte till privatpersoner. En OCES-signatur kan beställas via certifikatutfärdarens webbsidor med hjälp av personbeteckning, hemadress och e postadress. Den PIN-kod som aktiverar signaturen sänds till hemadressen. Personbeteckningen utgör en väsentlig beståndsdel vid skapandet av certifikat för signaturer, och därför är certifikaten tillgängliga enbart för dem som har dansk personbeteckning.

Estland

Estlands lag om elektroniska signaturer från 2000 bygger begreppsmässigt klart på PKI tekniken. Lagen stiftades innan landet anslöt sig till Europeiska unionen och utgår från ett nationellt perspektiv. Lagen reglerar dock i likhet med direktivet endast avancerade elektroniska signaturer och kvalificerade certifikat. Utfärdare av kvalificerade certifikat ska liksom utfärdare av tidsstämplar registrera sig i ett nationellt register. Bestämmelserna om tidsstämplar för elektroniska signaturer är ett särdrag i den estniska lagstiftningen. Man har på senare tid velat ändra den estniska lagen så att elektroniska signaturer även kan utfärdas i företags namn. Sådana signaturer kallas elektroniska stämplar.

I Estland använder man elektroniska identitetskort och i dag har nästan varje medborgare ett sådant. Användningen av identitetskort grundar sig, som i Finland, på en lag om identitetskort. Kvalificerade certifikat håller förutom i smartkort även på att tas i bruk i SIM kort. Urvalet av kort ska utvecklas. Den privata sektorn och den estniska regeringen har som en del av landets informationssäkerhetsprogram kommit överens om att användningen av identitetskort mera än tidigare ska ersätta annan teknik.

I Estlands lag om elektroniska signaturer fastställs certifikatutfärdarens ansvar när den inte iakttar de krav som ställs på den. Certifikatutfärdaren ska dessutom ha en ansvarsförsäkring. När det gäller ansvarsfrågorna följer ordalydelsen i lagen inte direktivet. I lagen tillämpas inte omvänd bevisbörda. Begränsningar kan införas för användningen av certifikat. Det har dock ansetts att certifikatutfärdaren inte ansvarar för skada som åsamkats utomstående på grund av användningen av certifikat, utan att det är innehavaren av certifikatet som bär detta ansvar.

Den elektroniska identitetshandlingen grundar sig på personbeteckningen. I lagen om elektroniska signaturer specificeras inga metoder för inledande identifiering, utan det är upp till certifikatutfärdaren att besluta om detta. När det gäller elektronisk identifiering bör det noteras att enligt lagen ska en elektronisk signatur identifiera den person i vars namn signaturen utfärdas. På så sätt reglerar lagen också användningen av elektroniska signaturer för identifiering, trots att identifieringsfunktionen inte har behandlats i detalj i lagen. Certifikaten i de identitetskort som används delas upp i signaturcertifikat och identifieringscertifikat.

Landets ministerium för ekonomi och kommunikation övervakar efterlevnaden av lagen om elektroniska signaturer.

Tyskland

Tysklands lag om elektroniska signaturer (Gesetz über Rahmenbedingungen für elektronische Signaturen) är från 2001 och bygger på direktivet. I lagen finns det dock även bestämmelser om tidsstämpling som härstammar från en tidigare lag från 1997, och även vissa bestämmelser om certifikatutfärdare härstammar från tidigare lagstiftning.

Den tyska lagen känner bland annat till kvalificerade tidsstämplar. De elektroniska signaturerna delas in i vanliga, avancerade och kvalificerade elektroniska signaturer. I Tyskland finns det tiotals utfärdare av kvalificerade certifikat och den materiella lagstiftningen om till exempel elektroniska signaturer och offentlig upphandling har länge krävt mera avancerade former av elektroniska signaturer.

Ansvarsbestämmelserna om certifikatutfärdare är mera omfattande än de som finns i direktivet. Certifikatutfärdarna ansvarar uttryckligen även för de tekniska säkerhetssystemen. I den tyska lagen har ansvarsgrunderna inte räknats upp mera detaljerat än så här, och ansvaret hos den som utfärdar kvalificerade certifikat bestäms utifrån en generalklausul.

I lagen finns det inga detaljerade krav på hur den som ansöker om certifikat ska identifieras, utan lagen kräver att sökanden identifieras på ett lämpligt sätt. Lagens efterlevnad övervakas av den myndighet som övervakar energi, datakommunikation, post och järnvägar. I lagen anges enligt typ de avgifter som de myndigheter som övervakar certifikatutfärdarnas verksamhet tar ut, men det mera exakta innehållet i avgifterna anges i författningar på lägre nivå.

Lagen om elektroniska signaturer kan inte tillämpas direkt på elektronisk identifiering och det har inte heller utarbetats någon annan allmän lag om elektronisk identifiering. I Tyskland håller man för närvarande på att skapa ett elektroniskt identitetskort som är avsett att tas i bruk 2010. Ett av särdragen med kortet är att det även tillåter användning av pseudonym. En tysk medborgare som använder kortet kan således välja vilka uppgifter som han eller hon lämnar ut om sig själv till tjänsteleverantören. Registrering av fingeravtryck på kortet är frivillig. Kortet möjliggör användning av elektroniska tjänster, dvs. fungerar som ett redskap för legitimering, och det kommer att kunna användas för elektronisk signering.

Österrike

Österrike stiftade år 2000 en lag om elektroniska signaturer utifrån EU-direktivet och senast år 2004 en motsvarande förordning. Elektroniska signaturer kan utfärdas endast för fysiska personer, men speciallagstiftningen om elektronisk förvaltning innehåller bestämmelser om användningen av signaturer för någon annans räkning.

I lagen används definitionen av säker elektronisk signatur på samma sätt som när man i Tyskland talar om kvalificerad elektronisk signatur. Ansvarsbestämmelserna i lagen om elektroniska signaturer bygger på EU-direktivet, men den österrikiska lagen innehåller också ett krav om ansvarsförsäkring för certifikatutfärdare.

Myndighetstillsynen i Österrike hör till landets kommunikationsverk, som övervakar alla certifikatutfärdare. Certifikatutfärdarna ska skriftligen informera kommunikationsverket om sin säkerhetspolitik. På så sätt omfattas i princip även certifikat som utfärdats för elektronisk identifiering av tillsynen. För närvarande finns det bara en utfärdare av kvalificerade certifikat enligt lagen om elektroniska signaturer i landet.

Medborgarnas elektroniska identitetshandlingar grundar sig på personbeteckningen, från vilken man har härlett en PIN-kod som påminner om den elektroniska kommunikationskod som används i Finland. Användaren kan välja när koden ska introduceras. Det elektroniska identitetskortet förenar identifieringen (identification), verifieringen av ursprunget (authentication), den elektroniska signaturen och eventuella auktorisationsuppgifter (mandate). Identitetskortet kan också användas via mobiltelefonen (mobilcertifikat). Även privata instanser som banker kan utfärda identitetskort. Identifiering och signering som funktioner avviker dock inte från varandra, utan inloggning i till exempel den offentliga förvaltningens system kräver en viljeyttring som uttryckts genom en elektronisk signatur.

Förenade kungariket

Direktivet om elektroniska signaturer har genomförts genom två olika lagar, av vilka den viktigare är The Electronic Signatures Regulations 2002. Till ordalydelsen bygger lagen klart på direktivet. Elektroniska signaturer kan utfärdas även för juridiska perso-

ner. Beträffande ansvarsfrågor innehåller lagen inte några omnämnanden av de begränsningar av skadeståndsansvaret som direktivet tillåter. Certifikatutfärdarens ansvar inför en part som inte ingår i avtalsförhållandet och som förlitar sig på tjänsten är som allmän princip utomkontraktuellt skadeståndsansvar (tort liability).

Förenade kungadömet kommer enligt beslut att börja utfärda elektroniska identitetskort, och för detta ändamål behöver man också skapa en centraliserad folkbokföring. Detta är en stor förändring eftersom man av tradition inte har haft folkbokföring eller register som grundar sig på folkbokföring i landet. Registrering är dock frivillig och sker i praktiken just för skapandet av elektroniska identitetshandlingar genom identitetskort. Systemet har skapats genom parlamentets lag om identitetskort (Identity Cards Act 2005). Identitetskortet är avsett särskilt för anlitande av offentliga tjänster och det utfärdas av en myndighet.

Lagen om identitetskort grundar sig på att individer låter registrera sig i ett befolkningsregister, och identitetskortet utfärdas på basis av denna registrering. Myndigheterna har rätt att enligt egen prövning kräva utredningar för fastställande av individers identitet efter det att de har ansökt om registrering i befolkningsregistersystemet. Myndigheterna kan kräva ett personligt besök, att en person fotograferas eller till och med att biometriska kännetecken tas. Lagen innehåller inga bestämmelser om myndighetsansvar när det gäller misstag som begås i samband med att kort utfärdas, utan sådana rättas till med stöd av de allmänna reglerna om skadeståndsrätt.

Belgien

Belgiens lag om elektroniska signaturer är från 2001. Lagen bygger ganska detaljerat på bestämmelserna i direktivet. Certifikat kan utfärdas även för juridiska personer.

Någon allmän lagstiftning om elektronisk identifiering finns inte, men i Belgien har man tagit i bruk elektroniska identitetshandlingar som bygger på identitetskort. Identitetskorten baserar sig på befolkningsregistersystemet och lagstiftningen om det. År 2003 utfärdades det en förordning om elektroniska identitetskort och systemet täcker redan de flesta som bor i landet. Identitetskortet innehåller ett certifikat med en kvalificerad elektronisk signatur och detta certifikat används i praktiken även för legitimering. Certifikaten utfärdas av Certipost, som är ett samföretag som består av det belgiska postverket och landets ledande teleoperatör Belgacom. Landets myndigheter har godkänt tre utfärdare av kvalificerade certifikat och deras certifikat godkänns i de system som används inom den elektroniska förvaltningen.

Utöver de elektroniska identitetskorten ger även kommersiella certifikat tillträde till datasystemen inom den elektroniska förvaltningen. I fråga om dessa certifikat krävs det alltid att den som ansöker om certifikat identifieras genom ett personligt besök. De kommersiella certifikaten är lämpliga att använda eftersom de har ett större datainnehåll än de elektroniska identitetskorten och eftersom de också kan användas för kryptering.

Spanien

Spaniens lag om elektroniska signaturer är från 1999 och kompletteras av en förordning från 2000. Enligt lagen får sådana kvalificerade elektroniska signaturer som avses i direktivet även utfärdas för juridiska personer. Det finns ingen allmän lag om elektronisk identifiering i Spanien, utan man har satsat på att utveckla ett elektroniskt identitetskort.

Den spanska lagen om elektroniska signaturer omfattar ett klart större område än kvalificerade elektroniska signaturer. Lagen innehåller en ansvarsbestämmelse som även omfattar andra certifikatutfärdare än de som utfärdar kvalificerade certifikat, men som grundar sig på direktivets system. Lagen innehåller en likadan detaljerad förteckning över grunderna för ansvarsfrihet eller begränsat ansvar för certifikatutfärdare som 16 § i den finska lagen om elektroniska signaturer. Ansvarsbestämmelserna som gäller certifikatutfärdare kan i praktiken utöver signaturer även gälla legitimering, eftersom de certifikat som är avsedda för elektronisk signering även används för legitimering. Lagen innehåller också ett krav om att certifikatutfärdare ska ha en ansvarsförsäkring som täcker ett försäkringsbelopp på minst

3 000 000 euro. Certifikatutfärdarna är skyldiga att hålla sin certifikatpolitik offentlig.

I Spanien har man tagit i bruk elektroniska identitetskort som enligt den författning som gäller korten (Real Decreto 1553/2005) möjliggör fastställande av identitet och elektroniska signaturer i alla tillämpningar inom den elektroniska förvaltningen. Enligt författningen krävs en fysisk inledande identifiering för att ett identitetskort ska utfärdas. Även förnyande av kortet kräver fysisk identifiering.

Slovenien

Sloveniens lag om elektroniska signaturer är från 2000 och innehåller även bestämmelser om elektronisk handel. Lagen bygger på EU-direktivet trots att Slovenien ännu inte var medlem av Europeiska unionen när lagen stiftades. Den slovenska lagen har inga särskilda bestämmelser om elektronisk identifiering.

När det gäller elektroniska signaturer omfattar den slovenska lagen om elektroniska signaturer till skillnad från direktivet även begreppet tidsstämpling. Direktivets ansvarsbestämmelser har tagits in i lagen i oförändrad form. Man har dock även räknat upp vissa andra ansvarsgrunder för certifikatutfärdare i lagen, utöver de som finns i direktivet. Lagen kompletteras av en förordning som reglerar de krav som ställs på certifikatutfärdarna, till exempel obligatorisk ansvarsförsäkring, krav som gäller personal och utrustning och interna regler. En offentligägd inrättning för certifiering utfärdar certifikat för tjänstemannakåren, och dessutom för enskilda medborgare och företag.

År 2004 fogades bestämmelser om utvecklande av ett system för elektroniska identitetskort till lagen om elektroniska signaturer och elektronisk handel. Systemet har ännu inte genomförts. Identitetskortet är ett traditionellt identitetsbevis som innehåller ett kvalificerat certifikat. Systemet bygger på personbeteckningar och separata elektroniska kommunikationskoder.

Turkiet

Turkiets lag om elektroniska signaturer är från 2004. Lagen bygger på Europeiska unionens direktiv, men innehåller även bestämmelser om bland annat tillsyn och brott och straffpåföljder i anslutning till elektroniska signaturer. Definitionsdelen innehåller också en definition av tidsstämpling, även om lagen i likhet med Estlands lag inte innehåller detaljerade bestämmelser om verksamheten för certifikatutfärdare som utfärdar tidsstämplar. I lagen talas det om säkra elektroniska signaturer, men man använder inte begreppet avancerade elektroniska signaturer. Säkra elektroniska signaturer lyfts med avvikelse från direktivet klart fram i en särställning i juridisk mening. Liksom direktivet innehåller lagen inga bestämmelser om elektronisk identifiering.

De ansvarsbestämmelser som gäller elektroniska signaturer är mera detaljerade än de som finns i direktivet, men uppfyller också de grundläggande principerna i det ansvarssystem som skapats genom direktivet. Det finns särskilda bestämmelser om bland annat certifikatutfärdarens principalansvar i förhållande till sina anställda i olika situationer. Det är obligatoriskt med ansvarsförsäkring för certifikatutfärdarna. Lagen kräver ingen uttrycklig inledande identifiering, utan den som ansöker om certifikat ska identifieras på ett tillförlitligt sätt genom dokument.

Turkiets kommunikationsverk övervakar efterlevnaden av lagen. Tillsynen gäller dock endast sådana utfärdare av kvalificerade elektroniska signaturer och utfärdare av tidsstämplar som den turkiska lagen självständigt har angett. Funktioner i anslutning till elektronisk identifiering omfattas alltså inte.

Internationella organisationer

OECD

Organisationen for ekonomiskt samarbete och utveckling OECD har redan i tio års tid arbetat med att utveckla den elektroniska identifieringen. Vid en ministerkonferens i Ottawa i Kanada 1998 antog man en deklaration (Declaration on Authentication for Electronic Commerce). Organisationen har publicerat flera jämförande studier om elektronisk identifiering och elektroniska signaturer. I

juni 2007 gav OECD ut en rekommendation (OECD Recommendation on Electronic Authentication), som kompletteras av tillämpningsanvisningar.
I rekommendationen rekommenderar OECD sina medlemsländer att inta ett teknologineutralt förhållningssätt till elektronisk identifiering av personer och organisationer såväl nationellt som internationellt och hänvisar samtidigt till sina egna riktlinjer (guidelines) för verksamheten när det gäller informationssäkerhet och dataskydd. Medlemsländerna bör också stödja utvecklingen, utbudet och användningen av kommersiellt gångbara och säkra varor och tjänster för elektronisk identifiering. Likaså bör medlemsländerna inom såväl den privata som den offentliga sektorn främja den kommersiella kompatibiliteten och den tekniska driftskompatibiliteten (interoperability) hos systemen för identifiering, så att de kan betjäna den elektroniska kommunikationen och det elektroniska utbytet oberoende av branscher och rättsordning och så att de kan tas i bruk såväl nationellt som internationellt. OECD rekommenderar även att man ökar medvetenheten om fördelarna med elektronisk identifiering såväl nationellt som internationellt.

UNCITRAL

Förenta Nationernas (nedan FN) kommission för internationell handelsrätt (nedan UNCITRAL) antog vid sin 34 session sommaren 2001 en modellag om elektroniska signaturer (nedan modellagen). Dessutom har det utarbetats en handledning för tolkningen av modellagen (Guide to Enactment).

Arbetet med UNCITRAL:s modellag erbjöd FN-staterna ett välbehövligt internationellt diskussionsforum för utvecklandet av lagstiftningen om elektroniska signaturer. Modellagen fungerade som exempel för lagberedningen i synnerhet i de icke-europeiska länderna. Lagstiftningsprojekt som beaktat de problem och problemlösningar som aktualiserats i samband med beredningen av modellagen har varit under arbete eller slutförts i bland annat Argentina, Australien, Brasilien, Indien, Kanada, Korea, Mexiko, Nya Zeeland, Rumänien, Thailand och Singapore. Också i arbetet med direktivet om elektroniska signaturer drog man nytta av resultatet av arbetet med UNCITRAL:s modellag.

Modellagen innehåller bestämmelser som liknar de som finns i direktivet om ett gemenskapsramverk för elektroniska signaturer om bland annat elektroniska signaturers rättsverkningar, datainnehållet i certifikat, certifikatutfärdares ansvar och ömsesidigt godkännande av certifikat. Modellagen skiljer sig från direktivet i det att den betonar avtalsparternas rätt att avtala om avvikelser från modellagens bestämmelser. Denna utgångspunkt, som betonar avtalsparternas autonomi, är huvudsakligen en följd av det starka inflytande som Förenta staternas lagstiftning har haft på arbetet med modellagen. Till skillnad från direktivet innehåller modellagen också bestämmelser om undertecknarens ansvar. I modellagen föreskrivs det bland annat att undertecknaren är skyldig att uppbevara nyckeln omsorgsfullt och att omedelbart underrätta certifikatutfärdaren om nyckeln försvinner eller något annat som kan äventyra signaturens säkerhet sker.

Annat internationellt samarbete

Ett flertal stater har offentliggjort åtgärdsprogram i anslutning till identifiering. Även vissa privata organisationer och grupperingar arbetar med identifiering, elektroniska identitetshandlingar för medborgarna och internationellt samarbete inom branschen. I synnerhet den finskgrundade Borgågruppen kan nämnas. Den är ett internationellt samarbetsnätverk vars främsta mål är att främja genomförandet av ett system för elektroniska identitetshandlingar som grundar sig på tekniken med öppna nycklar samt smartkort och chipförsedda identitetskort och som är kompatibelt mellan olika länder. Syftet är att hjälpa till att trygga säker elektronisk kommunikation inom den offentliga och privata sektorn i Europa. Gruppen främjar även ibruktagande av kompatibla certifikat och tekniska specifikationer, ömsesidigt godkännande av identifierings- och autentiseringsmekanismer länder emellan och skapande av online-förbindelser över landsgränserna när det gäller administrativa tjänster.

Standardisering

För att uppfylla kraven i direktivet om elektroniska signaturer inleddes 1999 ett samprojekt mellan den europeiska industrin och organisationerna inom standardiseringen, European Electronic Signature Standardization Initiave (nedan EESSI). Inom ramen för EESSI har man vid European Telecommunications Standards Institute (nedan ETSI) och European Committee for Standardization (nedan CEN) inom ett flertal områden tagit fram standarder för produkter, system och tjänster som gäller elektroniska signaturer och certifikat. En av de viktigaste ETSI standarderna är ETSI TS 101 456 (Policy requirements for certification authorities issuing qualified certificates), som gäller verksamheten för utfärdare av kvalificerade certifikat. Även datainnehållet i kvalificerade certifikat och formatet på elektroniska signaturer har standardiserats vid ETSI. I CEN har man standardiserat bland annat kraven på informationssäkerhet när det gäller de system som utfärdarna av kvalificerade certifikat använder och kraven på säkra anordningar för signaturframställning i enlighet med kraven i direktivet om elektroniska signaturer. Referensnumren för dessa standarder har även publicerats i Europeiska unionens officiella tidning (EUT L 175, 15.7.2003, s. 45).

EESSI avslutades i oktober 2004. Arbetet med att ta fram standarder för elektroniska signaturer fortsätter, men koncentreras på andra än grundläggande krav. I ETSI:s TC ESI har prioriteringsområdena varit elektronisk bokföring och fakturering (digital accounting and invoicing) och certifierad e-post (Registered E-mail, REM). CEN:s arbetsgrupp för standardisering av anordningar som används för elektroniska signaturer (CEN/ISSS E-sign) drogs in 2003, men CEN:s medlemmar upprätthåller och uppdaterar fortfarande standarderna inom området. I CEN finns det dessutom flera andra arbetsgrupper som utarbetar standarder för olika områden inom den elektroniska kommunikationen. Efter det att EESSI avslutades är det ICTSB:s (ICT Standards Board) Network and Information Security Steering Group (NISSG) som är ansvarig vid eventuella behov av samordning av arbetet med att ta fram standarder i anslutning till elektroniska signaturer.

Betaltjänstdirektivet

Europaparlamentet och rådet utfärdade den 13 november 2007 ett direktiv om betaltjänster på den inre marknaden (2007/64/EG). Målet med direktivet är att skapa ett gemensamt betalningsområde där ökade skalfördelar och ökad konkurrens leder till en minskning av de för närvarande höga kostnaderna för betalningssystemen. Genom direktivet skapas ett gemensamt ramverk för lagstiftningen för gemenskapsmarknaden i anslutning till betalningar, vilket skapar förutsättningar för integrering och rationalisering av betalningssystemen. Direktivet är viktigt med tanke på denna proposition, eftersom det finns vissa gemensamma drag hos tillhandahållandet av tjänster för elektronisk identifiering och tillhandahållandet av betaltjänster. Dessutom kan de som tillhandahåller tjänster för stark autentisering samtidigt också tillhandahålla betaltjänster.

Betaltjänstdirektivet är till sin natur huvudsakligen ett exempel på totalharmonisering. Medlemsstaterna kan förutom när det gäller de undantag som anges i direktivet inte nationellt utfärda eller vidmakthålla andra bestämmelser om de frågor som regleras genom direktivet.

Betaltjänstleverantörerna delas upp i fyra grupper i artikel 1: kreditinstitut, institut för elektroniska pengar, postgiroinstitut som enligt nationell lagstiftning har möjlighet att tillhandahålla betaltjänster samt betalningsinstitut, som är andra fysiska eller juridiska personer som i enlighet med direktivet har auktoriserats att tillhandahålla betaltjänster. I direktivet finns det bestämmelser om vilka uppgifter som ska ges om betaltjänsterna och om rättigheter och skyldigheter för dem som använder eller tillhandahåller betaltjänster.

Direktivets tillämpningsområde täcker enligt artikel 2 betaltjänster där betalning sker för någon annans räkning och där åtminstone en betaltjänstleverantör är etablerad inom EU:s territorium. Direktivet tillämpas på såväl gränsöverskridande som rent nationella betaltjänster. Utgångspunkten är att direktivet tillämpas på betalningar i alla valutaslag.

De funktioner som enligt artikel 3 undantas från tillämpningsområdet är bland annat betalningar i kontanter, betalningar som görs med presentkort, check eller annat pappersbaserat betalningsmedel, valutaväxling och betalningar mellan betaltjänstaktörer. Från tillämpningsområdet undantas även betalningar som görs med mobiltelefon eller annan digital eller informationsteknisk utrustning, under förutsättning att den som tillhandahåller tjänster som gäller elektronisk kommunikation, system för automatisk databehandling eller nät aktivt deltar i utvecklandet av de digitala nyttigheterna eller tjänsterna, att nyttigheterna och tjänsterna inte kan tillhandahållas utan tjänsteleverantören och att det inte heller finns andra sätt att genomföra betalningarna.

Det nationella genomförandet av direktivet är under beredning i två arbetsgrupper som leds av finansministeriet och justitieministeriet. De nationella lagarna ska enligt direktivet ha trätt i kraft senast den 1 november 2009.

Tjänstedirektivet

Europaparlamentets och rådets direktiv 2006/123/EG om tjänster på den inre marknaden (nedan tjänstedirektivet) antogs i december 2006, i slutet av Finlands EU-ordförandeskap. Tjänstedirektivet ska genomföras inom tre år efter det att det trädde i kraft, dvs. senast den 28 december 2009. De tjänster som det föreskrivs om i denna proposition omfattas av tillämpningsområdet för tjänstedirektivet.

Direktivets innehåll i sak bildar en sorts referensram mot vilken de förfaranden och formaliteter som gäller för tjänsteleverantörerna ska utvärderas. Förfarandena och formaliteterna ska vara icke-diskriminerande, motiverade av tvingande hänsyn till allmänintresset, nödvändiga och stå i rätt proportion till det eftersträvade syftet. Medlemsstaterna ska också se över vissa myndighetsfunktioner för att säkra en administrativ förenkling.

För att administrativ förenkling ska uppnås effektivt finns det i tjänstedirektivet bestämmelser om att medlemsstaterna ska inrätta gemensamma kontaktpunkter genom vilka tjänsteleverantörerna kan få information om nationella krav som gäller tillhandahållandet av tjänster. Tjänsteleverantörerna ska också kunna sköta alla administrativa förfaranden och formaliteter i anslutning till tillhandahållandet av tjänster elektroniskt vid dessa gemensamma kontaktpunkter.

Enligt tjänstedirektivet är medlemsstaterna skyldiga att utveckla det administrativa samarbetet myndigheter emellan. Betydelsen av gränsöverskridande myndighetssamarbete kommer att accentueras när medlemsstaterna lättar på de administrativa förfarandena för tjänsteleverantörerna. Samarbete kommer att bedrivas bland annat med hjälp av kommissionens informationssystem för den inre marknaden (IMI, Internal Market Information System).

Enligt tjänstedirektivet är medlemsstaterna således tvungna att vidta även andra åtgärder än lagstiftningsåtgärder, till exempel att utveckla elektroniska förvaltningsförfaranden och strukturer för administrativt samarbete. När det gäller det nationella genomförandet är det således inte fråga om ett så kallat rent lagstiftningsprojekt, utan inom projektet ska ett betydande antal praktiska åtgärder vidtas för att säkra att direktivet genomförs på ett effektivt sätt.

Arbetet med det nationella genomförandet av tjänstedirektivet pågår vid arbets- och näringsministeriet. I den lag som föreslås har man också strävat efter att beakta tjänstedirektivet så att lagen inte innehåller något som står i strid med direktivet. Tjänstedirektivet innehåller i enlighet med sin huvudregel bland annat förbud mot förhandstillstånd. Leverantörerna av tjänster för stark autentisering omfattas endast av ett sådant anmälningsförfarande som är nödvändigt för att den övervakande myndigheten ska kunna fullgöra sina skyldigheter.

De föreslagna bestämmelserna ålägger Kommunikationsverket en skyldighet att förbjuda tjänsteleverantörer att tillhandahålla tjänster i form av stark autentisering, om de lagstadgade villkoren för tjänsterna eller tjänsteleverantörerna inte uppfylls. Tjänsteleverantörer kan dock börja tillhandahålla sina tjänster utan att Kommunikationsverket behöver vidta några åtgärder. Dessutom bör det observeras att bestämmelserna inte hindrar tillhandahållande av tjänster över huvud

taget, utan endast att tjänsterna tillhandahålls som en viss slags tjänst, om villkoren inte uppfylls. Arrangemanget motsvarar helt bestämmelserna i 4 kap. om kvalificerade certifikat, som grundar sig på direktivet om ett gemenskapsramverk för elektroniska signaturer. Om de krav som ställs i kapitlet inte uppfylls, ska Kommunikationsverket förbjuda tjänsteleverantören att tillhandahålla sina tjänster i form av kvalificerade certifikat. Detta hindrar dock inte tillhandahållande av tjänster i sig. Kapitel 4 innehåller dessutom bestämmelser om kontrollorgan, enligt vilka Kommunikationsverket utnämner kontrollorganen. Detta grundar sig också på direktivet om ett gemenskapsramverk för elektroniska signaturer, som måste ses som specialreglering i relation till tjänstedirektivet.

2.4 Bedömning av nuläget

Marknaden för elektroniska signaturer har inte börjat utvecklas på önskat sätt i Finland. För närvarande är det bara Befolkningsregistercentralen som tillhandahåller tjänster för elektroniska signaturer. Över huvud taget har elektroniska signaturer inte varit i stor användning i vare sig Finland eller resten av Europa. I synnerhet frågorna om förtroende och ansvar har visat sig vara svårlösta.

Även själva begreppet elektronisk signatur är problematiskt i länder som Finland, där det mycket sällan förekommer att något formkrav i likhet med underskrift är förutsättningen för en rättshandling. Med hjälp av elektronisk identifiering baserad på bankernas identifieringskoder har man i Finland i själva verket kunnat åstadkomma samma rättsverkningar som med hjälp av elektroniska signaturer. Följden har emellertid varit en fortgående diskussion om hurudana verktyg och metoder som krävs för att uppnå rättsverkningar i olika situationer.

Även i fortsättningen torde efterfrågan på och utbudet av tjänster för elektroniska signaturer vara av ganska litet mått. Kommissionens strävanden efter att utveckla den gränsöverskridande användningen av elektroniska signaturer i synnerhet med utgångspunkt i kvalificerade certifikat kan öka efterfrågan i någon mån. Med anledning av kommissionens strävanden verkar det i synnerhet med tanke på de finländska företagens verksamhet inom Europeiska ekonomiska samarbetsområdet åtminstone på kort sikt vara viktigt att man genom lagstiftning säkrar verksamhetsbetingelserna för de finländska aktörer som tillhandahåller kvalificerade certifikat för allmänheten. Givetvis kräver också direktivet om ett gemenskapsramverk för elektroniska signaturer fortsatt genomförande.

Det tycks finnas ett betydligt större behov av elektronisk identifiering än av elektroniska signaturer. En ökning av antalet e tjänster och tjänsternas mångfald kräver i framtiden allt oftare tillförlitlig elektronisk identifiering. Med anledning av detta behöver man i Finland skapa en fungerande marknad för stark autentisering. För närvarande används nästan enbart bankkoder för stark autentisering. Dessa koder kommer säkert att vara i användning ännu i flera år, men tillsammans med dem behövs det fler tjänster och tjänsteleverantörer. En fungerande konkurrensutsatt marknad ser också till att tjänsterna håller en skälig prisnivå.

Det finns ingen lagstiftning om elektronisk identifiering. På grund av denna brist har man sökt regler för verksamheten i synnerhet i lagen om elektroniska signaturer. Eftersom denna lag med utgångspunkt i direktivet i praktiken endast gäller tillhandahållande av kvalificerade certifikat för allmänheten, är bestämmelserna inte särskilt väl lämpade för tillhandahållandet av tjänster för elektronisk identifiering. Dessutom har bestämmelserna i lagen i viss mån feltolkats på ett sätt som har skapat alltför hårda krav på nya tjänsteleverantörer.

Det finns inte heller några bestämmelser där det allmänt definieras vilka elektroniska tjänster som ska förutsätta stark autentisering. Stark autentisering kan i typiska fall komma i fråga i synnerhet i samband med sådana elektroniska tjänster som ekonomiska eller rättsliga förbindelser förutsätter. Det är dock inte för närvarande och sannolikt inte heller i framtiden nödvändigt att utfärda några sådana allmänna bestämmelser, och denna proposition innehåller inte heller några sådana bestämmelser.

Det finns ändå redan nu bestämmelser som handlar om reglering i vissa situationer. 18 §

i lagen om elektronisk kommunikation i myndigheternas verksamhet gäller bevislig elektronisk delgivning. Enligt paragrafens 2 mom. ska parten eller dennes företrädare identifiera sig när beslutshandlingen hämtas. Dessutom har det i 18 § i lagen om förhindrande och utredning av penningtvätt och av finansiering av terrorism (503/2008) föreskrivits om skärpta krav på kontroll vid identifiering på distans. I paragrafens 3 punkt föreskrivs det om de identifieringsmetoder som kan användas i identifieringen på distans.

I fortsättningen kan antalet bestämmelser som gäller speciella situationer öka. Även med tanke på denna eventuella utveckling är det mycket viktigt att skapa en regleringsram som den övriga lagstiftningen kan stödja sig på.

Statens revisionsverks rapport

Statens revisionsverk publicerade våren 2008 en rapport om utvecklandet och användningen av identifieringstjänster i den offentliga förvaltningen (161/2008). I rapporten konstaterade revisionsverket många brister och missförhållanden bland annat när det gällde samarbete mellan och samordning av olika myndigheter, upphandlingsförfaranden, Befolkningsregistercentralens verksamhet och arrangemangen kring verksamheten samt i verksamheten vid Rättsskyddscentralen för hälsovården, Skattestyrelsen och dataskyddsombudsmannen.

Det är klart att man genom den lag som föreslås endast kan sträva efter att påverka en del av de missförhållanden som revisionsverket har fäst uppmärksamhet vid i sin rapport. Arbetet fortsätter särskilt under åren 2009 2010 i enlighet med vad som bestämts i det principbeslut om elektronisk identifiering som statsrådet godkände den 5 mars 2009.

Revisionsverkets rapport innehåller vissa observationer som har samband med denna proposition. I fråga om utvecklandet av strukturerna för styrning av verksamheten och lagstiftningen konstateras det i rapporten bland annat att enligt revisionsverkets uppfattning förutsätter en enhetligare och rationaliserad verksamhet, en effektivare övervakning, förfarandena gällande datasäkerheten, en fungerande fri identifierarmarknad samt i synnerhet individernas rättskydd och dataskydd att identifieringstjänsterna och identifieringen regleras i lag. Kommunikationsministeriet, finansministeriet och justitieministeriet bör också tillsammans vidta snabba åtgärder för att utveckla lagstiftningen om elektronisk identifiering.

Vidare ansåg revisionsverket att det inte finns några faktiska grunder för den certifikatavgift som Kommunikationsverket tar ut och som grundar sig på mängden certifikat och att avgiften är problematisk med tanke på en fungerande certifikatmarknad. Revisionsverket ansåg att kommunikationsministeriet bör vidta åtgärder för att förnya avgifterna för tillsynen över certifikat, så att något annat än certifikatens mängd ligger till grund för avgiften.

I fråga om marknaden för identifieringstjänster och riskerna i anslutning därtill fäste revisionsverket uppmärksamhet vid att det på den nuvarande marknaden för identifieringstjänster inte råder någon reell konkurrens, utan att användningen av identifikatorer har koncentrerats på användningen av nätbankskoder. På längre sikt kan detta vara förenat med ekonomiska risker. Emellertid har statsförvaltningens egna åtgärder bidragit till den uppkomna situationen. Det framkom i granskningen att Befolkningsregistercentralens verksamhet hade en snedvridande effekt på marknaden vid millennieskiftet, vilket bidrog till att privata aktörer som utövade motsvarande verksamhet med certifikattjänster upphörde med verksamheten. Befolkningsregistercentralen har å sin sida inte kunna erbjuda användbara alternativ till identifieringsverktyg för de stora massorna.

Vidare ansåg revisionsverket att endast reell konkurrens mellan identifieringstjänsterna ser till att priserna för identifieringstransaktioner håller sig på skälig nivå vid användningen av nätbankskoder och andra identifikatorer. Den offentliga förvaltningen bör vara öppen för de nya lösningar för identifieringstjänster som utvecklas på identifierarmarknaden. Den offentliga förvaltningen bör dock se till att säkerhetsnivån för nya identifieringstjänster fastställs och certifieras på ett jämlikt sätt, vilket ligger till grund för att användningen av identifieringstjänsterna kan tillåtas inom den offentliga förvaltningen,

t.ex. för e tjänster som kräver stark autentisering.

Enligt revisionsverket bör den offentliga förvaltningen koncentrera sig på att utnyttja de identifieringstjänster som redan finns på marknaden och som kan utvecklas och den bör inte delta direkt i produktionen av identifieringsverktyg. Det bör överlåtas åt de privata aktörerna att utveckla metoder och verktyg för identifiering och att ta dem i bruk på bred front. Den offentliga förvaltningen kan stödja utvecklingsverksamheten och skapa verksamhetsförutsättningar genom forsknings- och utvecklingsfinansiering, men dock på ett sätt som inte ger upphov till snedvridningar på marknaden.

I fråga om Befolkningsregistercentralen ansåg revisionsverket att centralen i framtiden bör koncentrera sig enbart på sin myndighetsuppgift och låta övriga uppgifter i anslutning till affärsverksamhet eller annan verksamhet än kärnverksamheten skötas av marknaden.

Enligt revisionsverket bör anskaffningen av infrastrukturer för certifikattjänster i framtiden skötas som helt externaliserade tjänster. Befolkningsregistercentralen har då till uppgift att säkra att tjänsten fungerar på ett högklassigt sätt och att sköta myndighetsuppgifter som närmast gäller registrering. Externalisering och applikationsuthyrning kan motivera även IT-leverantörerna på marknaden att utveckla sina tjänster så att de stöder verksamheten inom den offentliga förvaltningen. Handlingsmodellen följer statens IT-strategi genom att man på detta sätt inte förlitar sig på bara en tjänsteleverantör. Dessutom kan även andra myndigheter producera certifikat för egna användningssyften genom samma system av certifikattjänster som man fått tillgång till via ramarrangemangen, utan att Befolkningsdatacentralen fungerar som mellanhand och aktör som ger upphov till ökade kostnader. Även de allmänna förutsättningarna för certifikatverksamheten och statens roll i sammanhanget bör utvärderas på nytt.

3 MÅLSÄTTNING OCH DE VIKTIGASTE FÖRSLAGEN

3.1 Målsättning

Genom propositionen utfärdas en helt ny lag om stark autentisering och elektroniska signaturer. Samtidigt föreslås det att den gällande lagen om elektroniska signaturer upphävs jämte ändringar.

Syftet med lagen är att främja utbudet av tjänster för stark autentisering och att skapa grundläggande marknadsregler för tillhandahållandet av tjänster. Ett annat syfte med lagen är att främja användningen av elektroniska signaturer och tillhandahållandet av produkter och tjänster i anslutning till dem. Samtidigt strävar man efter att säkra att kraven på informationssäkerhet och dataskydd beaktas vid tillhandahållandet av tjänsterna. Genom att främja tillhandahållandet av elektroniska identifieringstjänster är syftet med lagen att främja e-tjänster och elektronisk kommunikation i allmänhet samt informationssäkerhet och dataskydd i anslutning därtill.

Genom lagen strävar man efter att skapa en fungerande marknad för elektronisk identifiering genom att förse aktörerna inom branschen med vissa grundläggande regler. Utgångspunkten för denna marknad är att identifieringsverktygen ska vara allmänt användbara och konkurrensen fri. Elektronisk identifiering fungerar i regel i förtroendenät som byggs upp av tjänsteleverantörerna. Vissa grundläggande regler och tillsyn över att de efterlevs informerar tjänsteleverantörerna om att alla aktörer inom branschen når upp till en viss grundläggande nivå i sin verksamhet. Detta är till avsevärd hjälp när förtroendenäten vidareutvecklas.

Ett annat syfte med lagen är att möjliggöra användningen av elektroniska signaturer och tillhandahållandet av produkter och tjänster i anslutning till dem. Avsikten är att man genom den del av lagen som gäller elektroniska signaturer ska fortsätta att genomföra det direktiv om ett gemenskapsramverk för elektroniska signaturer som gäller i EU. Det föreslås dock att lagen utfärdas som helt ny, eftersom en ändring av den skulle ge upphov

till en mycket oklar struktur och lagen därför skulle vara svårläst.

3.2 De viktigaste förslagen

Lagens viktigaste förslag i sak finns i 3 och 4 kap. Av dessa innehåller 3 kap. grundläggande bestämmelser om tillhandahållande av tjänster för stark autentisering och 4 kap. grundläggande bestämmelser om tillhandahållande av kvalificerade certifikat. Kapitlen innehåller uttömmande bestämmelser om tillhandahållandet av en viss tjänst. Elektroniska signaturer och avancerade elektroniska signaturer kan skapas med identifieringsverktyg på det sätt som verktygens egenskaper tillåter.

Elektronisk identifiering

Det föreslås att lagen endast ska reglera tillhandahållandet av tjänster för stark autentisering. Svag autentisering omfattas alltså inte alls av bestämmelserna. Metoderna för svag autentisering är nuförtiden de mest använda identifieringsmetoderna. I praktiken innebär detta en kombination av användarnamn och lösenord. Identifieringsmetoder av detta slag används i dag och även i framtiden till exempel i olika diskussionsforum på Internet. De är förknippade med betydande problem när det gäller användarvänlighet och informationssäkerhet, så man strävar inte speciellt efter att främja användningen av dem. Fördelen med dem är att de är avgiftsfria och därför passar de för tjänster som inte gäller ekonomiska fördelar eller rättshandlingar. Det är inte nödvändigt att försöka införa bestämmelser i lag om frågor som gäller tillhandahållandet av dessa tjänster.

Vid elektronisk identifiering är det möjligt att skilja mellan ”aktiv” identifiering (dvs. verifiering) och ”passiv” identifiering av personer. Med aktiv identifiering av en person avses här en situation där en person handlar aktivt, dvs. framför ett påstående om sin identitet, vars riktighet kan verifieras i samband med identifieringen. Vid passiv identifiering försöker man däremot identifiera en person utan att personen själv påstår något om sig. Ett exempel på detta är när man söker en viss person i en stor människomassa, till exempel med hjälp av kameraövervakning med ansiktsigenkänning. Passiv identifiering förutsätter inte någon aktiv åtgärd av den som ska identifieras. Den identifierade är inte nödvändigtvis ens medveten om att en identifiering skett. Som exempel på när identifiering av denna typ möjligen kan användas kan man nämna teknisk övervakning med ansiktsigenkänning.

Den föreslagna lagen gäller endast tjänster som tillhandahålls och användningen av dessa. I detta sammanhang krävs alltid aktiva handlingar av den som ska identifieras. Detta gäller vid såväl införskaffandet av identifieringsverktyg som enskilda identifieringstransaktioner. Den föreslagna lagen gäller således inte över huvud taget användning av metoder för passiv identifiering.

Lagen gäller identifiering av fysiska personer. Fysiska personer kan enligt bestämmelser om företrädande som finns någon annanstans i lag företräda andra fysiska eller juridiska personer, men kopplande av rollinformation till identifieringen föreslås inte omfattas av tillämpningsområdet för den föreslagna lagen. Dessa tjänster är ännu bara i ett utvecklingsskede.

Verksamhet som gäller tillverkning, import eller försäljning av verktyg för stark autentisering omfattas inte av tillämpningsområdet för den föreslagna lagen. Avsikten är således att lagen enbart ska gälla tillhandahållande av tjänster. Dessutom ska lagen endast tillämpas på tillhandahållande av tjänster för allmänheten. System som är avsedda för slutna miljöer, såsom system för företagens interna behov av identifiering, omfattas således inte av tillämpningsområdet.

Tillämpningsområdet omfattar inte heller sådant tillhandahållande av tjänster där en organisation använder sina egna metoder för stark autentisering enbart för att identifiera sina egna kunder inom ramen för sina egna tjänster. På sådan verksamhet tillämpas dock bestämmelserna i 3 §, 20 § 1 mom., 21 22 §, 23 § 1 mom., 25 § 1 och 2 mom., 27 § 1 mom., 2 mom. 1 punkten och 3 mom. samt 42 § 4 mom. Det är fråga om ett konsumentskyddsperspektiv och därför ska konsumentombudsmannen utöva tillsyn över verksamheten. Det är inte särskilt sannolikt att det uppstår särskilt många tjänster av detta slag,

eftersom de är ganska dyra för aktörerna och besvärliga för användarna.

Det föreslås således att lagen ska reglera tillhandahållandet av tjänster för stark autentisering. Enligt definitionerna avses med leverantör av identifieringstjänster en tjänsteleverantör som tillhandahåller tjänster för stark autentisering till tjänsteleverantörer som använder sådana tjänster eller som tillhandahåller elektroniska identifieringsverktyg eller identifieringsmetoder, eller bådadera, som används vid elektronisk identifiering. Lagen omfattar således både tillhandahållande av tjänster och utgivning av verktyg. Det är möjligt att en tjänsteleverantör har båda dessa roller, men särskilt i ett mera avancerat skede ska rollerna kunna skiljas från varandra.

Enligt 2 § 1 punkten i den förslagna lagen avses med stark autentisering ett förfarande där personer identifieras med hjälp av tillförlitliga elektroniska metoder samtidigt som identifikatorn verifieras som autentisk och riktig. Av de tre kriterier som finns i punkten måste två uppfyllas för att den elektroniska identifieringen ska räknas som stark autentisering. I 8 § föreslås dessutom krav som stark autentisering måste uppfylla. Enligt paragrafen ska en omsorgsfull inledande identifiering enligt 17 § ligga till grund för en identifieringsmetod och uppgifterna om den inledande identifieringen ska kunna kontrolleras i efterskott i enlighet med 24 §. Med hjälp av identifieringsmetoden ska det gå att entydigt identifiera innehavaren av ett identifieringsverktyg för stark autentisering och att med tillräckligt hög tillförlitlighet säkerställa att enbart innehavaren av identifieringsverktyget kan använda det. Metoden ska vara tillräckligt säker och tillförlitlig med tanke på de informationssäkerhetsrisker som är förknippade med den teknik som används.

Bestämmelser om krav som ställs på tjänsteleverantörerna finns i 9 §. Det är närmast fråga om att tjänsteleverantören inte får ha en viss typ av kriminell bakgrund.

Enligt 10 § i den föreslagna lagen ska de leverantörer av tjänster för stark autentisering som är etablerade i Finland göra en anmälan till Kommunikationsverket om tillhandahållandet av tjänster. Det föreslås att Kommunikationsverket kontrollerar tjänsteleverantörerna och deras tjänster på samma sätt som tjänsterna för kvalificerade certifikat när det gäller elektroniska signaturer. Tillsynen föreslås dock i huvudsak vara efterhandstillsyn i enlighet med bestämmelserna i 5 kap.

I 13–16 § i lagförslaget finns det bestämmelser om de grundläggande kraven för tillhandahållande av tjänster för stark autentisering. Den föreslagna 13 § innehåller bestämmelser om krav som ställs på tjänsteleverantörens personal, om ekonomiska resurser och om skyldigheter i fråga om informationssäkerhet. Den föreslagna 14 § kräver att tjänsteleverantören har principer för identifieringen. De föreslagna 15 och 16 § gäller informationsskyldighet. Dessutom innehåller 6 och 7 § bestämmelser om hur personuppgifter och uppgifter i befolkningsdatasystemet ska behandlas. De sistnämnda bestämmelserna är gemensamma för tjänsteleverantörer enligt 3 och 4 kap.

I 17 § i lagförslaget finns det bestämmelser om den inledande identifiering av personer som allmänt anses vara en av hörnstenarna i stark autentisering. Huvudregeln är att den som tillhandahåller tjänster för stark autentisering ska identifiera den som ansöker om ett verktyg för stark autentisering genom att fastställa hans eller hennes identitet 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 av tjänster för stark autentisering, om den så önskar, även använda ett giltigt pass som har utfärdats av en myndighet i någon annan stat. Enligt den övergångsbestämmelse som finns i den föreslagna 51 § får en tjänsteleverantör, om den så önskar, till och med den 31 december 2012 använda ett giltigt körkort som utfärdats efter september 1990 av en Finska myndighet.

Den inledande identifieringen ska göras personligen, förutom om leverantörerna av tjänster för stark autentisering sinsemellan har avtalat om möjligheten att lita på identifieringar som en annan leverantör har gjort. Det är således inte möjligt att ha kedjor av inledande identifiering, utan den tjänsteleverantör som utförde den ursprungliga inledan-

de identifieringen ska alltid vara med i avtalsarrangemangen.

I den föreslagna 5 § konstateras det i fråga om det gällande rättsläget att man med hjälp av verktyg för stark autentisering kan utföra rättshandlingar om parterna så önskar, såvida det i lagstiftningen inte finns särskilda formkrav som gäller den aktuella rättshandlingen. I Finland är rättshandlingar av detta slag i betydande minoritet. Rättshandlingar kan dock förbjudas i avtal mellan parterna, eller beläggas med begränsningar i fråga om art eller belopp. Den föreslagna 18 § innehåller närmare bestämmelser om sådana förbud och begränsningar.

Den föreslagna 19 § utgör ett undantag till den strävan efter teknologineutralitet som uttrycks i 2 kap. Paragrafen gäller användningen av certifikat som verktyg för stark autentisering och innehåller bestämmelser om datainnehållet i certifikat. En motsvarande bestämmelse om kvalificerade certifikat finns i 30 §.

Den föreslagna 20 § gäller utgivning av identifieringsverktyg. I 3 mom. konstateras det tydligt att verktygen ska vara personliga. På motsvarande sätt innehåller den föreslagna 23 § 2 mom. ett förbud mot att innehavaren av ett verktyg överlåter det åt en annan person.

Den föreslagna 21 § gäller överlåtande av identifieringsverktyg till dess innehavare. Avsikten är att även överlåtelse per post ska vara tillåtet under vissa villkor. I den föreslagna 24 § finns det bestämmelser om förvaring av uppgifter som gäller händelserna vid stark autentisering och identifieringsverktyget samt om förvaringstiderna.

De föreslagna 25 och 26 § gäller återkallande av ett verktyg för stark autentisering eller förhindrande av att verktyget används. Det kan till exempel vara fråga om att verktygets innehavare anmäler att verktyget har försvunnit. Det finns dessutom också situationer där tjänsteleverantören bör ha möjlighet att återkalla ett verktyg eller förhindra att det används.

Den föreslagna 27 § innehåller bestämmelser om ansvaret för innehavare av identifieringsverktyg när det gäller obehörig användning av verktyg. Huvudregeln är att innehavaren av ett verktyg för stark autentisering ansvarar för obehörig användning av verktyget endast om han eller hon har överlåtit verktyget åt en annan person, om det att verktyget har försvunnit, obehörigt har kommit i någon annans besittning eller obehörigt har använts beror på innehavarens vårdslöshet. Detsamma gäller om innehavaren har försummat att, utan obefogat dröjsmål efter det att saken har upptäckts, anmäla till tjänsteleverantören eller någon annan aktör som denne har angett att verktyget har försvunnit, obehörigt har kommit i någon annans besittning eller obehörigt har använts.

Elektroniska signaturer

I fråga om elektroniska signaturer motsvarar bestämmelserna i huvudsak bestämmelserna i lagen om elektroniska signaturer, genom vilka bestämmelserna i direktivet om ett gemenskapsramverk för elektroniska signaturer genomförs. Hänvisningarna i vissa paragrafer om att tillhandahållande av kvalificerade certifikat är utövning av offentlig makt slopas. Detta beror på utgångspunkten i propositionen att bestämmelserna i lagförslaget enbart ska gälla privata tjänsteleverantörer. Ämnet behandlas närmare i den del som gäller lagstiftningsordning.

Enligt 2 § 9 punkten i lagförslaget avses med elektronisk signatur data i elektronisk form som är fogade till eller logiskt knutna till andra elektroniska data och som används som en metod för verifiering av undertecknarens identitet. Definitionen är densamma som i den gällande lagen om elektroniska signaturer och baserar sig på direktivet om ett gemenskapsramverk för elektroniska signaturer.

Enligt 10 punkten i samma paragraf avses med avancerad elektronisk signatur en elektronisk signatur som är knuten uteslutande till undertecknaren, gör det möjligt att identifiera undertecknaren, är skapad med medel som endast undertecknaren kontrollerar, och är knuten till andra elektroniska data på ett sådant sätt att eventuella senare förvanskningar av dessa data kan upptäckas. Såsom ovan har konstaterats kan certifikat enligt definitionerna i den föreslagna lagen användas för såväl stark autentisering som elektroniska signaturer.

Lagförslagets 28 § innehåller bestämmelser om säkra anordningar för signaturframställning som motsvarar 5 § i den gällande lagen. Den största delen av det föreslagna 4 kap., dvs. 30-41 §, gäller endast kvalificerade certifikat och utfärdare av kvalificerade certifikat. Med kvalificerat certifikat avses ett certifikat som har utfärdats av en sådan utfärdare av kvalificerade certifikat som avses i 33-38 §. Ett kvalificerat certifikat ska innehålla uppgift om att certifikatet är ett kvalificerat certifikat, uppgift om certifikatutfärdaren och dennes etableringsstat, undertecknarens namn eller pseudonym med uppgift om att det är en pseudonym, signaturverifieringsdata som motsvarar de signaturframställningsdata som undertecknaren innehar, det kvalificerade certifikatets giltighetstid, det kvalificerade certifikatets identifieringskod, certifikatutfärdarens avancerade elektroniska signatur, eventuella begränsningar av användningen av det kvalificerade certifikatet, och särskilda uppgifter om undertecknaren, om de behövs med tanke på ändamålet med det kvalificerade certifikatet.

I 5 § 2 mom. i lagförslaget konstateras det att om det enligt lag krävs underskrift för en rättshandling, uppfylls detta krav åtminstone genom en sådan avancerad elektronisk signatur som baserar sig på ett kvalificerat certifikat och som har skapats med en säker anordning för signaturframställning. Dessutom konstateras det att elektroniska signaturer inte ska förvägras rättslig verkan enbart på den grunden att de har skapats med någon annan metod för framställning av elektroniska signaturer. Bestämmelsen motsvarar den gällande lagen, men den senare meningen har lagts till för att bestämmelsen ska följa artikel 5.2 i gemenskapsdirektivet om elektroniska signaturer. Avsikten är inte att ändra den gällande lagen, utan att förtydliga ett ställe som upprepade gånger har tolkats fel.

Övriga förslag

Till propositionen hänför sig tio andra lagar. De måste ändras därför att genom propositionen upphävs lagen om elektroniska signaturer. Hänvisningarna till denna lag ändras till hänvisningar till lagen om stark autentisering och elektroniska signaturer.

Därutöver föreslås det att till bestämmelserna om identifiering som ingår i 18 § i lagen om elektronisk kommunikation i myndigheternas verksamhet och i 18 § i lagen om förhindrande och utredning av penningtvätt och av finansiering av terrorism fogas ett identifieringsverktyg som nämns i propositionen för att uttryckligen godkännas i identifieringen.

Bestämmelserna om elektronisk signatur som ingår i vissa lagar om skatterätt ändras så att det i fråga om kravet på signatur förutsätts en avancerad elektronisk signatur eller annan godtagbar elektronisk signatur.

Utgångspunkten i vår rättsordning är att ett formkrav gäller bara mycket få rättshandlingar. Även kontakterna till myndigheter är vanligen formfria. När en signatur förutsätts är det fråga om ett formkrav. Användning av en avancerad elektronisk signatur är då behövligt. De ändrade föreskrifterna hindrar inte heller i fortsättningen godkännande av andra signaturer.

4 PROPOSITIONENS KONSEKVENSER

4.1 Ekonomiska konsekvenser

I Finland har produkter och tjänster i anslutning till elektroniska signaturer hittills tagits fram närmast med samhällsfinansiering. Inom tillhandahållandet av tjänster har man än så länge inte lyckats skapa någon lönsam modell för affärsverksamheten. Tillhandahållandet av elektroniska signaturer på det sätt som man från början av 1990-talet har tänkt sig den rättsliga strukturen för tillhandahållandet av tjänster kommer även framöver att innebära utmaningar med tanke på affärsverksamhetsmodellen. Detta beror på att det uttryckligen är kännetecknande för verksamheten att det inte finns något avtalsförhållande mellan leverantören av signaturtjänster och den part som förlitar sig på tjänsterna. Då finns det inte heller något naturligt faktureringsställe.

Direktivet som gäller elektroniska signaturer medför ganska hårda krav på tillhandahållandet av kvalificerade certifikat. Detta har för sin del också kunnat påverka den svaga utvecklingen på marknaden för tjänster som

gäller elektroniska signaturer. Man hoppas att den föreslagna lagen ska främja sådana tjänster som gäller elektroniska signaturer och speciellt utbudet av andra certificat än kvalificerade certifikat, eftersom det i lagen tydligt konstateras att elektroniska signaturer och avancerade elektroniska signaturer kan skapas med identifieringsverktyg på det sätt som verktygens egenskaper tillåter. Användningen av certifikat vid identifiering torde också öka i framtiden.

Finansministeriet har tillsatt en arbetsgrupp för att diskutera hur statens certifikatproduktion möjligtvis kan omorganiseras. Arbetsgruppen ska slutföra sitt arbete hösten 2009. Inom ramen för projektet är det av särskild vikt att man klarlägger Befolkningsregistercentralens verksamhet som dels myndighet och dels tjänsteleverantör. Projektet har direkta konsekvenser för Befolkningsregistercentralens verksamhet som tjänsteleverantör. Ur propositionens synvinkel är Befolkningsregistercentralen däremot en tjänsteleverantör bland andra, och propositionen har således inga direkta följder för Befolkningscentralens verksamhet. I praktiken torde dock en eventuell ökning av konkurrensen ha en viss påverkan. I finansministeriets arbetsgrupp dras slutsatser om bland annat huruvida man i framtiden kan eller bör använda statlig finansiering vid tillhandahållandet av tjänster, och i vilka situationer.

När det gäller elektronisk identifiering är det lättare att hitta en modell för affärsverksamheten. Detta beror i synnerhet på en skillnad i den juridiska grundstrukturen jämfört med tillhandahållandet av elektroniska signaturer, som innebär att det mellan dem som tillhandahåller tjänster för stark autentisering, de tjänsteleverantörer som använder dessa tjänster och innehavarna av verktygen råder ett rättsläge som regleras genom avtal. Trots detta bedöms det inte heller när det gäller identifiering vara fråga om någon speciellt betydande affärsverksamhet ekonomiskt sett. Elektronisk identifiering är inte ett värde i sig, utan ett verktyg för elektroniska tjänster och elektronisk kommunikation. Den indirekta ekonomiska betydelsen av elektronisk identifiering som möjliggörare av en betydande ökning av mängden och mångfalden av e-tjänster och tjänster för elektronisk kommunikation är anmärkningsvärd. Detta är den aspekt som man hoppas ska locka in nya aktörer på marknaden.

Det är skäl att anta att de tjänsteleverantörer som tillhandahåller tjänster för stark autentisering är stora aktörer, och åtminstone tills vidare finns det inga aktörer i blickfältet vars affärsverksamhet skulle bestå av enbart identifieringstjänster. Ett av målen med den föreslagna lagen är att det ska kunna komma in fler tjänsteleverantörer på vår marknad. Det är dock inte att vänta att antalet tjänsteleverantörer ska kunna stiga till fler än några få på vår marknad, som hursomhelst är ganska liten till omfattningen.

Av de potentiellt nya tjänsteleverantörer som finns i blickfältet torde teleföretagen ha kommit längst och kan eventuellt få ut sina mobilcertifikat på marknaden redan under 2009. Tillhandahållandet av mobilcertifikat innebär troligen ett ganska omfattande byte av SIM-kort för teleföretagen och samtidigt en betydande ekonomisk satsning. Mobilcertifikaten gör det dock möjligt att använda en mångfald av tjänster på ett tillförlitligt sätt oberoende av tid och plats. Mobilcertifikatens framgång torde förutsätta att certifikaten kan ges ut i betydande omfattning så snabbt som möjligt. En snabb utgivning ökar sannolikt samtidigt snabbt efterfrågan på nya tjänster. Detta skulle ha en stor ekonomisk betydelse för väldigt många tjänsteleverantörer som använder identifieringstjänster. Lagen strävar efter att en snabb start ska vara möjlig för alla nya leverantörer av identifieringstjänster.

Propositionen har inga direkta konsekvenser för användningen av bankernas identifieringskoder, utan de kan även i fortsättningen användas på samma sätt som hittills. Det system som föreslås torde på kort sikt i någon mån stärka bankkodernas ställning som tillförlitlig identifieringsmetod, under förutsättning att de banker som tillhandahåller dem gör en anmälan enligt lagen till Kommunikationsverket. I det omvända fallet kan användningen av bankernas identifieringskoder börja ifrågasättas, i synnerhet i samband med den offentliga sektorns tjänster.

I framtiden torde bankerna bli tvungna att också överväga huruvida de själva ska tillhandahålla identifieringstjänster eller om de

ska börja använda tjänster som tillhandahålls av andra, eller möjligen bådadera. Bankernas identifieringskoder kommer sannolikt att användas ännu under många år. De har dock sina begränsningar, i synnerhet i en värld som blir allt mer mobil. Det bör dock noteras att bankernas nuvarande identifieringskoder är mycket billiga för bankerna och att kostnaderna för dem ingår i de paketpris för banktjänster som kunderna betalar. Av denna anledning måste de nya identifieringsverktyg som eventuellt kommer ut på marknaden prismässigt vara mycket konkurrenskraftiga.

Efterlevnaden av den föreslagna lagen övervakas av Kommunikationsverket. Det är ett nettobudgeterat verk, vilket innebär att aktörerna ska betala för tillsynen. Eftersom det inte är möjligt att direkt skilja ut de prestationer som utförts och avgifterna för dem, är de avgifter som aktörerna betalar för tillsynen till sin juridiska natur skatter. Man har försökt fastställa nivån på avgifterna så att de inte blir ett hinder för nya tjänsteleverantörer att inleda sin verksamhet. Den tillsynsavgift som leverantörerna av identifieringstjänster ska börja betala per år föreslås vara 12 000 euro. Verksamheten för de certifikatutfärdare som tillhandahåller kvalificerade certifikat granskas årligen, och därför blir den tillsynsavgift som de ska betala klart större. Avgiften föreslås vara 40 000 euro om året. För Befolkningsregistercentralen innebär detta att avgiften blir klart mindre än den nuvarande.

Den föreslagna lagen har inga direkta konsekvenser för sådant tillhandahållande av tjänster som inte omfattas av lagens tillämpningsområde. Om lagen uppnår sitt mål att skapa förutsättningar för en fungerande marknad, kan behovet av att utarbeta egna lösningar för identifiering minska. Detta kan ge företagen kostnadsbesparingar och samtidigt öka säkerheten i identifieringsfunktioner.

4.2 Organisatoriska konsekvenser

Den lag som föreslås har i viss mån konsekvenser för Kommunikationsverket, vars uppgiftsfält kommer att inkludera tillsyn över tillhandahållandet av tjänster för stark autentisering. Eftersom tillsynen dock i regel är efterhandstillsyn, kräver verksamheten ingen betydande ökning av resurserna. Mest arbete föranleds Kommunikationsverket av registreringen av aktörerna, för vilken det fastställs en särskild avgift.

Hittills har ungefär ett halvt årsverke funnits till förfogande för tillsynen över tjänsterna för elektroniska signaturer. Endast Befolkningsregistercentralen har gjort en anmälan enligt lagen om elektroniska signaturer om tillhandahållande av kvalificerade certifikat. Centralen har betalat 80 000 euro per år i tillsynsavgift till Kommunikationsverket.

I fortsättningen kräver tillsynen över tillhandahållandet av tjänster för stark autentisering och kvalificerade certifikat uppskattningsvis cirka ett årsverke av Kommunikationsverkets arbetskraft. Antalet potentiella leverantörer av elektroniska identifieringstjänster antas för närvarande vara högst 12. Av dessa är nio banker eller sammanslutningar av tjänsteleverantörer enligt 10 § i lagen som bildats av banker och tre är teleföretag. Eftersom antalet betalare väntas stiga, har man samtidigt kunnat minska den avgift som betalas av de certifikatutfärdare som tillhandahåller kvalificerade certifikat. Samtidigt ändras också avgiftsgrunden för dem så att den utgår från tjänsteleverantören. Tills vidare är Befolkningsregistercentralen den enda tillhandahållaren av kvalificerade certifikat i blickfältet.

Eftersom tillsynsavgifterna är skatter till sin juridiska natur, måste det föreskrivas om deras storlek i lag. Av denna anledning bör det finnas beredskap att ändra lagen även med kort tidtabell, om man ser att den avgiftsnivå som nu har fastställts eller att grunderna för fastställande av avgiften inte möjliggör tillräckligt med resurser för Kommunikationsverkets tillsyn, eller om avgifterna ger upphov till ett överskott hos verket.

Enligt den föreslagna lagen ska dataombudsmannen övervaka efterlevnaden av lagens bestämmelser om personuppgifter. Dessutom ska Konsumentverket övervaka tillhandahållandet av tjänster enligt 1 § 2 mom. när en sammanslutning tillämpar en egen metod för stark autentisering för att identifiera enbart sina egna kunder i de egna tjänsterna. Man kan inte bedöma att dessa

bestämmelser på något betydande sätt skulle öka uppgifterna för dessa myndigheter.

Den föreslagna lagen har inga direkta konsekvenser för andra myndigheters verksamhet. Befolkningsregistercentralens certifikatverksamhet utvärderas inom finansministeriets projekt för omorganisering av statens certifikatproduktion. Dessutom ska social- och hälsovårdsministeriet enligt statsrådets principbeslut om elektronisk identifiering omvärdera Tillstånds- och tillsynsverket för social- och hälsovårdens (Valvira) roll som producent av certifikattjänster så snabbt som möjligt efter det att finansministeriet har slutfört projektet för omorganisering av statens certifikatproduktion.

4.3 Konsekvenser för informationssamhället

Finland har under de senaste åren förlorat sin ställning som föregångare inom informationssamhällsutvecklingen. En orsak till detta är att utbudet och användningen av e tjänster och tjänster inom den elektroniska kommunikationen har utvecklats långsamt. Just nu befinner vi oss dock i en situation där människorna så småningom börjar ha samlat på sig erfarenhet av att använda e tjänster. Det är skäl att anta att efterfrågan på e tjänster kan öka betydligt i fortsättningen. Ökad efterfrågan är en följd av de fördelar som e tjänsterna kan erbjuda användarna, eftersom ärenden kan skötas hemifrån, utan köer och oberoende av öppettider.

Man försöker kraftigt stödja en ökad efterfrågan på e tjänster genom åtgärder av det allmänna. Det ökade antalet tjänster och särskilt deras mångfald kräver i framtiden allt oftare tillförlitlig elektronisk identifiering. För tillfället pågår en del lagstiftningsprojekt, t.ex. en reform av lagstiftningen om konsumentkrediter, där planen är att stark autentisering ska vara en förutsättning för tjänster som erbjuds genom fjärranslutning. Mängden lagstiftning av denna typ torde öka under de närmaste åren. För att systemet ska fungera måste det också finnas ett sådant regelverk som definierar tillförlitlig elektronisk identifiering, dvs. stark autentisering, och de grundläggande förutsättningarna för att tillhandahålla tjänster.

E tjänster förutsätter att parterna får förtroende för varandra på ett helt annat sätt än när ärenden sköts på traditionellt sätt genom fysisk närvaro. Den som använder tjänsterna ska kunna lita på att tjänsteleverantören har byggt upp sin service så att till exempel kraven på informationssäkerhet och integritetsskydd har beaktats. Tjänsteleverantören ska å sin sida bland annat kunna lita på att den som använder tjänsterna via en fjärranslutning är den som han eller hon ger sig ut för att vara.

Av det ovan nämnda följer att främjandet av stark autentisering är en nödvändig grundförutsättning för utvecklingen av det finländska informationssamhället. En fortsatt utveckling av tillförlitliga elektroniska tjänster och elektronisk kommunikation är knappast möjlig utan tillförlitlig elektronisk identifiering och lagstiftning som gäller sådan identifiering. Samtidigt kan några särskilda problem lösas, såsom t.ex. frågan om tillförlitlighet när det gäller tillhandahållande och användning av elektroniska tjänster som har en viss åldersgräns.

Om man får till stånd en fungerande marknad för elektronisk identifiering, främjas utvecklingen av e tjänster och tjänster för elektronisk kommunikation betydligt i vårt land. Propositionens konsekvenser för informationssamhället är således betydande.

5 Beredning

Beredning vid kommunikationsministeriet

Propositionen har beretts vid kommunikationsministeriet. Vid beredningen har man tagit hjälp av den sakkunskap som finns hos arbetsgruppen för utvecklande av elektronisk identifiering, som lyder under delegationen för vardagens informationssamhälle. Under beredningsarbetet har det förts förberedande diskussioner med företrädare för bland annat Europeiska gemenskapernas kommission, justitieministeriet, inrikesministeriet, arbets- och näringsministeriet, Kommunikationsverket, Finansinspektionen, Konsumentverket, Befolkningsregistercentralen, Finanssialan Keskusliitto - Finansbranschens Centralförbund ry, Tietoliikenteen ja tietotekniikan

keskusliitto, FiCom ry och enskilda aktörer såsom banker och teleoperatörer.

Remissyttranden och hur de har beaktats

Utkastet till lag sändes på en omfattande remissbehandling i november 2008. Utlåtande gavs av justitieministeriet, undervisningsministeriet, försvarsministeriet, inrikesministeriet, social- och hälsovårdsministeriet, arbets- och näringsministeriet, finansministeriet, Försörjningsberedskapscentralen, Centralkriminalpolisen, Konkurrensverket, Konsumentverket, Huvudstaben, Finansinspektionen, Skyddspolisen, Statskontoret, Statens revisionsverk, Skattestyrelsen, Kommunikationsverket, Befolkningsregistercentralen, CSC – Tieteen tietotekniikan keskus Oy, Finlands näringsliv rf, Elisa Abp, Pensionsskyddscentralen, F-Secure Oyj, Finanssialan Keskusliitto - Finansbranschens Centralförbund ry, Helsingin seudun kauppakamari - Helsingforsregionens handelskammare ry, IKI ry, Folkpensionsanstalten, Kesko Abp, Centralhandelskammaren, Logica Suomi Oy, Nordea Bank Finland Abp, OP-Centralen anl, Oy Samlink Ab, Sampo Bank Abp, Stakes, Tjänstemannacentralorganisationen FTFC rf, Finlands Fackförbunds Centralorganisation FFC rf, Suomen Asiakkuusmarkkinointiliitto ry, Finlands Konsumentförbund rf, Finlands Kommunförbund rf, Företagarna i Finland rf, Tammerfors stad, Tampereen yliopisto, TeliaSonera Finland Oyj, Rättsskyddscentralen för hälsovården, TIEKE Utvecklingscentralen för Informationssamhälle rf, Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry, Tietotekniikan liitto ry, Forskningsinstitutet för informationsteknologi HIIT, Valimo Wireless Oy, Ubisecure Solutions Ab och Mediernas Centralförbund rf.

Eftersom det inte finns någon motsvarighet till denna lag i Europa, och veterligen inte heller någon annanstans i världen, arrangerades remissbehandlingen i ett ganska tidigt skede, så att man skulle få respons om de grundläggande lösningarna i lagen innan man började finslipa detaljerna i regeringspropositionen. Några remissgivare fäste också uppmärksamhet vid att utkastet var halvfärdigt.

I det stora hela fick utkastet till lag ett relativt positivt mottagande. Det kom in 53 egentliga utlåtanden. Det meddelades inte i ett enda av dem att man motsatte sig att lagen utfärdades. Av remissinstanserna var det 35 som sade att de utan vidare stöder lagförslaget och dess målsättningar eller att de uppskattar verkningarna vara positiva.

I ungefär vart tredje utlåtande framfördes synpunkter av enbart allmän natur, i ungefär vart tredje föreslogs det några ändringar eller preciseringar i propositionen och i ungefär vart tredje fanns det en stor mängd ändringsförslag.

Anmärkningarna i utlåtandena hade stor variation. Endast några punkter berördes av flera än en anmärkning. Med stöd av den respons som kom in har lagförslagets grundläggande lösningar behållits. Nedan beskrivs de viktigaste ändringarna som gjorts till följd av utlåtandena. En betydande mängd ändringar och preciseringar av mindre betydelse gjordes också.

De viktigaste ändringarna på basis av utlåtandena gjordes i lagförslagets 1 och 2 kap. Begränsningen av tillämpningsområdet i 1 §, enligt vilken slutna system inte omfattas av tillämpningsområdet, är en direkt följd av att man genom lagen strävar efter att skapa förutsättningar för en fungerande marknad för stark autentisering. På denna marknad har endast verktyg som är i allmänt bruk möjlighet att konkurrera med varandra. I slutna system är det främsta målet för tillhandahållandet av tjänsten inte ens själva identifieringen, utan identifieringen tjänar andra syften. Till paragrafens andra moment fogades dock med tanke på konsumentskyddet en bestämmelse som gör gällande att man även i vissa slutna system bör iaktta vissa bestämmelser i den föreslagna lagen som gäller tjänsteleverantörens ansvar. Efterlevnaden av dessa bestämmelser övervakas inte av Kommunikationsverket, utan av konsumentombudsmannen.

När det gäller definitionerna fäste man i vissa utlåtanden bland annat uppmärksamhet vid att de tre villkor som även i internationellt perspektiv allmänt har ansetts som definition av stark autentisering inte nämndes i paragraftexten i definitionen av stark autentisering i 2 § 1 punkten. Dessa villkor i motiveringstexten togs med i paragraftexten.

Till 3 § fogades en bestämmelse om bestämmelsernas tvingande natur när det gäller kundförhållanden.

I vissa utlåtanden ansågs det att lagförslaget inte skulle ha utvidgat bestämmelserna i lagen om elektroniska signaturer när det gäller vilka signaturer som kan ges rättslig verkan. Med anledning av utlåtandena flyttades paragraferna som gällde rättslig verkan från 3 och 4 kap. till 2 kap. och slogs samtidigt ihop. Trots att lagen om elektroniska signaturer inte har begränsat rättsverkningarna i fråga om kvalificerade certifikat, har lagen tolkats så på många håll ända fram till den senaste tiden. För att skapa klarhet i detta fogades det till 5 § 2 mom. en mening som gäller elektroniska signaturer och som följer artikel 5.2 i gemenskapsdirektivet. Där konstateras det att elektroniska signaturer inte ska förvägras rättslig verkan enbart på den grunden att de har skapats genom någon annan metod för elektronisk signering än genom en avancerad elektronisk signatur som baserar sig på ett kvalificerat certifikat och som har skapats med en säker anordning för signaturframställning.

Begränsningarna av tillämpningsområdet som finns i 1 § 2 mom. om tillämpningsområdet begränsar inte tillämningsområdet för sådana paragrafer som gäller stark autentisering och elektroniska signaturer i allmänhet. Begränsningarna av tillämpningsområdet gäller tillhandahållande av tjänster och verksamhet som endast gäller tillverkning, import eller försäljning av verktyg för stark autentisering eller för elektroniska signaturer. De föreslagna 4 och 5 § gäller inte enbart tillhandahållande av tjänster, utan stark autentisering och elektroniska signaturer i allmänhet. Aktörerna kan själva bedöma vilken typ av stark autentisering och elektroniska signaturer de ger rättslig verkan, om inte denna prövningsmöjlighet begränsas av andra bestämmelser i lag.

Till 4 § 1 mom. fogades en bestämmelse som fastställer att elektroniska signaturer och avancerade elektroniska signaturer kan skapas med verktyg för stark autentisering på det sätt som verktygens egenskaper tillåter, om parterna så önskar och om något annat inte föreskrivs på något annat ställe i lag. I syfte att skapa klarhet fogades till 2 mom. i samma paragraf en bestämmelse om att elektroniska signaturer får tillhandahållas som en del av tjänster för stark autentisering, varvid 3 kap. tillämpas på tjänsten i sin helhet, om det inte är fråga om en certifikatutfärdare som tillhandahåller kvalificerade certifikat. Samtidigt slopades i 4 kap. en bestämmelse i remissversionens 23 § om att bestämmelserna i remissversionens 2 kap. skulle gälla i tillämpliga delar för vissa typer av tjänster för elektroniska signaturer.

Den förteckning som Kommunikationsverket enligt remissversionen skulle föra över tjänsteleverantörer som gjort anmälan ändrades i enlighet med lagens 12 § till ett register. Samtidigt ålades Kommunikationsverket en skyldighet att förbjuda en tjänsteleverantör att tillhandahålla sina tjänster som stark autentisering, om tjänsterna eller tjänsteleverantören inte uppfyller kraven i 2 kap. Av bestämmelsen framgår det samtidigt att Kommunikationsverket ska kontrollera tjänsteleverantörerna och deras verksamhet på basis av de anmälningar som gjorts, innan en registeranteckning görs. Detta medför givetvis betydligt mera arbete för Kommunikationsverket än modellen i remissversionen. Av denna anledning ändrades samtidigt den paragraf som gäller avgifter som ska betalas till Kommunikationsverket så att en separat avgift ska betalas för registrering.

Till 3 kap. fogades en helt ny paragraf om förnyande av verktyg för stark autentisering. Villkoren för dem som tillhandahåller tjänster för stark autentisering fick utgöra en egen paragraf. Många av de bestämmelser i 3 kap. som tryggar ställningen för innehavare av verktyg för stark autentisering preciserades och utvidgades.

Flest meningsskiljaktigheter torde ha uppstått på grund av paragrafen om inledande identifiering, övergångsbestämmelsen och bestämmelserna om tjänsteleverantörernas ansvar. De centrala aktörerna inom branschen har meddelat tämligen enhälligt att de vill behålla de grundläggande lösningar som finns i remissversionen och att de anser att dessa lösningar är mycket viktiga för man ska uppnå lagens målsättning. Av denna anledning har paragraferna i fråga endast preciserats.

6 Samband med andra propositioner

Regeringens proposition med förslag till lag om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (RP 98/2008 rd) är för närvarande under behandling i riksdagen. Genom den föreslagna lagen upphävs befolkningsdatalagen (507/1993) som trädde i kraft 1993. Den föreslagna lagen syftar till att styra uppdateringen och nyttjandet av uppgifterna i befolkningsdatasystemet och uppgifterna och tjänsterna inom Befolkningsregistercentralens certifierade elektroniska kommunikation samt utvecklingen av systemet och servicen.

Det finns några synnerligen viktiga beröringspunkter mellan den ovan nämnda propositionen och det aktuella lagförslaget. Hit hör i synnerhet de nya bestämmelserna om utlämnande av elektroniska kommunikationskoder och om den särskilda regleringen av Befolkningsregistercentralens certifikatverksamhet.

Lagförslaget om befolkningsdatasystemet innehåller detaljerade lagbestämmelser om personbeteckningars och elektroniska kommunikationskoders innehåll samt om hur de tilldelas, rättas, ändras och får lämnas ut. Permanenta beteckningar och koder är huvudregel också i den föreslagna lagen, men det föreslås bli bestämt att uppenbara skrivfel och tekniska fel uttryckligen ska kunna rättas och att beteckningen och koden ska kunna ändras av skäl som hänför sig till behov av skydd, förhindrande av missbruk och fastställande av transsexuella personers könstillhörighet.

Propositionen innehåller en reform som gäller utlämnande av sådana elektroniska kommunikationskoder som används vid certifierad elektronisk kommunikation och den utvidgar kodernas användningsområde. Enligt propositionen får en kommunikationskod lämnas ut om den används som en uppgift som identifierar innehavaren av ett certifikat i samband med produktion av tjänster eller prestationer som baserar sig på användningen av medborgarcertifikat. Till denna del motsvarar de föreslagna bestämmelserna dagens bestämmelser. Enligt förslaget får en kommunikationskod dessutom lämnas ut åt andra certifikatutfärdare än Befolkningsregistercentralen som är etablerade i Finland, om de använder den i ett sådant certifikat som avses i lagen om elektroniska signaturer som en uppgift som identifierar innehavaren av certifikatet. Detta är en betydande utvidgning av användningsområdet för koderna och syftet är att stödja och förbättra verksamhetsbetingelserna för elektronisk kommunikationen.

Propositionen innehåller förslag till bestämmelser där Befolkningsregistercentralens samlade tjänster inom certifierad elektronisk kommunikation fastställs i detalj. I propositionen har servicehelheten indelats i två självständiga delar. Den första gäller Befolkningsregistercentralens myndighetsuppgifter, dvs. uppgifter i anslutning till de föreskrivna medborgarcertifikaten och den därtill direkt anslutna uppgiftshelheten. Den andra delen gäller övriga certifikatuppgifter och certifikattjänster som Befolkningsregistercentralen kan tillhandhålla t.ex. som företagsekonomiska tjänster. Med undantag för medborgarcertifikaten medger bestämmelsen inte någon som helst monopolställning för Befolkningsregistercentralen när det gäller produktion av de tjänster och prestationer som nämns där.

Enligt förslaget ska ansökan om medborgarcertifikat alltid göras skriftligen hos polisen, som identifierar sökanden. I förfarandet för ansökan om andra certifikat som Befolkningsregistercentralen producerar kan centralen samarbeta med andra myndigheter och privata företag och organisationer.

DETALJMOTIVERING

1 Motivering av lagförslag

1.1 Lag om stark autentisering och elektroniska signaturer

Terminologin. I terminologin på området används på finska allmänt orden ”tunnistaminen” och ”tunnistus” som parallella termer, och det görs ingen egentlig betydelseskillnad mellan orden. I denna lag används ordet ”tunnistaminen” då det står ensamt eller som efterled i en sammansättning. Ordet ”tunnistus” används som förled i sammansättningar, varvid det bildas sammansatta ord såsom ”tunnistusväline”, ”tunnistuspalvelu” och ”tunnistustapahtuma”. Det finns veterligen inte en risk att dessa ord förväxlas med den terminologi som används inom 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 sammmansättningar med ”stark autentisering”.

1 kap. Allmänna bestämmelser

1 §. *Tillämpningsområde*. I paragrafen föreskrivs om lagens tillämpningsområde och begränsningar av det. I 1 mom. anges tillämpningsområdet och i 2 och 3 mom. undantagen från huvudregeln. I 4 mom. preciseras tillämpningsområdet ytterligare.

Enligt 1 mom. föreskrivs i lagen om stark autentisering och elektroniska signaturer. I lagen föreskrivs också om tillhandahållande av tjänster för stark autentisering och elektroniska signaturer till tjänsteleverantörer som använder tjänsterna och till allmänheten. Bestämmelser om stark autentisering och elektroniska signaturer finns främst i 4, 5 och 28 §. Största delen av bestämmelserna i den föreslagna lagen gäller tillhandahållande av tjänster.

Tjänster tillhandahålls för det första till allmänheten. Samma avgränsning har gjorts i lagen om elektroniska signaturer. Med allmänheten avses ett antal personer som inte har begränsats på förhand. Till allmänheten räknas t.ex. inte en grupp personer som har begränsats på basis av ett anställnings- eller tjänsteförhållande.

För det andra tillhandahålls tjänster till tjänsteleverantörer som använder identifieringstjänster. Ett typfall av tillhandahållande av identifieringstjänster kan anses vara när en tjänsteleverantör använder stark autentisering för att tillhandahålla en annan tjänst och inte själv identifierar den som ska identifieras utan överför identifieringen till någon annan utanför den egna tjänsten. Kännetecknande 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. Till den föreslagna lagens tillämpningsområde hör också olika center för identifiering eller verifiering och andra motsvarande centraliserade system, om de utför identifieringen för kundens räkning.

Elektroniska signaturer grundar sig i princip på en annan rättslig ram än stark autentisering. Vid elektroniska signaturer står den som tillhandahåller signeringstjänster, i allmänhet en certifikatutfärdare, och den som förlitar sig på signaturen inte i ett avtalsförhållande med varandra. Trots det tillhandahåller certifikatutfärdare tjänster till dem som förlitar sig på signaturen t.ex. så att certifikatutfärdarna upprätthåller en spärrlista.

Regleringen om tjänster för elektroniska signaturer gäller främst tillhandahållande av kvalificerade certifikat. Bestämmelser om det finns i 4 kap. I det föreslagna 4 § konstateras dessutom att elektroniska signaturer och avancerade elektroniska signaturer kan skapas med identifieringsverktyg på det sätt som verktygens egenskaper tillåter.

I 2-4 mom. preciseras lagens tillämpningsområde genom att vissa situationer lämnas utanför tillämpningsområdet. För det första tillämpas lagen inte på användning av stark autentisering eller tillhandahållande av tjänster för elektroniska signaturer som endast sker internt inom en sammanslutning. Det är fråga om tillhandahållande av tjänster för

stark autentisering, men tjänsterna tillhandahålls inte till allmänheten eller andra tjänsteleverantörer. En och samma leverantör av identifieringstjänster kan tillhandahålla samma tjänst till en tjänsteleverantör som använder identifieringstjänster för att identifiera en grupp personer som inte har bestämts på förhand och till en sammanslutning för att användas för sammanslutningens interna behov. Den förstnämnda situationen omfattas av lagens tillämpningsområde, medan den sistnämnda inte gör det.

De begränsningar av tillämpningsområdet som nämns i 2 mom. gäller endast tillhandahållande av tjänster. Däremot gäller det som sägs t.ex. i 4 och 5 § stark autentisering och elektroniska signaturer i allmänhet. Bestämmelsen begränsar inte företags och sammanslutningars möjlighet att pröva vilken stark autentisering och vilka elektroniska signaturer ska ges rättslig verkan. Det bör dock noteras att denna prövningsrätt eventuellt begränsas av bestämmelser i andra lagar.

Till lagens tillämpningsområde hör inte heller sådana situationer där en sammanslutning använder en egen metod för stark autentisering uteslutande för att identifiera sina egna kunder i de egna tjänsterna. I en sådan verksamhet är det egentligen inte alls fråga om att tillhandahålla tjänster för stark autentisering utan tjänsteleverantörens syfte är att tillhandahålla en annan egen tjänst och identifieringen är endast en biprodukt av tjänsten. Det är inte särskilt sannolikt att dessa metoder för stark autentisering, som används för ett visst slutet ändamål, kommer att bli mycket vanligare.

Det föreslagna tillämpningsområdet och begränsningarna av det är en direkt följd av att avsikten med lagen är att ge grundläggande regler för en fungerande marknad för verktyg för stark autentisering i allmänt bruk. Verktyg med en på förhand begränsad användarkrets kan inte konkurrera på en öppen marknad som är inriktad på metoder och verktyg för allmänt bruk. De som använder företags och organisationers interna system behöver inte heller på samma sätt skydd som de som skaffar sina verktyg själv på marknaden och som ofta agerar i egenskap av konsument. Behovet av skydd är också mindre i fråga om identifieringsverktyg som används för ett visst slutet ändamål, eftersom en sådan användning självfallet innebär mindre risker.

Dessutom bör det beaktas att den föreslagna lagen är det första som syftar till att reglera tillhandahållandet av tjänster för elektronisk identifiering i vårt land. Tillhandahållandet av dessa tjänster är i ett kraftigt utvecklingsskede och det är möjligt att den tekniska utvecklingen också medför nya identifieringsmetoder under de kommande åren. Därför är det ytterst viktigt att de föreslagna bestämmelserna ger utrymme för nya arrangemang som utvecklas. Nya metoder kan t.ex. testas i slutna miljöer innan de erbjuds som verktyg för allmänt bruk på den öppna marknaden. Fenomen som verkar behöva regleras kan införas i regleringen i ett senare skede. Det är emellertid en betydligt större utmaning att upphäva en reglering som redan gäller. En alltför strikt reglering av en marknad som håller på att skapas kan leda till alltför tunga förpliktelser och därigenom till ett tynande tjänsteutbud.

När en sammanslutning tillämpar en egen metod för stark autentisering för att identifiera sina egna kunder i de egna tjänsterna tillämpas dock bestämmelserna i 3 §, 20 § 1 mom., 21 - 22 §, 23 § 1 mom., 25 § 1 och 2 mom., 27 § 1 mom., 27 § 2 mom. 1 punkten och 27 § 3 mom. Dessa bestämmelser gäller hantering av ansvarsfrågor. Eftersom det i ett sådant tillhandahållande av tjänster inte är fråga om tjänster för stark autentisering omfattas verksamheten inte av Kommunikationsverkets tillsynsbehörighet enligt 42 § 2 mom. Enligt det föreslagna 42 § 4 mom. ska verksamheten övervakas av konsumentombudsmannen. I övrigt har bestämmelsen betydelse närmast när ansvarsfrågor avgörs t.ex. vid domstolar.

Det är klart att om en aktör som inte omfattas av lagens tillämpningsområde frivilligt vill iaktta de kvalitativa bestämmelser i lagen som gäller tjänsteleverantörer och tjänster som tillhandahålls finns det inte några allmänna hinder för det i vår rättsordning. Sådana aktörer kan självfallet inte göra en anmälan enligt 10 § eller registreras enligt 12 §. De omfattas inte heller av tillsynen enligt 5 kap.

Enligt den sista meningen i 4 mom. ska lagen inte heller tillämpas på tillverkning, im-

port och försäljning av verktyg för stark autentisering eller för elektroniska signaturer. Utgivning av verktyg för stark autentisering kan åtskiljas från tillverkning, import och försäljning så att det mellan en utgivare och en innehavare av ett verktyg i regel råder ett avtalsförhållande. I fråga om elektroniska signaturer gör t.ex. den spärrlista som en certifikatutfärdare upprätthåller att verksamheten är tillhandahållande av en tjänst till skillnad från renodlad tillverkning, import eller försäljning.

2 §. *Definitioner*. I 1 punkten definieras stark autentisering. Med stark autentisering avses identifiering av en person och verifiering av identifikatorns autenticitet och riktighet genom tillämpning av en elektronisk metod. Minst två av de tre villkor som nämns i punkten ska uppfyllas samtidigt. Stark autentisering grundar sig på någonting som en innehavare av ett identifieringsverktyg vet, någonting som en innehavare av ett identifieringsverktyg har eller någonting som en innehavare av ett identifieringsverktyg är.

De föreslagna a-c punkterna och kravet på att två av dessa alternativ ska ingå för att en metod för elektronisk identifiering ska kunna betraktas som stark autentisering motsvarar den allmänna internationella definitionen av stark autentisering. I a-punkten avses ett lösenord eller en lösenfras, som användaren måste ge tillsammans med sin användaridentifikation. I b-punkten avses däremot ett identifieringsverktyg som innehåller data som gör det möjligt att fastställa användaridentiteten. Exempel på sådana verktyg är smartkort och mobiltelefoner med ett visst SIM-kort. I c-punkten avses i praktiken någon biometrisk egenskap hos användaren, t.ex. fingeravtryck, ansiktsform eller ögats iris.

Definitionen av stark autentisering innefattar också alltid verifiering, som säkerställer identifikatorns autenticitet och riktighet. Med identifikator avses den data som används för identifieringen.

I 2 punkten definieras identifieringsverktyg. Definitionen syftar till att vara tekniskt neutral och beskriva allt det som i fysisk eller elektronisk form eller i form av data tillsammans bildar ett identifieringsverktyg. Med ett verktyg kan således avses t.ex. 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 3 punkten definieras identifieringsmetod. Med identifieringsmetod avses den helhet som bildas av identifieringsverktyget och det system som behövs för att verifiera en enskild transaktion baserad på stark autentisering. Med system avses särskilt den maskinvara och programvara som behövs. I 8 § föreskrivs om de krav som gäller identifieringsmetoden.

I 4 punkten definieras leverantör av identifieringstjänster. I den föreslagna 9 § anges som krav att en leverantör av identifieringstjänster ska vara tillförlitlig.

I enlighet med definitionen kan tjänster som anknyter till den egentliga identifieringen tillhandahållas och verktyg ges ut antingen av samma eller av olika aktörer. Bestämmelsen ger utrymme för flexibilitet och en eventuell särutveckling i framtiden. Samtidigt gör den det möjligt att även tillhandahålla stark autentisering utan att avtalsförhållande mellan tjänsteleverantörerna. I Finland bedrivs denna typ av verksamhet av Befolkningsregistercentralen. På motsvarande sätt som i 1 § 1 mom. avses med allmänheten en grupp personer som inte har bestämts på förhand.

En tjänsteleverantör får använda en metod för stark autentisering för att identifiera sina egna kunder och tillhandahålla samma metod till andra, dvs. till tjänsteleverantörer som använder stark autentisering. Den förstnämnda situationen omfattas inte av lagens tillämpningsområde, medan den sistnämnda gör det. En sådan situation är t.ex. när bankerna använder sina identifieringskoder för sina egna kunders bankärenden och tillhandahåller samma koder för att användas för stark autentisering i andra tjänster.

En leverantör av identifieringstjänster kan i princip vara en fysisk eller juridisk person. I praktiken kommer sannolikt bl.a. det krav på tillräckliga ekonomiska resurser som nämns i 13 § att leda till att fysiska personer inte kommer att vara verksamma som tjänsteleverantörer.

I 5 punkten definieras innehavare av identifieringsverktyg. Med innehavare avses i denna lag alltid en person som innehar ett verktyg för stark autentisering med stöd av laglig rätt. Om den berättigade innehavaren förlorar verktyget, kan t.ex. den som hittar det inte bli en sådan innehavare av ett verktyg som avses i definitionen. Eftersom ett verktyg ska vara personligt enligt 20 § 3 mom., är innehavaren också alltid samma person som verktyget har tillhandahållits till. I det föreslagna 23 § 2 mom. anges det tydligt att innehavaren av ett verktyg för stark autentisering inte får överlåta verktyget för att användas av någon annan.

Med den inledande identifiering som definieras i 6 punkten avses verifiering av identiteten hos den som ansöker om ett identifieringsverktyg i samband med att verktyget ges ut. Den inledande identifieringen är kanske den viktigaste grundläggande förutsättningen för tillförlitlighet i stark autentisering. Bestämmelser om det finns i 17 §. Inledande identifiering är en term som har skapats med tanke på den föreslagna lagen. Man har velat införa en term som tydligt skiljer denna särskilda identifiering från de senare identifieringstransaktioner som upprepas flera gånger. I regel behöver en leverantör av identifieringstjänster utföra en inledande identifiering av en innehavare av ett identifieringsverktyg endast en gång.

I 7 punkten definieras certifikat. Med certifikat avses ett intyg i elektronisk form som verifierar identiteten eller verifierar identiteten och kopplar ihop signaturverifieringsdata med en undertecknare. Certifikat kan användas både i identifieringstjänster och i tjänster för elektroniska signaturer. Ett certifikat är ett intyg som en tredje part har undertecknat elektroniskt och som anger att en viss öppen nyckel hör till en viss användare av nyckeln. Utöver en öppen nyckel innehåller ett certifikat även andra uppgifter, såsom personens eller organisationens namn, den dag certifikatet utfärdats, sista giltighetsdag eller ett unikt serinummer.

En certifikatutfärdare är enligt 8 punkten en fysisk eller juridisk person som tillhandahåller certifikat. På samma sätt som i fråga om leverantörer av identifieringstjänster är det inte troligt att fysiska personer i verkligheten kan bedriva verksamhet som certifikatutfärdare. Den föreslagna punkten motsvarar 2 § 8 punkten i den gällande lagen om elektroniska signaturer, förutom att ordet allmänheten har fogats till punkten så att ordet inte behöver upprepas i de andra paragraferna. Termen används endast i samband med elektroniska signaturer även om certifikat också kan användas vid stark autentisering. Då omfattas dock certifikatutfärdare av den tekniskt neutrala termen leverantör av identifieringstjänster.

Enligt 9 punkten avses med elektronisk signatur data i elektronisk form som är fogade till eller logiskt knutna till andra elektroniska data och som används som en metod för verifiering av undertecknarens identitet. Punkten motsvarar 2 § 1 punkten i lagen om elektroniska signaturer.

En elektronisk signatur 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 signatur är ett vitt begrepp. Syftet med enkla elektroniska signaturer är att identifiera den person som signerar och att verifiera uppgifter. Det kan röra sig om något så enkelt som att underteckna ett e-postmeddelande med en persons namn.

Definitionen grundar sig på EU:s direktiv om ett gemenskapsramverk för elektroniska signaturer och motsvarar den allmänna internationella definitionen av elektroniska signaturer. Definitionen innefattar alltid även verifiering av identiteten.

I 10 punkten definieras avancerad elektronisk signatur. Definitionen motsvarar 2 § 2 punkten i den gällande lagen om elektroniska signaturer. En avancerad elektronisk signatur ska enligt a-underpunkten vara knuten uteslutande till undertecknaren. Detta kan säkerställas genom att endast undertecknaren har tillgång till de signaturframställningsdata som behövs för att framställa en elektronisk signatur. Signaturframställningsdata definieras i den föreslagna 11 punkten.

En avancerad elektronisk signatur ska enligt b-underpunkten göra det möjligt att identifiera undertecknaren. Certifikatutfärdaren kan därmed inte utfärda identiska certifikat till två olika personer. De personer till vilka certifikat utfärdats ska kunna skiljas från var-

andra genom särskilda kännetecken eller åtminstone genom certifikatens serienummer.

De medel med vilka en avancerad elektronisk signatur är skapad ska enligt c-underpunkten vara sådana att endast undertecknaren kontrollerar dem. Ett sådant medel för kontroll kan vara t.ex. en PIN-kod med vars hjälp endast undertecknaren har tillgång till signaturframställningsdata, såsom den privata nyckeln.

Enligt den sista underpunkten ska en avancerad elektronisk signatur vara knuten till de data som ska signeras på ett sådant sätt att eventuella förvanskningar av dessa data kan upptäckas. Signaturen ska därmed senare kunna bekräfta integriteten hos de undertecknade data. Kondensatet av det meddelande som ingår i den elektroniska signaturen kan i det öppna nyckelsystemet jämföras med det kondensat som följer med meddelandet, vilket gör det möjligt för mottagaren att kontrollera att meddelandet inte förvanskats.

Enligt 11 punkten avses med signaturframställningsdata unika data, såsom koder eller privata nycklar, som undertecknaren använder för att skapa en elektronisk signatur. Definitionen motsvarar 2 § 4 punkten i lagen om elektroniska signaturer.

Det är fråga om sådana unika data med hjälp av vilka en elektronisk signatur kan skapas. Inom det öppna nyckelsystemet är signaturframställningsdata undertecknarens privata nyckel, som består av en unik sifferserie. När nyckeln används tillsammans med en viss algoritm för kryptering av kondensatet av meddelandet, åstadkoms en särskild kod som kan dekrypteras endast med hjälp av den öppna nyckel som svarar mot den privata nyckeln.

Enligt 12 punkten avses med anordning för signaturframställning programvara eller maskinvara som används som hjälpmedel tillsammans med signaturframställningsdata för att skapa en elektronisk signatur. Definitionen motsvarar 2 § 5 punkten i lagen om elektroniska signaturer.

Inom det öppna nyckelsystemet kan en anordning för signaturframställning innehålla t.ex. en algoritm för beräkning av kondensatet, en annan algoritm för kryptering av kondensatet samt undertecknarens privata nyckel. Dessutom innehåller anordningen för signaturframställning särskild programvara för skapande av den elektroniska signaturen.

I 13 punkten definieras signaturverifieringsdata. Med signaturverifieringsdata avses data, såsom koder eller öppna nycklar, som används för att verifiera en elektronisk signatur. Det är således fråga om data som används av mottagaren för att verifiera en elektronisk signatur som mottagits. Inom det öppna nyckelsystemet är dessa data den s.k. öppna nyckeln. Den föreslagna definitionen motsvarar 2 § 6 punkten i lagen om elektroniska signaturer.

2 kap. Rättsverkningar och behandling av personuppgifter

3 §. *Bestämmelsernas tvingande natur.* I paragrafen föreskrivs att en leverantör av identifieringstjänster och en konsument i egenskap av innehavare av ett identifieringsverktyg inte kan ingå avtal som avviker från bestämmelserna i lagen, om det inte i lag uttryckligen föreskrivs något annat. Enligt paragrafen är ett sådant avtalsvillkor utan verkan. Att ett avtalsvillkor är ogiltigt innebär att villkoret i förhållandet mellan parterna inte har någon effekt. Domstolarna och konsumentklagonämden ska beakta ett villkors ogiltighet å tjänstens vägnar. Bestämmelsen hindrar inte att parterna ingår ett avtal som avviker från lagen, om avtalet är till fördel för innehavaren av identifieringsverktyget.

Bestämmelsens tvingande natur gäller endast konsumenterna. Bestämmelsen motsvarar dock lagens utgångspunkt att andra aktörer, i synnerhet när de bildar ett förtroendenät, ska kunna lita på att alla leverantörer av identifieringstjänster iakttar bestämmelserna i denna lag och särskilt bestämmelserna i 3 kap. och ser dem som en sorts minimireglering för sin verksamhet.

4 §. *Elektroniska signaturer som skapas med identifieringsverktyg.* I paragrafen konstateras det rättsläge som de facto råder, dvs. att elektroniska signaturer och avancerade elektroniska signaturer också kan skapas med metoder och verktyg för stark autentisering på det sätt som deras egenskaper tillåter. Det föreslagna momentet är av konstaterande karaktär och ändrar inte det rådande rättsläget. Situationen blir dock mycket tydligare ge-

nom att saken nämns i det föreslagna momentet. Bestämmelsen utesluter inte heller en sådan möjlighet att elektroniska signaturer eventuellt också kan skapas med vissa verktyg för svag autentisering. Paragrafen gäller dock endast verktyg för stark autentisering, eftersom verktyg för svag autentisering inte omfattas av lagens tillämpningsområde.

I sin enklaste form kan en elektronisk signatur vara t.ex. en persons namn som skrivits i slutet av ett e-postmeddelande. Med certifikat som bygger på en teknik med öppen nyckel kan man däremot skapa avancerade elektroniska signaturer. Alla verktyg för stark autentisering är inte nödvändigtvis sådana att det kan anses vara elektroniska signaturer som skapas med hjälp av dem. Såsom det konstateras i 5 § hindrar detta i och för sig inte att identifieringsverktyg används vid utförandet av rättshandlingar. Möjligheten att skapa elektroniska signaturer beror inte bara på tekniska och andra egenskaper hos ett identifieringsverktyg utan eventuellt också på annan lagstiftning och parternas vilja. Bestämmelser om parternas vilja att förhindra eller begränsa användningen av identifieringsverktyg för att utföra rättshandlingar finns i 18 §.

Möjligheten att framställa signaturer kan också vara en separat egenskap som hör till identifieringsverktyget. I identifieringsverktyget kan det t.ex. placeras signeringsnycklar som är avsedda speciellt för signering.

5 §. *Rättshandlingar.* I 1 mom. konstateras det att möjligheten att skapa elektroniska signaturer i regel inte påverkar möjligheten att utföra en rättshandling med verktyg för stark autentisering, om parterna så önskar. Detta är en följd av att krav på underskrift inte är ett formkrav för största delen av de rättshandlingar som utförs i Finland. Genom den föreslagna bestämmelsen stärks det faktiskt rådande rättsläget. I praktiken har det redan länge varit möjligt att utföra rättshandlingar t.ex. med hjälp av bankkoder.

Momentet är således inte av lagstiftande karaktär utan konstaterande. Verkningarna av en rättshandling är inte direkt bundna till själva identifieringen, utan utförandet av rättshandlingar med hjälp av verktyg för stark autentisering är en egenskap som kan kopplas till användningen av ett identifieringsverktyg. Det som är av vikt är parternas visioner. Ingen part, dvs. leverantörer av identifieringstjänster, tjänsteleverantörer som använder dessa tjänster eller innehavare av identifieringsverktyg, kan generellt eller i ett enskilt fall tvingas att utföra en rättshandling med ett identifieringsverktyg, men de som vill ha ett sådant alternativ ska ges en möjlighet att få det. Möjligheten att utföra rättshandlingar ökar säkert intresset för att tillhandahålla och skaffa verktyg för stark autentisering. Tjänsteleverantören ska se till att användaren faktiskt känner till alla omständigheter i samband med utförande av rättshandlingar.

Bestämmelsen hindrar inte att rättshandlingar eventuellt också kan utföras med sådana identifieringsverktyg som inte uppfyller kraven i denna lag, om parterna så önskar. Förslaget gäller endast verktyg för stark autentisering, eftersom svag autentisering inte omfattas av lagens tillämpningsområde. Det finns inga allmänna bestämmelser om när stark autentisering är nödvändig. Typiska användningssituationer kunde vara e-tjänster som förutsätter i synnerhet ekonomiska eller juridiska förbindelser eller behandling av konfidentiella uppgifter, t.ex. känsliga personuppgifter enligt personuppgiftslagen eller sekretessbelagda uppgifter inom organisationer. I framtiden kommer man eventuellt att uppställa krav på stark autentisering för vissa tjänster om vilka det föreskrivs särskilt i lag.

I den föreslagna bestämmelsen avses sådana rättshandlingar som inte omfattas av några särskilda formkrav någon annanstans i lagstiftningen. I lag eller andra normer kan man separat bestämma om olika formkrav, men sådana bestämmelser är inte särskilt vanliga i vårt rättssystem. När det gäller privaträttsliga avtal är de vanligaste formkraven i lagstiftningen närmast kraven på att avtal ska ingås skriftligen och att de ska undertecknas. Uttrycken "skriftligen" och "underteckna" har inte definierats närmare i lagstiftningen. Även myndigheter kan i allmänhet kontaktas utan formaliteter.

I 2 mom. föreskrivs om elektroniska signaturers rättsverkan. I den första meningen i momentet konstateras det att om det beträffande en rättshandling i lag ställs krav på underskrift, uppfylls detta krav åtminstone ge-

nom en sådan avancerad elektronisk signatur som baserar sig på ett kvalificerat certifikat och har skapats med en säker anordning för signaturframställning. Bestämmelsen motsvarar bestämmelsen i 18 § i lagen om elektroniska signaturer, som syftar till att genomföra artikel 5.2. i direktivet om ett gemenskapsramverk för elektroniska signaturer. I artikeln föreskrivs att en elektronisk signatur inte kan förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att signaturen är i elektronisk form, inte är baserad på ett kvalificerat certifikat, eller inte är skapad av en säker anordning för skapande av signaturer.

I Finland har dock tolkningen av 18 § i lagen om elektroniska signaturer visat sig vara problematisk på det sättet att i flera sammanhang har endast kvalificerade certifikat ansetts duga för att skapa elektroniska signaturer. I syfte att göra situationen klarare föreslås därför att en mening som hämtats från artikel 5.2. i direktivet fogas till momentet. I meningen konstateras det att elektroniska signaturer inte ska förvägras rättslig verkan enbart på den grunden att de har skapats genom någon annan metod för elektronisk signering än genom en avancerad elektronisk signatur som baserar sig på ett kvalificerat certifikat och har skapats med en säker anordning för signaturframställning.

Såsom det redan konstaterades i samband med 1 mom. har det i allmänhet inte uppställts några särskilda formkrav på rättshandlingar i Finland. Vilken elektronisk signatur som helst kan naturligtvis bestridas på samma sätt som en traditionell handskriven namnteckning. Vid finländska domstolar tillämpas fri bevisprövning.

Användningen av elektroniska signaturer förutsätter naturligtvis att det är tillåtet och möjligt att utföra en rättshandling elektroniskt. Den föreslagna bestämmelsen har inte någon betydelse t.ex. för när en rättshandling ska utföras på något annat sätt än elektroniskt.

I 3 mom. konstateras det att i fråga om användningen av elektroniska signaturer inom förvaltningen föreskrivs särskilt. Bestämmelsen motsvarar 3 § 2 mom. i lagen om elektroniska signaturer. Med stöd av 9 § i lagen om elektronisk kommunikation i myndigheternas verksamhet uppfyller också elektroniska dokument som sänts till en myndighet kravet på skriftlig form när ärenden anhängiggörs och behandlas. 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 18 § i lagen om elektroniska signaturer. Ett elektroniskt dokument som inkommit 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. Enligt lagens 16 § kan en beslutshandling signeras elektroniskt. En myndighets elektroniska signatur ska uppfylla kraven i 18 § lagen om elektroniska signaturer. I propositionen ingår också förslag till ändring av lagen om elektronisk kommunikation i myndigheternas verksamhet, där hänvisningarna till lagen om elektroniska signaturer har ändrats till hänvisningar till denna lag.

6 §. *Behandling av personuppgifter.* I den föreslagna 6 § föreskrivs om behandling av personuppgifter i samband med tillhandahållande av tjänster för såväl stark autentisering som för elektroniska signaturer som är baserade på certifikat. Bestämmelsen gäller alla certifikatutfärdare som tillhandahåller elektroniska signaturer, dvs. även andra än de som tillhandahåller kvalificerade certifikat. Om elektroniska signaturer tillhandahålls som en del av en identifieringstjänst, är det terminologiskt sett fråga om en leverantör av identifieringstjänster. Genom bestämmelsen genomförs till de delar som gäller elektroniska signaturer artikel 8.1 och 8.2 i direktivet om ett gemenskapsramverk för elektroniska signaturer.

I 1 mom. föreskrivs om syftet och grunderna för behandling av personuppgifter. Leverantörer av identifieringstjänster får behandla personuppgifter som behövs vid utgivningen av identifieringsverktyg och upprätthållandet av tjänsterna samt vid identifieringstransaktioner. Certifikatutfärdare som tillhandahåller elektroniska signaturer får behandla personuppgifter som behövs vid utfärdandet och upprätthållandet av certifikat. De personuppgifter som får behandlas med stöd av den aktuella bestämmelsen kan variera beroende på

de identifieringsverktyg och metoder som används. I allmänhet är det sannolikt nödvändigt att behandla åtminstone verktygsinnehavarens namn, kontaktuppgifter och identifieringskod. I 19 § finns en särskild bestämmelse om innehållet i de certifikat som används vid stark autentisering och i 30 § föreskrivs om innehållet i kvalificerade certifikat. Det föreslagna momentet uppfyller kraven på ändamålsbundenhet i 7 § i personuppgiftslagen.

Uppgifter får behandlas på de grunder som avses i 8 § 1 mom. 1 och 2 punkten i personuppgiftslagen. Detta innebär att personuppgifter får behandlas endast med den registrerades entydiga samtycke och på uppdrag av den registrerade eller för att fullgöra ett sådant avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås. Leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller elektroniska signaturer får således inte behandla personuppgifter på de grunder som nämns i 8 § 1 mom. 3-9 punkten i personuppgiftslagen. Det sagda hindrar naturligtvis inte att enligt någon annan lag kan en tjänsteleverantör i någon annan egenskap ha rätt att behandla personuppgifter även med stöd av de andra punkterna i 8 § 1 mom. i personuppgiftslagen.

I bestämmelsen avses med behandling detsamma som i 3 § 2 punkten i personuppgiftslagen och således har man i denna proposition använt en övergripande term för behandling som motsvarar regleringen i den nämnda lagen. Med behandling avses all slags behandling av personuppgifter, såsom registrering, lagring och förstörande av uppgifter.

I 3 § 7 punkten i personuppgiftslagen definieras samtycke. Med samtycke avses varje slag av frivillig, särskild och på information baserad viljeyttring genom vilken den registrerade godtar behandling av personuppgifter som gäller honom. Samtycket ska vara en informerad viljeyttring från den registrerade. När den registrerade ger sitt samtycke ska han eller hon således vara medveten om vad samtycket innebär. Samtycket ska också alltid vara frivilligt. Om det uppstår en tvist om huruvida samtycke föreligger har den registeransvarige bevisbördan för förekomsten av samtycke. Samtycket gäller tills vidare, om inte något annat framgår av samtycket. Den registrerade har rätt att när som helst återta sitt samtycke. Till samtycket har i vissa paragrafer i personuppgiftslagen i överensstämmelse med personuppgiftsdirektivet fogats uttryck som preciserar vad som avses med samtycke. Det är bl.a. i 8 § 1 mom. 1 punkten som det förutsätts att den registrerade har gett sitt entydiga samtycke. Kravet på entydighet betonar klarheten i den registrerades samtycke.

I 1 mom. föreskrivs att leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller elektroniska signaturer dessutom får inhämta personuppgifter från personen själv. Syftet med insamlingen av uppgifter ska motsvara syftet med behandlingen av uppgifter i övrigt. Leverantörer av identifieringstjänster får behandla personuppgifter som behövs vid utgivningen av identifieringsverktyg och upprätthållandet av tjänsterna samt vid transaktioner baserade på stark autentisering. Certifikatutfärdare som tillhandahåller elektroniska signaturer får behandla personuppgifter som behövs vid utfärdandet och upprätthållandet av certifikat. Såsom det konstateras ovan ges begreppet behandling en vidsträckt tolkning i personuppgiftslagen och inbegriper också insamling av uppgifter. Ett separat tillägg om insamling av uppgifter har dock fogats till det föreslagna momentet av den orsaken att det i artikel 8.2. i direktivet om ett gemenskapsramverk för elektroniska signaturer finns en uttrycklig bestämmelse om saken.

I 2 mom. konstateras det att personuppgifter får behandlas i andra syften än de som nämns i 1 mom. endast på de grunder som avses i 8 § 1 mom. 1 punkten i personuppgiftslagen. Orsaken till att behandlingsgrunderna har begränsats till personens entydiga samtycke är att det sannolikt sällan är möjligt att i ett uppdrag eller avtal ange en tillräckligt exakt begränsning av behandlingen av personuppgifter i andra syften. Även denna bestämmelse har sin grund i artikel 8.2.

Regleringen motsvarar i sak 19 § i lagen om elektroniska signaturer.

I 3 mom. föreskrivs om behandling av personbeteckningar. Enligt 13 § 1 mom. i personuppgiftslagen får en personbeteckning

behandlas med den registrerades entydiga samtycke eller när behandlingen regleras i lag. Dessutom får en personbeteckning behandlas, om det är nödvändigt att entydigt individualisera den registrerade för att uppfylla den registrerades eller den registeransvariges rättigheter och skyldigheter.

Det är nödvändigt att behandla personbeteckningar i samband med identifieringstjänster och certifikattjänster för elektroniska signaturer därför att tillhandahållandet av tjänster på ett tillförlitligt sätt uttryckligen förutsätter att det går att särskilja personer på ett säkert sätt. Detta är redan i sig en sådan omständighet enligt 13 § 1 mom. i personuppgiftslagen som berättigar till behandling av personbeteckningar utan en uttrycklig bestämmelse i lag. Man har dock velat ta in tydliga bestämmelser om saken i paragrafen. De behövs särskilt eftersom det i 19 § 2 mom. i lagen om elektroniska signaturer föreskrivs att en personbeteckning inte får tas in i certifikat. Det föreslagna momentet ersätter samtidigt bestämmelsen i lagen om elektroniska signaturer.

När leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller elektroniska signaturer kontrollerar sökandens identitet ska de enligt det föreslagna momentet få kräva att sökanden uppger sin personbeteckning. Leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller elektroniska signaturer får behandla personbeteckningar i sina register i de syften som nämns i 1 mom.

Identifieringsverktyg och certifikat får innehålla personbeteckning enbart om verktygets eller certifikatets innehåll är tillgängligt endast för dem som nödvändigt behöver den för att tillhandahålla tjänsten. Personbeteckningen får dock inte vara tillgänglig i en offentlig katalog. Om tjänsten är sådan att den inte kan tillhandahållas utan en offentlig katalog, måste tjänsteleverantören använda någon annan identifierande kod. Då kan t.ex. en elektronisk kommunikationskod i fortsättningen tas in i certifikatet. I riksdagen behandlas för närvarande ett förslag till lag om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster. Enligt lagens 43 § 2 mom. 2 punkten får elektroniska kommunikationskoder lämnas ut till certifikatutfärdare som är etablerade i Finland och som använder koderna i certifikat som en uppgift som identifierar innehavaren av certifikatet.

Enligt 3 mom. gäller i fråga om behandling av personuppgifter i samband med tjänster för stark autentisering i övrigt vad som föreskrivs i personuppgiftslagen. För tjänsteleverantörer och deras anställda som behandlar personuppgifter räcker det således inte med att känna till bestämmelserna i den föreslagna lagen, utan största delen av de materiella bestämmelserna om behandling av personuppgifter finns i den allmänna lagstiftningen på området, dvs. i personuppgiftslagen. Dessutom gäller även 19, 24, 30, 37, och 38 § i denna lag i viss mån behandling av personuppgifter.

I den föreslagna 15 § föreskrivs om skyldighet för leverantörer av identifieringstjänster att lämna uppgifter innan avtal ingås. I paragrafens 3 mom. anges att bestämmelser om skyldigheten att lämna uppgifter vid behandlingen av personuppgifter finns i personuppgiftslagen.

7 §. *Användning av uppgifter i befolkningsdatasystemet.* Enligt 1 mom. får leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller elektroniska signaturer inhämta och kontrollera personuppgifter om en sökande eller innehavare som har registrerats i befolkningsdataregistret på de grunder som avses i 8 § 1 mom. 1 och 2 punkten i personuppgiftslagen. Detta innebär alltså att personuppgifter får behandlas endast med den registrerades entydiga samtycke och på uppdrag av den registrerade eller för att fullgöra ett sådant avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.

Också syftet med behandlingen ska vara detsamma som i 6 §. Leverantörer av identifieringstjänster får således behandla personuppgifter som behövs vid utgivningen av identifieringsverktyg och upprätthållandet av tjänsterna samt vid transaktioner baserade på stark autentisering. Certifikatutfärdare som tillhandahåller elektroniska signaturer får behandla personuppgifter som behövs vid utfärdandet och upprätthållandet av certifikat.

I 4 kap. i den nya befolkningsdatalagen finns bestämmelser om utlämnande av uppgifter ur befolkningsdatasystemet. Uppgifter får lämnas ut för vissa syften som nämns i kapitlet. I 34 § föreskrivs om utlämnande av uppgifter i andra syften än de som särskilt anges i befolkningsdatalagen. I 1 mom. föreskrivs om vissa situationer där uppgifter får lämnas ut. I 2 mom. konstateras det att i övrigt får uppgifter i befolkningsdatasystemet lämnas ut endast om sökanden har rätt att behandla dem med stöd av personuppgiftslagen eller någon annan lag. Den föreslagna bestämmelsen i 1 mom. behövs uttryckligen av denna orsak.

Bestämmelsen följer bestämmelserna i artikel 8.1 och 8.2 i direktivet om ett gemenskapsramverk för elektroniska signaturer.

I paragrafens 2 mom. konstateras det att uppgifterna i befolkningsdatasystemet lämnas ut som en offentligrättslig prestation enligt lagen om grunderna för avgifter till staten (150/1992). I praktiken innebär bestämmelsen självkostnadspris.

Den föreslagna paragrafen motsvarar i sak 20 § i lagen om elektroniska signaturer.

3 kap. Stark autentisering

8 §. Krav som gäller identifieringsmetoden. I paragrafens 1 mom. räknas upp fyra faktorer som utgör en förutsättning för att en identifieringsmetod ska kunna anses vara stark. Förteckningen har uppgjorts på motsvarande sätt som definitionen på avancerad elektronisk signatur i 2 § 10 punkten.

Enligt paragrafens 1 mom. 1 punkt ska identifieringsmetoden grunda sig på en noggrann inledande identifiering, vars uppgifter kan kontrolleras i efterskott. Inledande identifiering definieras i 6 punkten i identifieringsparagrafen och om den föreskrivs i 17 §. Huvudregeln i den föreslagna 17 § är att identifieringen sker personligen på basis av identitetshandlingar som utfärdats av polisen. Dessutom ska leverantören av identifieringstjänster enligt den föreslagna 24 § registrera de uppgifter som behövs om den inledande identifieringen och om den handling som anlitats för identifieringen.

Enligt momentets 2 punkt är ett krav för identifieringsmetoden att man med den kan identifiera innehavaren av identifieringsverktyget entydigt. Med detta avses bland annat att två personer inte kan beviljas likadana identifieringsverktyg. Personer som beviljas identifieringsverktyg ska också särskiljas med personliga unika identifikatorer.

Enligt momentets 3 punkt ska man med metoden med tillräckligt hög tillförlitlighet kunna säkerställa att endast innehavaren av identifieringsverktyget kan använda verktyget. Det kan t.ex. vara fråga om en PIN-kod eller ett biometriskt kännetecken, vars användning helt kontrolleras av verktygets innehavare.

Enligt momentets 4 punkt ska identifieringsmetoden fortsättningsvis vara tillräckligt säker och tillförlitlig med tanke på de informationssäkerhetsrisker som är förknippade med den teknik som används. Om den identifieringsmetod som används t.ex. grundar sig på certifikat, ska tjänsteleverantören se till att den algoritm som används är tillräckligt stark och att nyckelparets längd är tillräcklig.

Av de metoder för stark autentisering som används är bankernas identifieringskoder de klart allmännaste. Dessutom används certifikat som baseras på ett system med öppen nyckel. Sådana har under de senaste åren närmast tillhandahållits av Befolkningsregistercentralen, men i blickfältet finns en möjlighet att teleföretagen börjar erbjuda mobilcertifikat redan år 2009. Dessa identifieringsverktyg torde tillhandahållas ännu en lång tid framöver. Särskilt användningen av certifikat som baseras på ett system med öppen nyckel torde bli allt allmännare i framtiden. Utöver dessa kan identifieringsmetoder som grundar sig på biometrik komma att tas i bruk under de närmaste åren. Däremot utgör till exempel användningen av paret användaridentifikation–lösenord och frågor som grundar sig på födelsedatum, hemadress och motsvarande personuppgifter svag autentisering.

Paragrafens 2 mom. gör det möjligt att tillhandahålla tjänster för elektronisk identifiering anonymt, så att en tjänsteleverantör som använder en identifieringstjänst inte får reda på verktygsinnehavarens faktiska identitet. Denna bestämmelse möjliggör t.ex. tjänster vilkas användning är beroende av personens ålder, men där en egentlig identifiering inte

är nödvändig. Personens faktiska identitet kan dock alltid utredas även i dessa fall, om det av någon anledning senare visar sig vara nödvändigt. Dessa situationer regleras i 24 §.

Med hjälp av 2 mom. genomförs artikel 8.3 i direktivet om ett gemenskapsramverk för elektroniska signaturer. Såsom i 4 § konstateras, kan elektroniska signaturer skapas med verktyg för stark autentisering och erbjudas som en del av identifieringstjänsterna.

Paragrafens 3 mom. innehåller ett bemyndigande som är särskilt nödvändigt av den anledningen att elektronisk identifiering är en mycket teknikbetonad bransch som ständigt utvecklas. Enligt det föreslagna momentet kan Kommunikationsverket utfärda närmare tekniska föreskrifter om uppfyllandet av kraven enligt 1 mom.

9 §. Krav som gäller leverantörer av identifieringstjänster. Enligt paragrafens 1 mom. ska 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 ha uppnått myndighetsålder, inte vara försatta i konkurs och inte ha begränsad handlingsbehörighet. Begränsningar av handlingsbehörigheten kan till exempel vara en följd av omyndighet.

I paragrafens 2 och 3 mom. föreskrivs om tillförlitligheten för en leverantör av identifieringstjänster. Enligt 2 mom. betraktas en leverantör av identifieringstjänster inte som tillförlitlig om en sådan person som avses i 1 mom. genom en lagakraftvunnen dom under de senaste fem åren har dömts till fängelsestraff eller under de senaste tre åren har dömts till böter för ett brott som kan anses visa att personen i fråga är uppenbart olämplig att tillhandahålla tjänster för stark autentisering. En sådan uppenbar olämplighet kan t.ex. vara en följd av tillräckligt allvarliga ekonomiska brott eller medlemskap i en organiserad brottsorganisation.

Enligt 3 mom. betraktas en leverantör av identifieringstjänster inte heller som tillförlitlig, om en sådan person som avses i 1 mom. i övrigt genom sin tidigare verksamhet har visat sig vara uppenbart olämplig som leverantör av identifieringstjänster.

Tecken på uppenbar olämplighet som leverantör av identifieringstjänster som avses i momentet kan till exempel vara en dom för ett sådant brott som avses i 2 mom. som inte vunnit laga kraft. Bestämmelsen kan även tillämpas i det fall att personen i fråga har dömts till fängelse för över fem år sedan eller till böter för över tre år sedan och domen har vunnit laga kraft, om brottet ger vid handen att personen är uppenbart olämplig som leverantör av identifieringstjänster.

Det att en person är uppenbart olämplig att tillhandahålla identifieringstjänster förutsätter inte att han eller hon har dömts till straff för ett brott. Personen kan även ha meddelats näringsförbud enligt lagen om näringsförbud (1059/1985). Näringsförbudet kan till exempel bero på försummelser som gäller skattskyldigheten eller bokföringen. Meddelande av näringsförbud förutsätter inte att det har utdömts ett straff för försummelsen. Om näringsförbudet fortfarande är giltigt kan man naturligtvis inte tillhandahålla identifieringstjänster. Ett näringsförbud som upphört att gälla ska beaktas vid bedömningen av tillförlitligheten.

10 §. Skyldighet för leverantörer av identifieringstjänster att anmäla att verksamheten inleds. Enligt paragrafens 1 mom. ska en leverantör av identifieringstjänster som är etablerad i Finland göra en anmälan till Kommunikationsverket innan verksamheten inleds. Anmälan ska göras skriftligen. Bestämmelsen riktar sig till i Finland etablerade tjänsteleverantörer på grund av de krav som uppställs i EU:s tjänstedirektiv. Tjänstedirektivet utgår från att medlemsstaterna riktar sin lagstiftning uttryckligen på de tjänsteleverantörer som är etablerade inom deras territorium. Artikel 16.2 i direktivet förbjuder bl.a. en medlemsstat att begränsa friheten att tillhandahålla tjänster för en tjänsteleverantör som är etablerad i en annan medlemsstat till exempel genom att ställa krav på inskrivning i ett register på landets territorium. Det är naturligtvis klart att regleringen inte får vara diskriminerande eller hindra den fria rörligheten för tjänster.

I det 37 skälet i tjänstedirektivet behandlas begreppet etablering. Enligt det bör den ort

där en tjänsteleverantör är etablerad fastställas i enlighet med domstolens rättspraxis, enligt vilken begreppet etablering förutsätter ett faktiskt utövande av en ekonomisk verksamhet genom fast etablering för en obegränsad period. Detta krav kan även anses uppfyllt om ett företag bildas för en viss period eller om det hyr den byggnad eller anläggning genom vilken det bedriver sin verksamhet. Etableringen behöver inte ske i form av ett dotterbolag, en filial eller en agentur utan kan bestå av ett kontor som sköts av tjänsteleverantörens egen personal eller av någon fristående person som har stående fullmakt att handla för företagets räkning på samma sätt som skulle vara fallet med en agentur. Definitionen fordrar att tjänsteleverantören faktiskt bedriver ekonomisk verksamhet på etableringsorten, varför enbart en postadress inte utgör en etablering.

I det föreslagna 1 mom. föreskrivs dessutom att anmälan också kan göras av en sådan sammanslutning av tjänsteleverantörer som administrerar en tjänst som ska betraktas som en enda identifieringstjänst. Samarbetsarrangemangen mellan leverantörer av identifieringstjänster i förtroendenät kan i framtiden utgöra egna juridiska personer, varvid ett sådant samarbetsarrangemang ska anses utgöra en egen tjänsteleverantör. I detta fall ska den även göra en anmälan om inledande av verksamheten till Kommunikationsverket. Om detta inte är fallet, utan samarbetsarrangemanget baseras på avtal mellan parterna, ska behövliga uppgifter om samarbetsarrangemanget meddelas till Kommunikationsverket som en del av de principer för identifiering som avses i 14 §. Om utgivningen av identifieringsverktyget och övriga identifieringstjänster (issuing/acquiring) avskiljs till en egen juridisk person och till separata tjänstehelheter, ska de båda tjänsteleverantörerna även göra en anmälan i fråga om dessa.

I framtiden blir tjänsteleverantörer som deltar i olika samarbetsarrangemang tvungna att göra sina egna anmälningar i det fall att var och en av dem administrerar sitt eget identifieringssystem och endast tjänsternas gränssnitt mot användarna är gemensamt.

Om samarbetsarrangemanget mellan tjänsteleverantörerna dock är så fast, att väsentliga delar av tjänsten sköts genom ett gemensamt arrangemang som administreras som en helhet, kan tjänsteleverantörerna även göra en gemensam anmälan. I praktiken kan det vara fråga om en sådan situation när det gäller den bankgrupp som består av Aktiabankerna, sparbankerna och lokalandelsbankerna. Deras identifieringstjänst sköts av Samlink. Om tjänsteleverantörerna i ett sådant fall gör en gemensam anmälan, betalas den registreringsavgift och den tillsynsavgift som avses i den föreslagna 47 § av sammanslutningen.

Anmälan ska enligt det föreslagna 2 mom. innehålla tjänsteleverantörens namn och fullständiga kontaktuppgifter, uppgifter om de tjänster som tillhandahålls, uppgifter om de omständigheter som avses i 8, 9, 13 och 14 § i den föreslagna lagen, och övriga uppgifter som behövs för tillsynen. Med uppgifter om de tjänster som tillhandahålls avses bland annat en redogörelse för det tekniska genomförandet av de tjänster som erbjuds. Om man på marknaden erbjuder till exempel utgivning av ett identifieringsverktyg och en egentlig tjänst som gäller identifieringstransaktioner, eller om det kommer ut sådana samarbetsarrangemang på marknaden som utgör en självständig juridisk person, ska dessa omständigheter framgå ur anmälan. Till uppgifter om tjänster som tillhandahålls hör också uppgifter om det är möjligt att framställa elektroniska signaturer med de identifieringsverktyg som leverantörer av identifieringstjänster har, och hurdana dessa signaturer är.

Det är inte fråga om ett tillstånd för att inleda verksamheten, utan endast om en anmälan. Kommunikationsverket redogör för uppfyllandet av de villkor som fastställs i denna lag innan tjänsteleverantören och de tjänster som erbjuds införs i det register som avses i 12 §. Tjänsteleverantören kan dock börja erbjuda en tjänst redan innan en anteckning har gjorts i registret.

Om inte alla uppgifter som nämns i 1–5 punkten har getts eller om de är bristfälliga, ska Kommunikationsverket uppmana anmälaren att komplettera sin anmälan. Syftet med anmälningsskyldigheten är att tillsynsmyndigheten ska ha klara uppgifter om de tjänsteleverantörer som bedriver verksamhet i Finland.

Enligt det föreslagna 3 mom. ska leverantören av identifieringstjänster utan dröjsmål underrätta Kommunikationsverket om ändringar av de uppgifter som avses i 2 mom. Även denna anmälan ska ske skriftligen. Dessutom ska anmälan göras när verksamheten avslutas eller funktionerna överförs till en annan tjänsteleverantör.

Enligt det föreslagna 4 mom. kan Kommunikationsverket meddela för tillsynen behövliga tekniska föreskrifter om det närmare innehållet i de uppgifter som ska lämnas och om inlämnandet av dem till Kommunikationsverket. De bestämmelser som Kommunikationsverket med stöd av det föreslagna momentet kan utfärda är mycket tekniska till sin natur. Den föreslagna bestämmelsen är nödvändig på grund av att det är fråga om ett tekniskt mycket komplicerat tillhandahållande av tjänster, som dessutom hela tiden utvecklas. Bestämmelserna behövs även i tjänsteleverantörernas intresse, eftersom de annars kan ha svårt att veta till exempel hur noggranna tekniska beskrivningar som krävs av dem. I 9 § 1 mom. i lagen om elektroniska signaturer och i det föreslagna 32 § 1 mom. ingår motsvarande bestämmelser för kvalificerade certifikat.

Kommunikationsverket har den 29 januari 2003 med stöd av den gällande lagen meddelat en föreskrift om skyldighet för certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat att göra anmälan om sin verksamhet till Kommunikationsverket (7/2003 M). Enligt 50 § 2 mom. om lagens ikraftträdande är de föreskrifter som Kommunikationsverket har utfärdat med stöd av lagen om elektroniska signaturer i kraft till dess att nya föreskrifter har utfärdats med stöd av denna lag.

11 §. Leverantör av identifieringstjänster etablerad i en annan medlemsstat inom Europeiska ekonomiska samarbetsområdet. I denna paragraf konstateras att en leverantör av identifieringstjänster som är etablerad annanstans än i Finland om leverantören så önskar får göra en sådan anmälan att verksamheten inleds som avses i 10 §. Denna bestämmelse är nödvändig för att säkerställa den fria rörligheten för tjänster inom Europeiska ekonomiska samarbetsområdet. Enligt artikel 16 i tjänstedirektivet ska medlemsstaterna respektera tjänsteleverantörernas rätt att tillhandahålla tjänster i en annan medlemsstat än den där de är etablerade. Medlemsstaterna får inte heller för att tillåta tillträde till eller utövande av en tjänsteverksamhet på sitt territorium ställa krav som är diskriminerande.

I kapitel VI i tjänstedirektivet föreskrivs om det administrativa samarbetet mellan medlemsstaterna. Enligt artikel 29.1 i detta kapitel ska etableringsstaten när det gäller tjänsteleverantörer som tillhandahåller tjänster i en annan medlemsstat lämna uppgifter om tjänsteleverantörer som är etablerade inom dess territorium, om en annan medlemsstat begär det. Enligt artikel 29.2 ska etableringsmedlemsstaten utföra de kontroller, inspektioner och utredningar som en annan medlemsstat begär och upplysa medlemsstaten i fråga om resultaten och om de åtgärder som eventuellt vidtagits.

12 §. Register över leverantörer av identifieringstjänster. Enligt paragrafens 1 mom. för Kommunikationsverket ett offentligt register över de leverantörer av identifieringstjänster som har gjort en anmälan enligt 10 §. I praktiken är registret lättast att hitta om det finns på Kommunikationsverkets webbsidor. Registret är en av hörnstenarna för det planerade arrangemanget. Både den som skaffar ett identifieringsverktyg, som ofta agerar i egenskap av konsument, och en tjänsteleverantör som skaffar en identifieringstjänst blir tvungna att avgöra vilken leverantör av identifieringstjänster de kan lita på. Ett offentligt register på Kommunikationsverkets webbsidor ger på ett enkelt sätt information om de tjänsteleverantörer som i princip kan förväntas iaktta bestämmelserna i denna lag och som övervakas av myndigheten. Uppgifterna i registret ska emellertid endast vara av informativ karaktär.

I paragrafens 2 mom. föreskrivs om Kommunikationsverkets skyldighet att förbjuda en tjänsteleverantör att tillhandahålla sina tjänster som stark autentisering, om tjänsterna eller tjänsteleverantören inte uppfyller kraven i detta kapitel. Det är Kommunikationsverkets uppgift att kontrollera att tjänsteleverantören och den tjänst som tillhandahålls på basis av uppgifterna i den anmälan som avses i 10 § motsvarar de förutsättningar som uppställs i denna lag, särskilt dess 3 ka-

pitel. Anteckningarna i registret kan göras först efter detta. Det är fråga om det mest arbetskrävande skedet för tillsynsmyndigheten. Av denna anledning ska tjänsteleverantören betala en registreringsavgift enligt 47 § 1 mom. till Kommunikationsverket.

Dessutom konstateras i 2 mom. att Kommunikationsverket kan fastställa en tidsfrist för tjänsteleverantören, inom vilken leverantören ska avhjälpa en bristfällighet som konstaterats i tjänsten eller hos tjänsteleverantören, om bristfälligheten kan anses vara endast ringa. Kommunikationsverket ska i sin verksamhet naturligtvis beakta förvaltningslagen (434/2003). Om det t.ex. är fråga om att anmälan är bristfällig, ska Kommunikationsverket uppmana tjänsteleverantören att komplettera anmälan enligt 22 § 1 mom. i förvaltningslagen.

Det förfarande som fastställs i denna paragraf ska inte anses som ett sådant tillståndsförfarande som avses i tjänstedirektivet, eftersom tjänsteleverantören kan tillhandahålla tjänsten så snart anmälan gjorts, och Kommunikationsverket kan ingripa i detta endast i efterskott. Bestämmelserna hindrar inte heller tjänsteleverantören från att överhuvudtaget tillhandahålla sin tjänst. Om villkoren enligt lagen inte uppfylls får tjänsteleverantören inte tillhandahålla sin tjänst som stark autentisering. Samma bestämmelser gäller enligt 32 § även för tillhandahållande av kvalificerade certifikat.

13 §. Allmänna skyldigheter för leverantörer av identifieringstjänster. I paragrafens 1 mom. föreskrivs om de krav som ställs på de anställda hos en leverantör av identifieringstjänster. Enligt det föreslagna momentet ska leverantören av identifieringstjänster se till att de anställda har tillräcklig sakkunskap, erfarenhet och kompetens med tanke på verksamhetens omfattning. Med sakkunskap avses såväl teknisk som juridisk sakkunskap. Till exempel de krav som den gällande lagstiftningen ställer på behandlingen av personuppgifter är betydande. Kraven på sakkunskap, erfarenhet och kompetens, som t.ex. utbildningskrav, fastställs för varje person enligt de uppgifter som personen i fråga innehar. Den som direkt har att göra med elektronisk identifiering ska till exempel ha tillräcklig sakkunskap om tekniska omständigheter och informationssäkerhet i anknytning till elektronisk identifiering. Det föreslagna momentet motsvarar 10 § 2 mom. 1 punkten i lagen om elektroniska signaturer och 33 § 2 mom. 1 punkten i det föreliggande förslaget.

Enligt 2 mom. ska leverantören av identifieringstjänster ha tillräckliga ekonomiska resurser med tanke på verksamhetens omfattning och för att täcka ett eventuellt ersättningsansvar. Tjänsteleverantören ska bedöma riskerna i anslutning till sin verksamhets tekniska och ekonomiska säkerhet och vidta nödvändiga åtgärder för att minimera riskerna. Tillräckliga ekonomiska resurser förutsätter av tjänsteleverantörens ekonomi, att balansräkningen upptar tillräckliga medel för att täcka riskerna. Tjänsteleverantören kan även uppfylla detta krav genom frivilliga försäkringar. Den första delen av det föreslagna 2 mom. motsvarar 10 § 2 mom. 2 punkten i lagen om elektroniska signaturer och 33 § 2 mom. 2 punkten i det föreliggande förslaget.

Paragrafens 3 mom. innehåller krav på informationssäkerheten för tjänsteleverantörens tjänst och om skyddet av uppgifter enligt 32 § i personuppgiftslagen. Med informationssäkerhet i fråga om tjänsterna enligt det föreslagna momentet avses åtgärder för att trygga säkerheten för verksamheten, datatrafiken, utrustningen och programmen samt för datamaterialet.

Med tjänsternas informationssäkerhet förstås i momentet detsamma som i 19 § 1 mom. i lagen om dataskydd vid elektronisk kommunikation (516/2004). Med säkerheten för verksamheten avses således bland annat att man uppehåller skriftliga anvisningar för hur dataskyddskraven skall uppfyllas, att man regelbundet följer med nivån på sitt eget dataskydd, att man garanterar att dataskyddskraven uppfylls då man använder underleverantörer och att man skyddar utrustningen och filerna mot olovligt intrång och användning. Dessutom avses med säkerhet för verksamheten att man för varje systems del för register över vem som har användarkod till systemet och vilka rättigheter varje användarkod medför, samt att man övervakar händelser som påverkar dataskyddet för uppgifter, dokument, kommunikationsnät, utrust-

ning, tjänster och filer så att för dataskyddet betydelsefulla händelser observeras.

Med säkerhet för datatrafiken avses bland annat att meddelanden och identifieringsuppgifter, som förmedlas genom kommunikationsnäten, inte avslöjas för obehöriga och att dessa inte kommer åt att ändra eller utplåna meddelanden som förmedlas i dessa nät.

Med säkerhet för utrustningen och programmen avses bland annat att man använder sådan utrustning, sådana informationssystem och program som medför endast ringa risker för dataskyddet samt att man ordnar säkerhetskopiering och trygg förvaring för program, som är viktiga för verksamheten.

Med säkerhet för datamaterialet avses bland annat att man ordnar säker behandling av detta material i enlighet med god databehandlingskutym, att man ordnar säkerhetskopiering och trygg förvaring av datamaterialet samt att man skyddar viktiga dokument, datalager och enskilda data.

Dessa åtgärder ska vara tillräckliga, dvs. de ska anpassas till hur allvarliga hot som föreligger samt till den tekniska utvecklingens nivå och till kostnaderna. Med detta avses att fullständig informationssäkerhet och fullständigt dataskydd allmänt taget inte kan uppnås, åtminstone inte utan oskäliga kostnader. Kraven på nivån av informationssäkerhet och skyddet av uppgifter kan variera beroende på de tjänster som tillhandahålls. Om tjänsteleverantören till exempel tillhandahåller tjänster för stark autentisering som baserar sig på biometriska kännetecken är kraven på verksamhetens säkerhet mycket höga. Det kan också finnas skillnader i om tjänsteleverantören tillhandahåller identifieringstjänster för andra tjänsteleverantörer eller om leverantören endast ger ut identifieringsverktyg. I det sistnämnda fallet innehar tjänsteleverantören t.ex. inte några sådana uppgifter som avses i 24 § 1 mom. 1 punkten som bör skyddas.

Enligt 32 § i personuppgiftslagen, som gäller skyddet av uppgifter, ska den registeransvarige genomföra de tekniska och organisatoriska åtgärder som behövs för att skydda personuppgifterna mot obehörig åtkomst och mot förstöring, ändring, utlämnande och översändande som sker av misstag eller i strid med lag eller mot annan olaglig behandling. Vid genomförandet av åtgärderna ska hänsyn tas till de tillgängliga tekniska möjligheterna, kostnaderna som orsakas av åtgärderna, uppgifternas art, mängd och ålder samt vilken betydelse behandlingen av uppgifterna har med avseende på integritetsskyddet.

Enligt det föreslagna 4 mom. svarar tjänsteleverantören för att tjänster och produkter som produceras av personer som tjänsteleverantören anlitar är tillförlitliga och fungerar. Det föreslagna momentet gäller t.ex. underleverantörer. Det är också naturligt att den som tillhandahåller identifieringstjänster inför de tjänsteleverantörer och verktygsinnehavare som använder tjänsterna svarar för sådana verktyg som tjänsteleverantören har skaffat av utomstående leverantörer. Ansvarsfördelningen mellan verktygets tillverkare eller importör och leverantören av en identifieringstjänst baserar sig på avtalsförhållandena mellan dessa. Den föreslagna bestämmelsen överensstämmer med de allmänna rättsprinciperna. Man har dock velat ta med den för tydlighetens skull.

I det föreslagna momentet avses med personer såväl fysiska som juridiska personer. Det föreslagna momentet motsvarar till stor del 10 § 1 mom. i lagen om elektroniska signaturer och 33 § 1 mom. i det föreliggande förslaget.

14 §. Principer för identifiering. I paragrafens 1 mom. förutsätts att leverantören av identifieringstjänster ska ha principer för identifiering som leverantören själv uppställt. I dessa principer definieras närmare hur tjänsteleverantören uppfyller sina skyldigheter enligt denna lag. Det är särskilt viktigt att närmare ange hur tjänsteleverantören utför den inledande identifieringen enligt 17 §.

Enligt paragrafens 2 mom. ska principerna för identifiering beskriva de viktigaste uppgifterna om tjänsteleverantören, de tjänster som tillhandahålls, tjänsteleverantörens viktigaste samarbetsparter och de kontroller som har utförts av utomstående bedömningsorgan samt andra uppgifter som är av betydelse för att tjänsteleverantörens verksamhet och tillförlitlighet ska kunna bedömas.

Principerna för identifiering är ett väsentligt redskap vid bedömningen av tillförlitligheten i fråga om tjänsteleverantören och de

tjänster som leverantören tillhandahåller. Det ligger därför i tjänsteleverantörens eget intresse att utarbeta så täckande principer för identifiering som möjligt. Samtidigt står det dock klart att tjänsteleverantören i sina principer för identifiering inte behöver yppa något som omfattas av affärshemligheten.

Särskilt uppgiften om tjänsteleverantörens samarbetsparter anknyter till marknadens eventuella framtida utvecklingsskede, där tjänsteleverantörerna eventuellt ingår olika öppna samarbetsarrangemang. Det är även skäl att ange uppgifter om underleverantörer, om inte detta är en affärshemlighet.

I 3 mom. förutsätts att principerna för identifiering också ska innehålla uppgifter om elektroniska signaturer, om en leverantör av identifieringstjänster även tillhandahåller elektroniska signaturer i anslutning till sina tjänster för stark autentisering. I detta sammanhang ska ges uppgifter om hur och på vilken nivå de elektroniska signaturerna tillhandahålls samt om säkerhetsfaktorerna i samband med tillhandahållandet. I fråga om hur tillhandahållandet sker är det fråga om det tekniska genomförandet, såsom t.ex. om tjänsten grundar sig på ett certifikat. När det gäller nivån är det närmast fråga om huruvida signaturen ska anses som en avancerad elektronisk signatur. Med hjälp av säkerhetsfaktorerna kan man t.ex. besvara frågan om och till vilka delar metoden för undertecknande kan anses uppfylla förutsättningarna för en säker anordning för signaturframställning.

Enligt 4 mom. ska tjänsteleverantören hålla sina principer för identifiering ständigt uppdaterade. De ska även hållas allmänt tillgängliga. Den föreslagna bestämmelsen grundar sig uttryckligen på tillhandahållande, dvs. tjänsteleverantören har ingen skyldighet att aktivt informera om sina interna bestämmelser. Bestämmelsen om att hålla principerna allmänt tillgängliga kan till exempel uppfyllas med hjälp av Internet på tjänsteleverantörens webbsidor. Frågan om att informera sig om principerna är beroende av den egna aktiviteten.

15 §. Skyldighet för leverantörer av identifieringstjänster att lämna uppgifter innan avtal ingås. I paragrafens 1 mom. föreskrivs om de faktorer som leverantören av identifieringstjänster ska informera sökanden om innan ett avtal ingås med den som ansöker om ett identifieringsverktyg. Uppgifter ska lämnas om leverantören av identifieringstjänster, de tjänster som tillhandahålls och priserna på dem, principerna för identifiering enligt 14 §, frivilliga ackrediteringssystem, parternas rättigheter och skyldigheter, eventuella ansvarsbegränsningar och förfarandena för klagomål och avgörande av tvister. Tjänsteleverantören ska dessutom informera om villkoren för användning av identifieringsverktyget, inbegripet eventuella begränsningar av användningen enligt 18 §.

Uppgifterna om tjänsteleverantören och de tjänster som tillhandahålls ska ges på allmän nivå. I fråga om principerna för identifiering ska uppgift ges om principernas existens och om var de utan besvär kan hittas. Den föreslagna paragrafen förutsätter alltså inte att uppgift ges om vad principerna för identifiering innehåller. Principerna för identifiering innehåller även närmare uppgifter om tjänsteleverantören och de tjänster som tillhandahålls. Enligt den föreslagna paragrafen om lämnande av uppgifter ska dock särskild uppmärksamhet fästas vid att den som ansöker om ett identifieringsverktyg informeras om villkoren för användning av identifieringsverktyget, eventuella ansvarsbegränsningar och eventuella begränsningar för användningen.

Med hänvisningen till parternas rättigheter och skyldigheter avses särskilt 21 § om överlåtelse av identifieringsverktyg till sökande, 23 § om skyldigheter för innehavare av identifieringsverktyg, 25 och 26 § om återkallande eller förhindrande av användning av identifieringsverktyg samt 27 § om innehavarens ansvar för obehörig användning av identifieringsverktyg.

I fråga om myndighetstillsyn och besvärsförfaranden ska uppgifter ges om tillsyn som Kommunikationsverket och dataombudsmannen i överensstämmelse med 5 kap. utövat på leverantören av identifieringstjänster samt om sökandens eller innehavarens rätt att hänskjuta ett ärende som gäller tjänsteleverantörens verksamhet till Kommunikationsverket.

Allmänt taget ingår de omständigheter som avses i det föreslagna momentet i tjänsteleve-

rantörens allmänna avtalsvillkor. Lämnande av uppgifter enligt den föreslagna paragrafen förutsätter dock aktiva åtgärder av tjänsteleverantören. Situationen är således en annan än när det gäller principerna för identifiering i föregående paragraf, eftersom det i fråga om den endast förutsätts att de hålls tillgängliga.

I 12 § 2 mom. i lagen om elektroniska signaturer finns en bestämmelse om informationsskyldighet för certifikatutfärdare som tillhandahåller kvalificerade certifikat. Detta moment omfattar delvis samma uppgifter som det föreslagna momentet. En bestämmelse som motsvarar 12 § 2 mom. i den gällande lagen ingår i 35 § 2 mom.

De uppgifter som avses i 2 mom. ska lämnas skriftligen eller elektroniskt så att den som ansöker om ett identifieringsverktyg kan spara och återge dem i oförändrad form. Om ett avtal på begäran av den som ansöker om ett identifieringsverktyg ingås genom distanskommunikation så att uppgifter och avtalsvillkor inte kan lämnas på det sätt som avses ovan innan avtalet ingås, ska uppgifterna utan dröjsmål lämnas på det nämnda sättet efter det att avtalet har ingåtts. Uppgifterna kan således ges till exempel i form av en pdf-fil som bifogas ett e-postmeddelande. Bestämmelsen motsvarar 6 a kap. 11 § i konsumentskyddslagen (38/1978).

I paragrafens 2 mom. konstateras att bestämmelser om skyldigheten att lämna uppgifter vid behandlingen av personuppgifter finns i personuppgiftslagen. Den bestämmelse som mera specifikt avses är 24 § i personuppgiftslagen. Enligt dess 1 mom. ska den registeransvarige vid insamling av personuppgifter se till att den registrerade kan få uppgift om den registeransvarige och vid behov om dennes företrädare, ändamålet med behandlingen av personuppgifterna samt vart uppgifter i regel lämnas ut, liksom om de uppgifter som behövs för att utöva den registrerades rättigheter vid behandlingen av personuppgifter. Uppgifterna ska ges då personuppgifter samlas in och registreras eller, om uppgifterna samlas in hos någon annan än den registrerade själv och avsikten är att lämna ut uppgifterna, senast då uppgifterna första gången lämnas ut.

I den föreslagna 6 § föreskrivs om behandlingen av personuppgifter. Den skyldighet att lämna uppgifter som avses i denna paragraf ska alltså uppfyllas innan personuppgifter börjar behandlas.

16 §. Skyldighet för leverantörer av identifieringstjänster att anmäla hot och störningar som riktas mot informationssäkerheten eller skyddet av uppgifter. Den skyldighet att anmäla hot och störningar som riktas mot informationssäkerheten eller skyddet av uppgifter gäller för avtalets giltighetstid, i motsats till föregående paragraf, där skyldigheten att lämna uppgifter gäller tiden innan avtal ingås.

Enligt paragrafens 1 mom. förutsätter skyldigheten att lämna uppgifter att leverantören av identifieringstjänster anmäler betydande hot och störningar som riktas mot tjänsternas informationssäkerhet till de tjänsteleverantörer som använder tjänsterna, till innehavarna av identifieringsverktyg och till Kommunikationsverket. Även dataombudsmannen ska enligt 2 mom. underrättas, om hotet eller störningen riktas mot skyddet av uppgifter enligt 32 § i personupppgiftslagen. Enligt 3 mom. ska tjänsteleverantören när anmälan görs samtidigt informera om de åtgärder som de olika aktörerna kan vidta för att avvärja hoten eller störningarna, och om kostnaderna för dessa åtgärder.

Motsvarande bestämmelse, om än mycket mera detaljerad, ingår även i 21 § i lagen om dataskydd vid elektronisk kommunikation. Genom informationen till de tjänsteleverantörer och innehavare av identifieringsverktyg som använder identifieringstjänsten försöker man hindra att skador uppkommer eller att de förvärras. Till exempel i samband med olika bedrägeriförsök kan det vara viktigt att det finns en allmän medvetenhet om pågående bedrägeriförsök. Om det är fråga om det tekniska skyddet av uppgifter, kan innehavarna av verktyg låta bli att använda verktyget tills felet är åtgärdat. Sammantaget är det fråga om att förhindra eller minimera eventuella skadeverkningar.

Bestämmelsen innehåller inga detaljerade anvisningar om hur anmälan ska ske eller till exempel om de sätt på vilka anmälan kan göras. Detta innebär att det är tjänsteleverantörens uppgift att överväga vilken metod som i

varje enskilt fall är den mest effektiva. Beroende på omständigheterna kan anmälan göras t.ex. via Internet eller massmedierna. Ibland kan även personlig kontakt vara det mest effektiva sättet. Bestämmelsen utgår från att det ligger i tjänsteleverantörens intresse att förhindra eller minimera skadeverkningarna.

Bestämmelsen innehåller inte heller något krav på att anmälan ska ske omedelbart, eftersom det ibland kan vara bättre att först försöka avhjälpa exempelvis en brist i skyddet av uppgifter som tjänsteleverantören känner till, men som inte är allmänt känd. Det är alltså upp till leverantören av identifieringstjänster att överväga när anmälan ska ske.

Syftet med anmälan till Kommunikationsverket, och i fråga om personuppgifter till dataombudsmannen, är att tillsynsmyndigheterna är medvetna om de hot och störningar som bestämmelsen avser. Myndigheterna kan bland annat vid behov delta i lämnandet av uppgifter, så att informationen sprids så snabbt som möjligt i de fall då sådan verksamhet kan hindra att skador uppkommer.

17 §. Inledande identifiering av den som ansöker om ett identifieringsverktyg. I den föreslagna paragrafen ingår den kanske viktigaste bestämmelsen i hela den föreslagna lagen. Enligt 1 mom. ska leverantören av identifieringstjänster noggrant identifiera den som ansöker om ett identifieringsverktyg. Antalet handlingar som accepteras vid en inledande identifiering enligt bestämmelsen är begränsat. Identiteten ska fastställas 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. Pass eller identitetskort som har utfärdats av en myndighet i en medlemsstat inom Europeiska ekonomiska samarbetsområdet har tagits med i bestämmelsen, eftersom området har harmoniserade bestämmelser om pass och identitetskort. Om dessa inte godkändes vid den inledande identifieringen, skulle det innebära ett hinder på den inre marknaden. Även med Schweiz och San Marino finns avtal om ömsesidigt erkännande.

Vid den inledande identifieringen får leverantören av identifieringstjänster, om denne så önskar, även godta ett giltigt pass som har utfärdats av en myndighet i någon annan stat. Det finns ingen skyldighet att godkänna övriga staters pass, och tjänsteleverantören kan välja de stater, av vilkas myndigheter beviljade pass leverantören kan anse sig kunna godkänna. Det är klart att riskerna ökar i fråga om sådana pass. Tjänsteleverantören måste bedöma vilka risker leverantören förmår ta på sig.

För leverantören av identifieringstjänster innebär bestämmelsen att tjänsteleverantören kan utbilda sin personal i att identifiera de handlingar som räknas upp i det föreslagna momentet. Om tjänsteleverantören utnyttjar möjligheten att godkänna övriga staters pass så som sägs i slutet av 1 mom., ska leverantören tydligt fastställa vilka staters pass som godtas. Dessa ska även nämnas i tjänsteleverantörens principer för identifiering. Dessutom ska tjänsteleverantören säkerställa att de anställda har fått tydliga och konsekventa anvisningar om detta och att de anställda även utbildas i att identifiera handlingarna med tillräcklig säkerhet.

I den föreslagna paragrafen eller i övriga paragrafer i lagförslaget ingår inget särskilt omnämnande av möjligheten att använda ombud. Eftersom användning av ombud vid inledande identifiering inte uttryckligen har förbjudits, innebär detta att det är tillåtet att använda ombud. Leverantören av identifieringstjänster svarar även till denna del för verksamheten hos de personer som tjänsteleverantören anlitar på det sätt som konstateras i det föreslagna 13 § 4 mom.

Enligt den sista meningen i 1 mom. ska den inledande identifieringen göras personligen. Enligt det föreslagna 2 mom. behöver den inledande identifieringen inte göras personligen, om leverantörer av identifieringstjänster sinsemellan har avtalat om möjligheten att lita på en inledande identifiering som en annan leverantör har gjort. Leverantörer av identifieringstjänster har ingen rätt att utnyttja en annans inledande identifiering utan ömsesidigt avtal. Det bör anses höra till näringsfriheten för en leverantör av identifieringstjänster att besluta om saken, dvs. det kan inte finnas någon fri rätt att utnyttja en inledande identifiering som gjorts av en annan tjänsteleverantör. Ömsesidigheten innebär inte att avtalet nödvändigtvis måste gälla i båda riktningar, utan tjänsteleverantörerna

kan också komma överens om att endast den ena leverantören vid sin inledande identifiering förlitar sig på ett identifieringsverktyg för stark autentisering som utgivits av den andra leverantören. Däremot förhindrar avtalets ömsesidighet möjligheten att bilda avtalskedjor utan att den leverantör av identifieringstjänster som gjort den inledande identifieringen är med i avtalsarrangemanget.

Tjänsteleverantörerna ska i sitt avtal fastställa hur ansvaret för en eventuell felaktig inledande identifiering fördelas mellan dem. Den tjänsteleverantör av identifieringstjänster som litar på en inledande identifiering som gjorts av en annan tjänsteleverantör bär ansvaret i förhållande till den skadelidande. Den senare bestämmelsen är logisk, eftersom innehavaren av ett identifieringsverktyg ofta även samtidigt är konsument. Den avgör emellertid dock inte frågan om regressrätt mellan tjänsteleverantörerna.

Vid utgivningen av ett identifieringsverktyg med förlitande på den inledande identifieringen som gjorts av en annan tjänstetillhandahållare behövs i regel en elektronisk process. Enligt paragrafens 3 mom. kan man på motsvarande sätt med elektronisk process ansöka om ett identifieringsverktyg också i ett sådant fall där det redan existerar ett kundförhållande mellan leverantören av identifieringstjänster och innehavaren av ett identifieringsverktyg. Det kan t.ex. vara fråga om att avtalet och identifieringsverktyget som avses i 20 § gäller tills vidare och innehavaren av verktyget vill fortsätta kundförhållandet. I ett sådant fall behöver den inledande identifieringen inte göras på nytt.

I paragrafens 4 mom. konstateras, att om identiteten hos den som skaffar ett identifieringsverktyg inte kan verifieras på ett tillförlitligt sätt, ska polisen utföra den inledande identifieringen i samband med ansökan. Det kan för det första vara fråga om en situation där innehavaren inte har någon av de handlingar som avses i 1 mom. För det andra kan det vara fråga om en situation där personen kan uppvisa en sådan handling, men tjänsteleverantörens kundservice ändå inte kan uppnå tillräcklig säkerhet om att handlingen faktiskt tillhör den person som uppvisar den. Detta kan till exempel vara fallet när personen uppvisar en mycket gammal handling. Giltighetstiden för pass kommer i framtiden att begränsas till fem år, vilket innebär att antalet situationer av denna typ sannolikt kommer att minska. Ett tredje exempel är fall där handlingen kan antas vara förfalskad.

Polisen underrättar leverantören av identifieringstjänster om slutresultatet. Polisen kan göra en tillförlitlig identifiering även utifrån pass från länder utanför EES-området, eftersom polisen har anställda med särskilda kunskaper om detta. Dessutom kan polisen utnyttja olika databaser för verifiering av identiteten. Det är fråga om polisens tjänst, dvs. en offentligrättslig prestation vars avgift fastställs enligt lagen om grunderna för avgifter till staten. Avgiften tas ut av den sökande som sådan.

18 §. Förhindrande eller begränsning av användningen av identifieringsverktyg i samband med rättshandlingar. Enligt den föreslagna paragrafens 1 mom. får användningen av identifieringsverktyg för att utföra rättshandlingar genom avtal mellan parterna förhindras eller utförandet av rättshandlingar begränsas både när det gäller användningsändamål och transaktionernas värde i pengar.

Direktivet om ett gemenskapsramverk för elektroniska signaturer innehåller motsvarande bestämmelser för kvalificerade certifikat i artikel 6.4. I lagen om elektroniska signaturer nämns motsvarande begränsningar av användningen i 7 § 2 mom. 8 punkten, liksom i 30 § 2 mom. 8 punkten i denna lag.

Av det föreslagna momentet framgår att begränsningarna kan gälla de användningsändamål som identifieringsverktyget kan användas till. Man kan till exempel begränsa kvaliteten på de rättshandlingar som utförs. Begränsningarna kan också anges i eurobelopp. Det finns inte heller något som hindrar att förse ett identifieringsverktyg med bägge begränsningarna.

Begränsningarna kan inte vara effektiva, om inte de som förlitar sig på identifieringsverktyget kan få kännedom om dem. Därför anknyter till fastställandet av en begränsning i 2 mom. ett krav på att leverantören av identifieringstjänster ska se till att alla parter känner till hindren eller begränsningarna eller att de är lätta upptäcka. Detta behöver dock inte göras om verktyget för stark autentisering är sådant, att användning i strid med

hindren och begränsningarna har förhindrats med hjälp av tekniska medel. En del av identifieringsverktygen för stark autentisering kan vara sådana, att åtgärder i strid med begränsningarna helt enkelt inte går att genomföra. I en de av verktygen går det inte att använda tekniska hinder, utan eventuella begränsningar av användningen måste kontrolleras särskilt.

I det föreslagna momentet konstateras vidare att leverantören av identifieringstjänster inte svarar för de åtgärder som har vidtagits i strid med sådana hinder eller begränsningar, trots att tjänsteleverantören fullgjort sina skyldigheter ovan. Regleringen motsvarar bestämmelserna i fråga om kvalificerade certifikat i direktivet om ett gemenskapsramverk för elektroniska signaturer och lagen om elektroniska signaturer, liksom det föreslagna 41 § 3 mom.

Paragrafens 3 mom. innehåller en bestämmelse om att leverantören av identifieringstjänster ska se till att det finns en möjlighet att vid behov kontrollera de hinder och begränsningar som gäller identifieringsverktyget dygnet runt. En sådan möjlighet behövs inte, om användning av verktyget i strid med hindren och begränsningarna har förhindrats med hjälp av tekniska medel.

Enligt paragrafens 4 mom. ska en tjänsteleverantör som använder en identifieringstjänst i samband med användningen av ett identifieringsverktyg vid behov kontrollera eventuella hinder eller begränsningar av användningen i de system och register som leverantören av identifieringstjänster upprätthåller. Det finns inget behov av kontroll om användning av identifieringsverktyget i strid med begränsningen av användningen har förhindrats med hjälp av tekniska medel. I annat fall ska en kontroll alltid göras.

Tjänsteleverantörens skyldighet motsvaras av den i 23 § föreslagna skyldigheten för innehavaren av ett identifieringsverktyg att använda verktyget i enlighet med avtalsvillkoren.

19 §. Certifikatets innehåll. Paragrafen gäller stark autentisering som genomförs med en viss teknik. Motsvarande paragraf ingår också i 7 § 2 mom. i den gällande lagen om elektroniska signaturer och i den föreslagna 30 §. Dessa gäller kvalificerade certifikat. Genom nämnda paragrafer genomförs artikel 1 i direktivet om ett gemenskapsramverk för elektroniska signaturer.

I paragrafens 1 mom. bestäms om de uppgifter som den som tillhandahåller certifikat åtminstone ska ange i certifikatet. Bestämmelsen är alltså inget hinder för att även andra nödvändiga uppgifter anges. Det är fråga om uppgifter om certifikatutfärdaren, innehavaren av certifikatet och innehavarens identifieringskod, certifikatets giltighetstid, certifikatets identifieringskod och eventuella hinder eller begränsningar som gäller användningen av certifikatet. Certifikatet ska även innehålla certifikatinnehavarens öppna nyckel och nyckelns användningsändamål samt certifikatutfärdarens avancerade elektroniska signatur.

Uppgiften om certifikatets innehavare kan vara namn eller pseudonym med uppgift om att det är en pseudonym. Såsom i 8 § 2 mom. konstateras kan tjänsten även tillhandahållas så att leverantören av identifieringstjänster endast meddelar den tjänsteleverantör som använder en identifieringstjänst den pseudonym som innehavaren av identifieringsverktyget använder eller ett begränsat antal personuppgifter. Certifikatinnehavarens identifieringskod kan till exempel vara en elektronisk kommunikationskod. Den kan även vara en personbeteckning, om förutsättningarna i 6 § 3 mom. uppfylls. Det är således endast den part som förlitar sig på certifikatet som får få kännedom om personbeteckningen, och den får inte vara tillgänglig i en offentlig katalog.

Elektroniska identifieringskoder har hittills inte lämnats ut till dem som tillhandahåller certifikattjänster. Den lag om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster som för närvarande är under behandling i riksdagen kommer dock sannolikt att förändra denna situation. Enligt 43 § 2 mom. 2 punkten i nämnda lag får en elektronisk kommunikationskod lämnas ut till en i Finland etablerad certifikatutfärdare som använder koden i certifikat som en uppgift som identifierar innehavaren av certifikatet.

Den föreslagna 3 punkten hindrar inte att leverantören av identifieringstjänster även kan använda någon annan identifieringskod, t.ex. en kod som leverantören själv skapat för

sina egna system, men det rekommenderas att den elektroniska kommunikationskoden används.

Med certifikatets giltighetstid avses både tidpunkten för när certifikatet börjar gälla och tidpunkten för när det upphör att gälla. Certifikatets identifieringskod kan utgöras av ett löpande serienummer eller någon annan teckensträng som fungerar som identifieringskod.

Av datainnehållet i certifikatet ska framgå eventuella begränsningar av användningen. Med detta hänvisas särskilt till begränsningarna enligt 18 §, som kan anknyta antingen till användningsändamålet eller till eurobelopp eller till bådadera. Certifikatet ska även innehålla certifikatinnehavarens öppna nyckel och nyckelns användningsändamål samt certifikatutfärdarens avancerade elektroniska signatur.

I paragrafens 1 mom. bestäms alltså om de uppgifter som åtminstone ska anges i certifikatet. Bestämmelsen utgör alltså inget hinder för att andra nödvändiga uppgifter tas med. Sådana uppgifter kan t.ex. vara uppgift om certifikatinnehavarens roll, uppgift om den certifikatpolitik som tillämpas och uppgift om etableringsstaten för leverantören av identifieringstjänster.

Certifikatpolitikens identifikator (OID Object Identifier) är en uppgift med vars hjälp man hittar det dokument som beskriver certifikatpolitiken. Utöver identifikatorn kan certifikatet även direkt innehålla politikens webbadress. I certifikatpolitiken finns alltid uppgifter om certifikatutfärdarens etablering och övriga kontaktuppgifter. I certifikatpolitiken ingår dessutom bland annat en redogörelse för arrangemangen i samband med beviljande av certifikat.

Med stöd av 2 mom. ska den som tillhandahåller certifikattjänster för sin del försäkra sig om att en tjänsteleverantör som använder ett certifikat för elektronisk identifiering har tillgång till certifikatets innehåll. Innehållet kan till exempel finnas tillgängligt direkt ur certifikatet eller från ett certifikatregister som upprätthålls av den som tillhandahåller certifikat.

20 §. Utgivning av identifieringsverktyg. I paragrafen meddelas grundläggande bestämmelser för reglering av avtalsförhållandet mellan leverantören av identifieringstjänster och innehavaren av verktyget. I paragrafens 1 mom. konstateras att utgivningen av identifieringsverktyget grundar sig på ett avtal mellan den som ansöker om verktyget och leverantören av tjänster för stark autentisering. Utgångspunkten torde vara uppenbar, men genom att skriva in bestämmelsen i lagen vill man betona parternas självbestämmanderätt. Enligt bestämmelsen ska avtalet ingås skriftligen. Detta är emellertid inget hinder för att avtalet ingås elektroniskt. I detta fall förutsätts att avtalets innehåll inte kan ändras ensidigt och att det hålls tillgängligt för parterna.

Enligt paragrafens 2 mom. kan avtalet gälla tills vidare eller för viss tid. Ett verktyg för stark autentisering kan ha en giltighetstid som är kortare än avtalets giltighetstid. I praktiken kan man bli tvungen att förnya verktyg för stark autentisering under avtalets giltighetstid till exempel på grund av att deras prestationsegenskaper försvagas när verktyget används eller med tiden. Det är självklart att verktygets giltighetstid avslutas när avtalet upphör att gälla ut även i fall av uppsägning eller hävning.

Enligt paragrafens 3 mom. beviljas identifieringsverktyget till fysiska personer. Innehavaren av verktyget kan dock företräda andra fysiska eller juridiska personer. Sammankopplingen av uppgiften om roll med en person ska ske i en särskild, om än eventuellt parallell process. En fungerande stark autentisering förutsätter till denna del att rolldatatjänsterna utvecklas. För närvarande har sådana tjänster skapats för skatteförvaltningen inom systemet Katso för autentisering av organisationer. Dessutom har patent- och registerstyrelsen utvecklat en rolldatatjänst. Erhållandet av grundläggande rolluppgifter och eventuell kommersiell verksamhet i anslutning till detta är mycket viktiga områden för vidareutveckling inom elektronisk identifiering.

I 3 mom. konstateras det också att ett identifieringsverktyg ska vara personligt. Till exempel bankkoder beviljades i verksamhetens inledningsskede familjevis. Denna praxis har redan frångåtts, men det är skäl att även ta upp saken i den föreslagna lagen. Identifieringens syfte förutsätter att identifierings-

transaktionen med säkerhet kan inriktas på en viss person. På motsvarande sätt har som en skyldighet för innehavaren av ett identifieringsverktyg i det föreslagna 23 § 2 mom. fastställts att verktyget inte får överlåtas för att användas av någon annan.

21 §. *Överlåtelse av identifieringsverktyg till sökande*. I den föreslagna paragrafen föreskrivs det om överlåtelse av identifieringsverktyg till sökande, som därefter betecknas som innehavare av verktygen. Som bakgrund till bestämmelsen finns en målsättning att sänka tröskeln för anskaffning av identifieringsverktyg så att den blir så låg som möjligt utan att säkerheten äventyras.

Enligt den föreslagna paragrafen ska en leverantör av elektroniska identifieringstjänster överlåta identifieringsverktyget till den sökande på det sätt som anges i avtalet mellan dessa parter och på ett sådant sätt att det inte finns någon risk att verktyget eller specificerande uppgifter som behövs vid användningen av verktyget obehörigt kommer i någon annans besittning. Enligt definitionen omfattar identifieringsverktyget också specificerande uppgifter som eventuellt behövs vid användningen av verktyget. Den föreslagna bestämmelsen innebär till stor del ett liknande arrangemang som i fråga om till exempel kreditkort.

Den som ansöker om ett identifieringsverktyg ska kunna avgöra om den vill ta emot verktyget per post eller inte, om den som tillhandahåller identifieringstjänsten erbjuder en sådan möjlighet. Tjänsteleverantören ska se till att till exempel en PIN kod eller motsvarande uppgifter som behövs vid användningen av verktyget inte levereras i samma försändelse eller samma dag som till exempel ett kort eller SIM kort, och att leveransen av verktyg och specificerande uppgifter i övrigt sker på ett säkert sätt. Absolut säkerhet kan dock inte heller i detta sammanhang eftersträvas och därför konstateras det i bestämmelsen att tjänsteleverantören på ett tillräckligt sätt ska säkerställa att leveransen sker på ett säkert sätt.

Den som tillhandahåller identifieringstjänsten står för risken i samband med att identifieringsverktyget, inklusive de specificerande uppgifter som behövs vid användningen av verktyget, skickas till betalaren. Ansvaret övergår enligt 23 § 1 mom. till innehavaren av identifieringsverktyget först när denne har tagit emot verktyget. Tjänsteleverantören är skyldig att bevisa att innehavaren av identifieringsverktyget har tagit emot verktyget och de specificerande uppgifter som eventuellt behövs vid användningen av verktyget.

22 §. *Förnyande av identifieringsverktyg*. I paragrafen föreskrivs det om förnyande av identifieringsverktyg. Såsom konstateras i 20 § 2 mom., kan ett identifieringsverktyg ha en egen giltighetstid som är kortare än giltighetstiden för avtalet mellan leverantören av identifieringstjänsten och innehavaren av identifieringsverktyget. Man kan bli tvungen att förnya verktyget då och då för att garantera att det fungerar klanderfritt. 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. Rätten begränsar sig uttryckligen till denna situation. Vid leveransen ska bestämmelserna i 21 § iakttas. Avsikten är att en bestämmelse med motsvarande innehåll ska föreslås i betaltjänstlagen.

23 §. *Skyldigheter för innehavare av identifieringsverktyg.* I paragrafen föreskrivs det i huvudsak om sådant som ska iakttas i ett avtalsförhållande i ren allmänhet. Bestämmelsen behövs dock av tydlighetsskäl.

Enligt 1 mom. ska innehavaren av ett identifieringsverktyg använda verktyget enligt de villkor som gäller utgivning och användning av identifieringsverktyg. Det gäller speciellt sådana eventuella begränsningar eller av hinder för användningen enligt den föreslagna 18 § som hänför sig till användningsändamål eller eurobelopp.

Enligt det föreslagna momentet ska innehavaren av verktyget också förvara verktyget omsorgsfullt. Såsom konstateras i 2 punkten i 2 § om definitioner, omfattar identifieringsverktyget också specificerande uppgifter som behövs för identifieringen. Med specificerande uppgifter avses till exempel kundkoder, PIN koder och andra koder. Vid bedömningen av vilka försiktighetsåtgärder det är skäligt att kräva av innehavaren av ett identifieringsverktyg, bör man beakta att vanliga hjälpmedel för identifiering i allmänhet är

avsedda att användas ofta och att de därför ska kunna medföras. Till de försiktighetsåtgärder som skäligen kan krävas av innehavaren av ett identifieringsverktyg kan man i allmänhet räkna till exempel att innehavaren förvarar identifieringsverktyget och de specificerande uppgifter som behövs vid användningen av verktyget separat så att en utomstående inte kan koppla dem till varandra. Man kan dock inte kräva oskäligt långtgående säkerhetsarrangemang av den som innehar ett identifieringsverktyg. Om innehavaren av ett identifieringsverktyg till exempel förvarar både identifieringsverktyget och koden i sitt hem, betyder det fortfarande inte i sig att denne skulle ha försummat sin aktsamhetsplikt. Som omsorgsfullt förfarande kan man i allmänhet betrakta till exempel att identifieringsverktyget förvaras i plånboken eller handväskan och koden hemma i en byrålåda.

Omsorgsfullheten när det gäller försiktighetsåtgärder bedöms som en helhet. Vid helhetsbedömningen bör man även fästa uppmärksamhet vid eventuella särskilda säkerhetsarrangemang som innehavaren av identifieringsverktyget har vidtagit. Om identifieringsverktyget och dess kod till exempel förvaras i samma kassaskåp eller på en annan motsvarande plats där utomstående endast i undantagsfall kan få tag på dem, är detta inte nödvändigtvis bevis på vårdslöshet.

Till de försiktighetsåtgärder som man skäligen kan kräva av innehavaren av ett identifieringsverktyg hör även att denne kontrollerar att verktyget är i behåll på ett sådant sätt som omständigheterna kräver. Om innehavaren av identifieringsverktyget till exempel rör sig i stora människomassor eller på andra platser där risken för fickstölder är särskilt stor, är dennes skyldighet att kontrollera att verktyget är i behåll större, eftersom man i allmänhet inte upptäcker en professionellt utförd fickstöld samtidigt som den sker.

Om innehavaren av ett identifieringsverktyg försummar sin aktsamhetsplikt enligt momentet, kan han eller hon bli ansvarig för obehörig användning av ett identifieringsverktyg i enlighet med 27 §.

I 2 mom. finns det ett förbud mot att överlåta ett verktyg för att användas av någon annan. Innehavaren av till exempel ett bank- eller kreditkort kan överlåta kortet till en familjemedlem och avslöja den specificerande uppgift som behövs vid användningen av kortet. I princip har detta ingen betydelse för kreditkortsföretaget så länge som räkningarna betalas i tid. För identifieringsverktygen är däremot identiteten på den person som kopplas till ett visst identifieringsverktyg det väsentliga. Av denna anledning bör även innehavarna av identifieringsverktyg förstå att verktygen inte får överlåtas åt någon annan.

Innehållet i den föreslagna paragrafen motsvarar till rätt stor del kraven i EU:s betaltjänstdirektiv, som genomförs i Finland genom den betaltjänstlag som är under beredning vid justitieministeriet.

24 §. *Registrering och användning av uppgifter om identifieringstransaktioner och om identifieringsverktyg.* I paragrafen föreskrivs det om uppgifter som behövs om man i efterskott blir tvungen att reda ut en identifieringstransaktion eller omständigheter i anslutning till en rättshandling som utförts mellan en tjänsteleverantör som använder stark autentisering och en innehavare av ett identifieringsverktyg.

Enligt 1 mom. ska leverantören av identifieringstjänster registrera uppgifter som behövs för att verifiera en enskild identifieringstransaktion. Med uppgifter som behövs för att verifiera identifieringstransaktionen enligt den föreslagna 1 punkten avses de uppgifter som leverantören av identifieringstjänsten i samband med identifieringen meddelade den tjänsteleverantör som använde tjänsten för stark autentisering, samt vilka omständigheter denna anmälan byggde på. Dessutom ingår bland annat klockslag och datum i dessa uppgifter.

Dessutom ska tjänsteleverantören registrera de uppgifter som behövs om den inledande identifiering av en sökande som avses i 17 § och om den handling som anlitats för identifieringen. Behövliga uppgifter kan till exempel vara passets eller identitetskortets nummer. I vissa fall kan det vara nödvändigt att bevara en fotokopia av de handlingar som använts. Det kan vara nödvändigt att i efterhand kunna bevisa ett sakförhållande, om identifieringsverktyget har getts till fel person. En utredning av den process som avses i 17 § kan vara nödvändig bland annat för att reda ut vem som ansvarar för eventuell ska-

da, om det visar sig att ett identifieringsverktyg har getts till fel person.

Vidare ska tjänsteleverantören registrera uppgifter om sådana eventuella begränsningar för användningen av identifieringsverktyget som avses i 18 § och, i fråga om certifikat, uppgifter om certifikatets innehåll enligt 19 §.

Bestämmelsen i den föreslagna 3 punkten säkerställer att eventuella begränsningar för användningen enligt den föreslagna 18 § kan redas ut även i efterskott. Även när det gäller dessa torde det oftast vara fråga om utredning av ansvarsförhållanden.

En bestämmelse som motsvarar den föreslagna 4 punkten finns i 14 § i lagen om elektroniska signaturer och i den föreslagna 37 §. I det certifikatregister som avses i 37 § registreras dock även andra uppgifter.

I 2 mom. finns det bestämmelser om förvaringstider. Enligt dessa ska de uppgifter som avses i 1 punkten förvaras i fem år från identifieringstransaktionen, medan de uppgifter som avses i 2–4 punkten ska förvaras i fem år från det att kundförhållandet mellan leverantören av identifieringstjänster och innehavaren av ett identifieringsverktyg upphörde. Bestämmelserna motsvarar kraven i regelverken om konsumentskydd och penningtvätt. Samtidigt innebär de att den som tillhandahåller identifieringstjänster måste förvara en mycket stor mängd information. I vissa fall är förvarandet av uppgifter naturligtvis även i tjänsteleverantörens eget intresse.

För jämförelsens skull kan det konstateras att uppgifterna i certifikatregistret enligt lagen om elektroniska signaturer ska förvaras i tio år. Enligt den föreslagna 38 § får utfärdare av kvalificerade certifikat som också tillhandahåller identifieringstjänster, oberoende av vad som föreskrivs i denna paragraf, förvara alla uppgifter i certifikatregistret i tio år från det att certifikatet upphörde att gälla.

Enligt 3 mom. ska de personuppgifter som har samlats in i samband med en identifieringstransaktion förstöras efter transaktionen, om det inte är nödvändigt att registrera dem enligt 1 mom. 1 punkten för att verifiera en enskild identifieringstransaktion. Med hjälp av bestämmelsen strävar man efter att minska mängden personuppgifter som registreras i tjänsteleverantörernas system.

I 4 mom. begränsas syftena för behandling av uppgifter. Leverantörer av identifieringstjänster får behandla uppgifter för eget behov endast för att tillhandahålla och upprätthålla tjänsterna, utföra fakturering och trygga sina egna rättigheter. Det sistnämnda fallet gäller tvister. Utöver detta får leverantören av identifieringstjänster behandla uppgifter om den får en begäran om behandling av en tjänsteleverantör som använder stark autentisering eller av en innehavare av ett identifieringsverktyg, eller av båda. I sådana fall torde det vara fråga om att det mellan dessa båda parter finns oklarheter om någon identifieringstransaktion och eventuella rättshandlingar i anslutning därtill.

Enligt den föreslagna bestämmelsen ska leverantören av identifieringstjänster registrera uppgifter om behandlingen av identifieringstransaktionen, tidpunkt och orsak till transaktionen samt vem som utfört den. Till exempel 15 § i lagen om dataskydd vid elektronisk kommunikation innehåller en motsvarande bestämmelse om registrering av uppgifter om behandlingen av identifieringsuppgifter.

Paragrafens 5 mom. gäller tjänsteleverantörer som endast ger ut identifieringsverktyg. Registreringsskyldigheten enligt den föreslagna 1 mom. 1 punkten gäller naturligtvis inte sådana tjänsteleverantörer, eftersom de inte har tillgång till sådana uppgifter. Den förvaringstid på fem år som avses i 2 mom. räknas då från det att verktyget upphörde att gälla.

25 §. *Anmälan om återkallande eller förhindrande av användning av identifieringsverktyg.* I 1 mom. föreskrivs att innehavaren av ett identifieringsverktyg ska anmäla till leverantören av identifieringstjänster eller någon annan aktör som denne har utsett att verktyget har försvunnit, obehörigt har kommit i någon annans besittning eller obehörigt har använts. Anmälan ska göras utan obefogat dröjsmål efter det att saken har upptäckts. Någon annan aktör som tjänsteleverantören har utsett kan t.ex. vara tjänsteleverantörernas gemensamma spärrtjänst. Frågan om innehavaren av identifieringsverktyget har gjort anmälan utan obefogat dröjsmål avgörs från fall till fall med beaktande av om-

ständigheterna. I den föreslagna paragrafen föreskrivs inte om någon särskild form för anmälan om försvinnande. En innehavare av ett identifieringsverktyg som har försummat sin anmälningsplikt kan med stöd av 27 § bli ansvarig för obehörig användning av identifieringsverktyget.

Enligt 2 mom. ska leverantören av identifieringstjänster se till att det är möjligt att när som helst göra en anmälan om återkallande eller förhindrande av användningen av ett verktyg. Tjänsteleverantören ska omedelbart återkalla verktyget eller förhindra att det används efter det att information om saken har mottagits.

I det föreslagna momentet avses med uttrycket ”när som helst” att en innehavare av ett identifieringsverktyg ska kunna göra en anmälan under alla dagar på året och alla tider på dygnet. En tjänsteleverantör kan uppfylla sin skyldighet t.ex. genom att ordna en telefonjour som alltid är öppen. Tjänsteleverantören ska dimensionera resurserna för telefonjouren eller motsvarande arrangemang så att innehavarna av identifieringsverktyg också i praktiken har möjlighet att alltid göra en anmälan utan hinder eller fördröjningar t.ex. på grund av rusning i telefontjänsten.

I 3 mom. föreskrivs att uppgift om tidpunkten för återkallandet ska registreras i systemet på lämpligt sätt och utan dröjsmål. Innehavaren av ett identifieringsverktyg har rätt att på begäran få ett intyg över att han eller hon har gjort anmälan enligt 1 mom. Den föreslagna bestämmelsen är en följd av att innehavaren av ett identifieringsverktyg har skyldighet att bevisa att han eller hon har gjort anmälan enligt 1 mom. Denna skyldighet är lättare att uppfylla med hjälp av det intyg som avses i det föreslagna momentet.

I bestämmelsen avses med intyg alla sådana utredningar som innehavaren av ett identifieringsverktyg i ett senare skede kan använda för att på ett entydigt och tillförlitligt sätt visa att anmälan har gjorts. Om innehavaren av ett identifieringsverktyg vill ha ett intyg, ska han eller hon begära det inom 18 månader från anmälan. Bestämmelsen om en tidsfrist förhindrar naturligtvis inte att tjänsteleverantören utfärdar ett intyg, även om det begärs först senare.

I 4 mom. ställs ett krav på att systemet ska vara sådant att en tjänsteleverantör som använder en identifieringstjänst vid behov lätt kan kontrollera uppgifterna i systemet vilken tid på dygnet som helst. Om användningen av identifieringsverktyget kan förhindras helt med hjälp av tekniska medel eller om verktyget kan spärras är det inte nödvändigt att ordna möjlighet att kontrollera uppgifterna.

Om en identifieringstjänst grundar sig på certifikat och uppgifter om återkallade certifikat ges med hjälp av en spärrlista, får den som tillhandahåller certifikattjänster med stöd av 5 mom. registrera uppgifter om kontroll av certifikatens giltighet som gjorts på spärrlistan. Certifikatutfärdaren kan alternativt lagra spärrlistan, vilket kan minska mängden uppgifter som registreras. I fråga om elektroniska signaturer finns en motsvarande bestämmelse i 21 § i lagen om elektroniska signaturer och i den föreslagna 39 §.

Den föreslagna paragrafen motsvarar till rätt stor del kraven i EU:s betaltjänstdirektiv, som genomförs i Finland genom den betaltjänstlag som är under beredning vid justitieministeriet.

26 §. *Rätten för leverantörer av identifieringstjänster att återkalla eller förhindra användning av identifieringsverktyg.* Paragrafen ger leverantörer av identifieringsverktyg rätt stora möjligheter att ingripa i användningen av identifieringsverktyg. Den föreslagna bestämmelsen är dock motiverad därför att obehörig användning av en annan persons identitet kan ha ödesdigra konsekvenser på individnivå. Rätten för leverantörer av identifieringstjänster att återkalla eller förhindra användning av identifieringsverktyg har begränsats till fem situationer.

Enligt 1 mom. 1 punkten får leverantören av identifieringstjänster återkalla eller förhindra användningen av ett identifieringsverktyg, om tjänsteleverantören har skäl att misstänka att verktyget används av någon annan än den som identifieringsverktyget har getts ut till. En sådan situation kan uppstå genom att innehavaren av ett identifieringsverktyg har överlåtit verktyget för att användas av någon annan i strid med den uttryckliga bestämmelsen i 23 § 2 mom. En sådan situation som avses i 1 punkten kan dock också

uppstå utan att innehavaren av identifieringsverktyget själv är medveten om situationen.

Enligt 1 mom. 2 punkten kan ett identifieringsverktyg återkallas eller användningen av det förhindras också om leverantören av identifieringstjänster upptäcker att verktyget innehåller ett uppenbart fel. Det är då fråga om ett fel som beror på leverantören av identifieringstjänster och som denne inte har upptäckt tidigare.

Enligt 1 mom. 3 punkten får ett identifieringsverktyg återkallas eller användningen av det förhindras, om leverantören av identifieringstjänster har skäl att misstänka att säkerheten vid användningen av verktyget har äventyrats. Bestämmelsen täcker både de fall där äventyrandet av säkerheten endast gäller identifieringsverktyget i fråga och de fall där användningen av identifieringsverktyget har äventyrats av orsaker som har samband med systemet i allmänhet.

Enligt 1 mom. 4 punkten kan ett identifieringsverktyg återkallas eller användningen av det förhindras om innehavaren av verktyget använder verktyget på ett sätt som väsentligt strider mot avtalsvillkoren. Det kan t.ex. vara fråga om användning i strid med de hinder och begränsningar som anges i 18 §. Det bör dock noteras att förseelsen ska vara betydande för att en tjänsteleverantör ska kunna utnyttja den rätt som avses i den föreslagna paragrafen.

Enligt 1 mom. 5 punkten kan ett identifieringsverktyg återkallas eller användningen av det förhindras också när leverantören av identifieringstjänster har fått veta att innehavaren av identifieringsverktyget har avlidit. Eftersom ett identifieringsverktyg är personligt på det sätt som konstateras i 20 § 3 mom. är det i ett sådant fall på sin plats att leverantören av identifieringstjänster kan börja vidta åtgärder för att förhindra möjligheterna att använda verktyget.

Enligt 2 mom. ska leverantören av identifieringstjänster underrätta innehavaren av identifieringsverktyget att verktyget har återkallats eller användningen av det förhindrats och ange tidpunkten för återkallandet eller förhindrandet av användningen och orsakerna till det. Det är skäl att anmäla saken så snart som möjligt. På samma sätt som den föreslagna 16 § innehåller inte heller denna bestämmelse något krav på att anmälan ska ske omedelbart. Orsaken till det är att det ibland kan vara bättre att först försöka avhjälpa exempelvis en brist i skyddet av uppgifter som tjänsteleverantören känner till, men som inte är allmänt känd. Det är alltså upp till leverantören av identifieringstjänster att överväga när anmälan ska ske. Det är i vilket fall som helst klart att det är tjänsteleverantörens skyldighet att försöka minimera eventuella skador.

Enligt 3 mom. ska leverantören av identifieringstjänster erbjuda en ny möjlighet att använda identifieringsverktyget eller tillhandahålla innehavaren av verktyget ett nytt verktyg genast efter det att en sådan orsak som avses 1 mom. 2 och 3 punkten inte längre föreligger. I fråga om 1 och 4 punkten har tjänsteleverantören frihet att för sin del överväga om avtalet med innehavaren av verktyget ska fortsätta.

Den föreslagna paragrafen motsvarar till rätt stor del kraven i EU:s betaltjänstdirektiv, som genomförs i Finland genom den betaltjänstlag som är under beredning vid justitieministeriet.

27 §. *Innehavarens ansvar för obehörig användning av ett identifieringsverktyg.* I paragrafen föreskrivs om verktygsinnehavarens ansvar i situationer där en annan person använder eller har använt ett identifieringsverktyg på ett obehörigt sätt. Ett typfall då paragrafen blir tillämplig är när ett identifieringsverktyg har försvunnit eller stulits och den som har hittat eller stulit verktyget lyckas använda det. Det bör noteras att det är svårare att använda ett identifieringsverktyg på ett obehörigt sätt än vad det hittills har varit t.ex. när det gäller olika betalkort. Enligt definitionen förutsätter användningen av ett identifieringsverktyg alltid åtminstone två element, varav det ena ofta är en PIN-kod. Däremot har betalkort hittills i allmänhet använts så att de förutsätter en underskrift.

I 7 kap. 19 § i den gällande konsumentskyddslagen finns bestämmelser om det ansvar som kontoinnehavare i konsumentställning har vid obehörig användning av kreditkort eller annat identifieringsmedel som berättigar till kontokredit. Motsvarande bestämmelser finns också i andra lagar, t.ex. i kommunikationsmarknadslagen. Nedan re-

dogörs skilt för varje bestämmelse till vilken del den föreslagna paragrafen till sitt innehåll motsvarar den nämnda paragrafen i konsumentskyddslagen eller avviker från den. Den föreslagna paragrafen motsvarar till stor del kraven i EU:s betaltjänstdirektiv, som genomförs i Finland genom den betaltjänstlag som är under beredning vid justitieministeriet. Den föreslagna lagen innehåller dock inte den bestämmelse i fråga betaltjänster som har sin grund i betaltjänstdirektivet och som gäller en självrisk på 150 euro för konsumenter-verktygsinnehavare. Orsaken är att tjänster för stark autentisering tillhandahålls i en helt annan miljö som bestämmelsen i fråga inte är avsedd att tillämpas på.

Huvudprinciperna i bestämmelsen motsvarar också bestämmelsen i den föreslagna 40 §, som gäller undertecknarens ansvar vid obehörig användning av signaturframställningsdata i fråga om kvalificerade certifikat. Den aktuella bestämmelsen är emellertid exaktare och avsikten har varit att skriva bestämmelsen på motsvarande sätt som betaltjänstlagen enligt det nuvarande sättet att skriva lagtexter på.

I 1 mom. ges en uttömmande förteckning över de situationer där innehavaren av ett identifieringsverktyg kan bli ansvarig för obehörig användning av identifieringsverktyget. Enligt 1 punkten kan innehavaren av ett verktyg bli ansvarig för obehörig användning om innehavaren har överlåtit verktyget till någon annan. En motsvarande ansvarsgrund ingår för närvarande i 7 kap. 19 § 1 mom. 1 punkten i konsumentskyddslagen.

I bestämmelsen avses med överlåtelse frivillig överlåtelse av besittningen oberoende av i vilket syfte det sker. Innehavaren av ett identifieringsverktyg kan anses ta en risk att verktyget används på ett obehörigt sätt, även om verktyget överlåts till någon annan t.ex. endast för att förvaras. Därför kan innehavaren bli ansvarig om risken förverkligas. Det är fråga om en sådan överlåtelse som avses i bestämmelsen endast då innehavaren av ett identifieringsverktyg avsiktligt överlåter besittningen av verktyget till någon annan. Bestämmelsen gäller således inte t.ex. en sådan situation där innehavaren av ett identifieringsverktyg överlåter en väska för att förvaras hos någon annan och väskan innehåller identifieringsverktyget. Om det anses att innehavaren av identifieringsverktyget har handlat försumligt i en sådan situation, kan ansvar dock inträda med stöd av 1 mom. 2 punkten.

Enligt 1 mom. 2 punkten kan innehavaren av ett identifieringsverktyg bli ansvarig för obehörig användning om verktyget har försvunnit, obehörigt kommit i någon annans besittning eller obehörigt använts på grund av innehavarens vårdslöshet, som inte är lindrig. En motsvarande ansvarsgrund ingår för närvarande i 7 kap. 19 § 1 mom. 2 punkten i konsumentskyddslagen. Innehavarens skyldighet att ansvara för identifieringsverktyget behandlas ovan i motiveringen till 23 §.

Med stöd av 1 mom. 3 punkten kan innehavaren av ett identifieringsverktyg bli ansvarig för obehörig användning av verktyget om han eller hon har försummat sin skyldighet enligt 25 § att, utan obefogat dröjsmål efter det att saken har upptäckts, anmäla till leverantören av identifieringstjänster eller någon annan aktör som denne har angett att identifieringsverktyget har försvunnit, obehörigt har kommit i någon annans besittning eller obehörigt har använts. En motsvarande ansvarsgrund ingår för närvarande i 7 kap. 19 § 1 mom. 3 punkten i konsumentskyddslagen.

I 2 mom. föreskrivs om de situationer då innehavaren av ett identifieringsverktyg inte ansvarar för obehörig användning av verktyget, även om någon av de ansvarsgrunder som anges i 1 mom. uppfylls.

Enligt 2 mom. 1 punkten ansvarar innehavaren av ett identifieringsverktyg inte för obehörig användning av identifieringsverktyget till den del verktyget har använts efter det att innehavaren har anmält till tjänsteleverantören eller någon annan aktör som leverantören har angett att verktyget har försvunnit, obehörigt har kommit i någon annans besittning eller obehörigt har använts. Bestämmelsen motsvarar i sak 7 kap. 19 § 2 mom. 1 punkten i konsumentskyddslagen.

Enligt 2 mom. 2 punkten ansvarar innehavaren av ett identifieringsverktyg inte heller för obehörig användning av verktyget om leverantören av identifieringstjänster har försummat skyldigheten enligt det föreslagna 25 § 2 mom. att se till att en användare av tjäns-

ter för stark autentisering när som helst har möjlighet att anmäla att identifieringsverktyget har försvunnit, obehörigt kommit i någon annans besittning eller obehörigt använts. Någon motsvarande bestämmelse finns inte i 7 kap. 19 § i konsumentskyddslagen. Bestämmelsen förbättrar således ställningen för innehavare av identifieringsverktyg och är en naturlig följd av försummelse av den skyldighet som har ålagts tjänsteleverantörer.

Enligt 3 mom. ansvarar innehavaren av ett identifieringsverktyg inte för obehörig användning av verktyget om en tjänsteleverantör som använder en identifieringstjänst vid användningen av verktyget har försummat att kontrollera om det finns begränsningar för användningen av verktyget eller uppgift om spärrning av verktyget. En motsvarande bestämmelse finns för närvarande i 7 kap. 19 § 2 mom. 2 punkten i konsumentskyddslagen. Tjänsteleverantörer som använder stark autentisering ska kontrollera om det finns sådana uppgifter när identifieringsverktyget används. Detta behöver inte göras om obehörig användning av verktyget kan förhindras med hjälp av tekniska medel. I annat fall tar leverantören av identifieringstjänster risken att ansvar inträder.

4 kap. Elektronisk signatur

28 §. *Säkra anordningar för signaturframställning*. I paragrafen föreskrivs om de krav som en anordning för signaturframställning ska uppfylla för att den ska kunna betraktas som en säker anordning för signaturframställning. En säker anordning för signaturframställning ska på ett tillräckligt tillförlitligt sätt säkerställa att kraven i 1 mom. 1- 5 punkten uppfylls. Med tillräckligt tillförlitlig avses en så stor tillförlitlighet som möjligt som kan uppnås genom att så högtstående tekniska lösningar som möjligt används.

Enligt 1 punkten i momentet ska en säker anordning för signaturframställning på ett tillförlitligt sätt säkerställa att signaturframställningsdata kan förekomma endast en gång och att de förblir konfidentiella. Den programvara och den utrustning som finns i undertecknarens dator eller någon annan anordning ska vara konstruerad så, att den framställer signaturen och genomför andra behövliga åtgärder på ett så tillförlitligt sätt som möjligt och så, att signaturframställningsdata förblir konfidentiella. Att data garanteras vara konfidentiella innebär bl.a. att de åtgärder som programmet utför sker på så sätt skyddat att man med hjälp av t.ex. ett separat program som installerats i datorn inte kan komma åt signaturframställningsdata.

Enligt 2 punkten i momentet ska en säker anordning för signaturframställning säkerställa att signaturframställningsdata inte kan härledas ur andra data. De åtgärder som vidtas med hjälp av en anordning för signaturframställning får således inte ge tillgång till unika signaturframställningsdata. Detta kan åstadkommas med hjälp av bl.a. programinställningar samt genom olika konstruktionsmässiga lösningar som gäller utrustningen och dess delar. Utöver detta ska den krypteringsalgoritm som används i anordningen för signaturframställning vara tillräckligt stark och nyckeln tillräckligt lång för att signaturframställningsdata, såsom den privata nyckeln, inte ska kunna härledas ur resultatet av krypteringen, dvs. ur den elektroniska signaturen.

Enligt 3 punkten ska en säker anordning för signaturframställning på ett tillförlitligt sätt säkerställa att signaturen är skyddad mot förfalskning. I praktiken kan förfalskning förhindras genom att tillräckligt starka algoritmer och tillräckligt omfattande nycklar används.

Enligt 4 punkten i momentet ska en säker anordning för signaturframställning säkerställa att undertecknaren kan skydda signaturframställningsdata så att andra inte kan använda dem. I praktiken kan detta ske genom att signaturframställningsdata, som finns t.ex. på ett aktivt kort, skyddas med lösenord eller ett system med biometriska kännetecken.

En säker anordning för signaturframställning får enligt 5 punkten i momentet inte förändra de uppgifter som ska signeras. De uppgifter som ska signeras ska förbli oförändrade under processens gång. En anordning för signaturframställning får inte heller hindra att de uppgifter som ska signeras presenteras för undertecknaren före signeringen.

Enligt 2 mom. 1 punkten anses en anordning för signaturframställning alltid uppfylla

kraven i 1 mom. om den överensstämmer med de allmänt erkända standarder som kommissionen har fastställt och som har publicerats i Europeiska gemenskapernas officiella tidning. Enligt 2 punkten anses en sådan anordning för signaturframställning också uppfylla kraven om ett kontrollorgan som har utsetts för att bedöma om kraven uppfylls har godkänt anordningen som en säker anordning för signaturframställning. Kontrollorganet ska ha utsetts särskilt för prövningsuppgiften i fråga samt finnas i Finland eller i en annan stat inom Europeiska ekonomiska samarbetsområdet. I artikel 3.4 andra stycket i direktivet förutsätts det att ett intyg om anordningens säkerhet som utfärdats av ett sådant organ ska erkännas av samtliga EU-medlemsstater. I den förslagna 29 § finns bestämmelser om kontrollorganet.

Paragrafen motsvarar 5 § i lagen om elektroniska signaturer. Genom 1 mom. i paragrafen genomförs bilaga III till direktivet. Genom bestämmelsen i 2 mom. 1 punkten och genom 34 § 2 mom. genomförs artikel 3.5 i direktivet. Genom bestämmelsen i 2 mom. 2 punkten genomförs artikel 3.4 andra stycket i direktivet.

29 §. *Kontrollorgan*. Enligt det föreslagna 1 mom. kan Kommunikationsverket vid behov utse kontrollorgan som har till uppgift att bedöma om en anordning för signaturframställning uppfyller kraven i 28 § 1 mom. Kontrollorganen kan vara antingen privata eller offentliga inrättningar.

Den kommitté för elektroniska signaturer som avses i artikel 9 i direktivet har kommit överens om de minimikrav som ska uppställas för kontrollorganen och som Europeiska gemenskapernas kommission har fastställt genom sitt beslut av den 6 november 2000 om de minimikriterier som skall beaktas av medlemsstaterna när de utser organ enligt artikel 3.4 i Europaparlamentets och rådets direktiv 1999/93/EG om ett gemenskapsramverk för elektroniska signaturer; Bryssel, 06/11/2000, K(2000) 3179 slutlig.

I enlighet med de villkor som kommittén uppställt ska kontrollorganet med hänsyn till verksamheten och ekonomin vara oberoende av andra parter som är verksamma på området. Kontrollorganet, dess ledning och den personal som deltar i bedömningen av anordningarna för signaturframställning får inte vara konstruktörer, tillverkare, leverantörer eller installatörer av säkra anordningar för signaturframställning och inte heller certifikatutfärdare eller deras auktoriserade representanter. Om organet är en del av en organisation som även utför annan än i denna paragraf avsedd kontrollverksamhet, ska organet kunna identifieras som en separat enhet i organisationen och de olika funktionerna inom organisationen tydligt kunna skiljas från varandra.

Kontrollorganets verksamhet ska vara ändamålsenlig och organet får t.ex. inte diskriminera någon som önskar använda sig av dess tjänster. Kontrollorganet ska tillämpa tydliga förfaranden vid bedömningen av säkra anordningar för signaturframställning och det ska dokumentera all relevant information gällande denna bedömning. Vem som helst ska ha rätt att använda kontrollorganets tjänster.

Kontrollorganet ska också ha tillräckliga ekonomiska resurser för att ordna verksamheten på ett ändamålsenligt sätt och för att täcka ett eventuellt ersättningsansvar. Man kan förbereda sig på eventuella ersättningsansvar med t.ex. en ansvarsförsäkring. Dessutom ska kontrollorganet ha tillräckligt med yrkeskunnig och opartisk personal samt sådana lokaler och sådan utrustning som verksamheten kräver. Personalen ska ha tillräcklig utbildning och erfarenhet för att på ett tillförlitligt sätt kunna utföra bedömningsuppgifterna i synnerhet när det gäller de tekniska egenskaperna hos elektroniska signaturer och till dem anslutna informationssäkerhetsaspekter. För att personalens opartiskhet ska kunna garanteras får deras lön inte vara beroende av antalet utförda överensstämmelsebedömningar eller av resultatet av dem.

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

Kommunikationsverket övervakar kontrollorganens verksamhet. Ett kontrollorgan ska underrätta Kommunikationsverket om sådana ändringar i verksamheten som kan inverka på förutsättningarna för att kunna utses till kontrollorgan. Om ett kontrollorgan inte längre uppfyller de krav som ställts på det eller om det bryter mot bestämmelserna, ska Kommunikationsverket återkalla utnämningsbeslutet.

Bestämmelsen motsvarar 6 § i lagen om elektroniska signaturer. Genom bestämmelsen genomförs artikel 3.4 punkt 1 i direktivet om ett gemenskapsramverk för elektroniska signaturer och kommissionens beslut om minimikriterier i fråga om kontrollorgan, som nämns ovan. I Finland har det tills vidare inte utsetts ett enda kontrollorgan.

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 §. I den finska versionen av den föreslagna lagen används, liksom i den gällande lagen, begreppet "laatuvarmenne" (kvalificerat certifikat), vilket motsvarar begreppet "hyväksytty varmenne" enligt definitionen i artikel 2.10 i direktivet. I paragrafen anges minimikraven för kvalificerade certifikat.

Ett kvalificerat certifikat ska enligt 2 mom. 1 punkten innehålla uppgift om att certifikatet är ett kvalificerat certifikat. Enligt 2 punkten ska det innehålla uppgift om certifikatutfärdaren och dennes etableringsstat. Etableringsstaten bestäms enligt var den ekonomiska verksamheten från ett fast verksamhetsställe de facto utövas. Om certifikatutfärdaren har många etableringsställen ska som etableringsstat betraktas den stat där centrumet för certifikatutfärdarens certifieringsverksamhet är beläget.

Undertecknarens namn ska enligt den föreslagna 3 punkten ingå i det kvalificerade certifikatets datainnehåll. Om namnet är en pseudonym, ska detta klart framgå av certifikatet.

Signaturverifieringsdata som motsvarar de signaturframställningsdata som undertecknaren innehar ska enligt den föreslagna 4 punkten utgöra en del av innehållet i det kvalificerade certifikatets datainnehåll. Inom systemet med öppna nycklar innebär detta att det i det kvalificerade certifikatets datainnehåll ska finnas en öppen nyckel som motsvarar den privata nyckeln.

Ett kvalificerat certifikat ska enligt den föreslagna 5 punkten innehålla uppgifter om certifikatets giltighetstid. Dessa uppgifter ska ange tidpunkten för både när certifikatet börjar gälla och när det upphör att gälla.

Ett kvalificerat certifikat ska enligt den föreslagna 6 punkten innehålla dess identifieringskod. En säker certifikatverksamhet förutsätter att certifikaten kan skiljas från varandra. Koden kan utgöras av ett löpande serienummer eller någon annan teckensträng som fungerar som identifieringskod.

Enligt den föreslagna 7 punkten ska certifikatutfärdarens avancerade elektroniska signatur ingå i det kvalificerade certifikatet. På så sätt garanteras det att certifikatets innehåll förblir oförändrat.

Eventuella begränsningar av certifikatets användningsområde eller av värdet på de transaktioner för vilka certifikatet kan användas ska enligt 8 punkten framgå av det kvalificerade certifikatet. Begränsningen kan gälla t.ex. det penningmässiga värdet av en rättshandling. Genom en sådan begränsning kan användningen av certifikatet också begränsas enbart till vissa rättshandlingar.

Enbart namnet räcker inte nödvändigtvis till för att identifiera undertecknaren tillräckligt entydigt. Särskilda uppgifter om undertecknaren ska enligt 9 punkten framgå av det kvalificerade certifikatet, om de behövs med tanke på ändamålet med det kvalificerade certifikatet. Sådana uppgifter kan vara t.ex. en uppgift om rätten att handla i något företags namn. Särskilda uppgifter kan också utgöras av någon av undertecknarens personuppgifter, t.ex. en av certifikatutfärdaren utfärdad identifieringskod.

I det föreslagna 3 mom. anges att om en certifikatutfärdare som tillhandahåller kvalificerade certifikat även tillhandahåller tjänster för stark autentisering enligt 3 kap., anses kraven i 1 mom. alltid också uppfylla de krav som gäller certifikatets innehåll i 19 § 1 mom. Genom bestämmelsen säkerställer man att datainnehållet i certifikat som tillhandahålls av en och samma tjänsteleverantör inte är föremål för sinsemellan motstridiga krav.

Genom paragrafen genomförs definitionen i artikel 2.10 i direktivet och bilaga I till direktivet. Genom bestämmelsen i 2 mom. 3 punkten genomförs dessutom artikel 8.3 i direktivet. Den föreslagna paragrafen motsvarar 7 § i lagen om elektroniska signaturer.

31 §. *Kvalificerade certifikat som tillhandahålls av en certifikatutfärdare som inte är etablerad i Finland.* I den föreslagna paragrafen föreslås bestämmelser om de förutsättningar under vilka ett certifikat som anges vara kvalificerat och som tillhandahålls av en certifikatutfärdare som inte är etablerad i Finland anses uppfylla kraven på kvalificerat certifikat enligt lagen. Certifikatet ska uppfylla åtminstone de krav som anges i det föreslagna 30 § 2 mom.

Enligt 1 mom. 1 punkten ska som kvalificerade certifikat erkännas sådana certifikat som tillhandahållits av en certifikatutfärdare som är etablerad i en annan stat inom EES-området. Utöver detta krävs att det certifikat som certifikatutfärdaren tillhandahållit uppfyller etableringsstatens krav på kvalificerat certifikat.

Enligt 2 punkten ska som kvalificerade certifikat erkännas sådana certifikat som tillhandahållits av certifikatutfärdare som har anslutit sig till ett frivilligt ackrediteringssystem i en annan stat inom EES-området och uppfyller de nationella krav som i denna stat föreskrivits för genomförande av direktivet om ett gemenskapsramverk för elektroniska signaturer. Det kan finnas många frivilliga ackrediteringssystem och det är frivilligt att ansluta sig till och höra till sådana system.

Enligt den föreslagna 3 punkten ska som kvalificerade certifikat erkännas sådana certifikat som garanteras av en certifikatutfärdare som är etablerad i en medlemsstat inom Europeiska ekonomiska samarbetsområdet och uppfyller de nationella krav som i denna stat föreskrivits för genomförande av direktivet om ett gemenskapsramverk för elektroniska signaturer.

Enligt den föreslagna 4 punkten anses ett certifikat som tillhandahållits av certifikatutfärdaren uppfylla kraven på kvalificerat certifikat om certifikatet eller certifikatutfärdaren har erkänts enligt ett bilateralt eller multilateralt avtal mellan Europeiska gemenskapen och ett eller flera tredjeländer eller internationella organisationer.

Genom bestämmelsen genomförs artikel 7.1 i direktivet. Bestämmlsen motsvarar 8 § i lagen om elektroniska signaturer.

32 §. *Anmälan om inledande av verksamhet*. Enligt paragrafens 1 mom. ska en certifikatutfärdare som avser att tillhandahålla allmänheten kvalificerade certifikat göra en anmälan till Kommunikationsverket innan verksamheten börjar. Anmälan ska göras skriftligen. Av anmälan ska framgå certifikatutfärdarens namn och kontaktuppgifter samt de uppgifter som behövs för att säkerställa att kraven i 30 § och 33—38 § uppfylls. Kommunikationsverket kan även i fortsättningen meddela behövliga föreskrifter eller rekommendationer om hur de uppgifter som ska uppges lämnas in och om det närmare innehållet i dem. Kommunikationsverket har den 29 januari 2003 med stöd av den gällande lagen meddelat en föreskrift om skyldighet för certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat att göra anmälan om sin verksamhet till Kommunikationsverket (7/2003 M). Enligt det föreslagna 50 § 2 mom. ska föreskriften gälla tills Kommunikationsverket utfärdar nya föreskrifter med stöd av den föreslagna lagen.

Enligt 2 mom. förutsätter inledandet av verksamhet för att tillhandahålla kvalificerade certifikat inte något förhandsgodkännande av Kommunikationsverket, men Kommunikationsverket ska efter att ha fått anmälan utan dröjsmål på det sätt som anges i 2 mom. förbjuda tillhandahållandet av certifikat som anges vara kvalificerade, om kraven gällande kvalificerade certifikat eller certifikatutfärdaren inte uppfylls. Förbudet gäller endast rätten att tillhandahålla certifikat som kvalificerade certifikat. Exempelvis får datainnehållet i ett certifikat inte innehålla uppgifter om det kvalificerade certifikatet. I övrigt kan certifikatutfärdaren fortsätta sin verksamhet trots förbudet och tillhandahålla andra än kvalificerade certifikat.

En certifikatutfärdare som tillhandahåller sina certifikat som kvalificerade certifikat ansvarar likväl alltid i egenskap av utfärdare av kvalificerade certifikat enligt detta lagförslag för sådana eventuella skador som kan uppstå när ett certifikat som inte uppfyller

kraven på kvalificerade certifikat används som ett kvalificerat certifikat. Kommunikationsverket ska med beaktande av anmälarens intressen och det skadeståndsansvar som påförts den certifikatutfärdare som tillhandahåller kvalificerade certifikat agera omedelbart i ärendet för att certifikatutfärdaren så snabbt som möjligt ska få besked från Kommunikationsverket till stöd för sin affärsverksamhet.

Certifikatutfärdaren ska enligt det föreslagna 3 mom. också omedelbart underrätta Kommunikationsverket om uppgifterna i anmälan ändras. Enligt lagförslaget ska Kommunikationsverket på det sätt som framgår av 5 kap. utöva tillsyn över de certifikatutfärdare som tillhandahåller kvalificerade certifikat. För att kunna utföra sina tillsynsuppgifter behöver Kommunikationsverket tillräckliga och korrekta uppgifter om de certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat.

I det föreslagna 4 mom. anges att Kommunikationsverket för ett offentligt register över certifikatutfärdare som utfärdar kvalificerade certifikat. Registret innehåller bl.a. uppgifter om certifikatutfärdarens namn och adress i den form utfärdaren har meddelat dem till Kommunikationsverket. Från registret ska man få uppgifter om de certifikatutfärdare som till Kommunikationsverket har anmält att de tillhandahåller kvalificerade certifikat i Finland. Uppgifterna i registret ska emellertid endast vara av informativ karaktär. Enligt den föreslagna 41 § ansvarar en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat för eventuella skador som verksamheten orsakar en tredje part, oberoende av om certifikatutfärdaren i fråga har införts i Kommunikationsverkets register eller inte.

I 5 mom. anges att certifikatutfärdare som tillhandahåller kvalificerade certifikat också kan göra en anmälan enligt 10 §, om de utöver kvalificerade certifikat även vill tillhandahålla identifieringstjänster. Bestämmelsen behövs av tydlighetsskäl.

Genom bestämmelsen genomförs artikel 3.1 och delvis artikel 3.3 i direktivet. Bestämmelsen motsvarar 9 § i lagen om elektroniska signaturer.

33 §. *Allmänna skyldigheter för certifikatutfärdare som tillhandahåller kvalificerade certifikat*. Paragrafen innehåller bestämmelser om de allmänna skyldigheterna för certifikatutfärdare som tillhandahåller kvalificerade certifikat. Enligt 1 mom. svarar den som tillhandahåller kvalificerade certifikat, dvs. den vars namn uppges i certifikatet, för alla delområden av verksamheten, även då en del av de tjänster och produkter som tillhandahålls köps av underleverantörer. Uppgifter som utförs av personer som certifikatutfärdaren anlitar kan vara t.ex. mottagande av certifikatansökningar, skapande av certifikat samt underhåll av spärrlistor.

Certifikatutfärdaren ska också ha tillräckliga tekniska kunskaper och ekonomiska resurser med tanke på verksamhetens omfattning. För att visa att verksamheten bedrivs på ett omsorgsfullt och tillförlitligt sätt ska certifikatutfärdaren bl.a. bedöma de tekniska och ekonomiska risker som hänför sig till verksamheten och vidta de åtgärder som behövs för att minimera dessa risker. Kravet på omsorgsfullhet och tillförlitlighet inbegriper också dokumentation av de förfaranden som certifikatutfärdaren tillämpar.

Enligt 2 mom. 1 punkten ska en certifikatutfärdare anställa personal som har tillräcklig sakkunskap, erfarenhet och kompetens. Certifikatutfärdaren ska alltså se till att de anställda, och särskilt de är i en ledande ställning, har sådan sakkunskap, erfarenhet och kompetens som certifieringsverksamheten kräver. Personalen ska ha tillräcklig sakkunskap om bl.a. tekniken för elektroniska signaturer och om datasäkerhetsfrågor.

Enligt den föreslagna 2 mom. 2 punkten ska certifikatutfärdaren se till att det finns tillräckliga ekonomiska resurser för att ordna verksamheten samt med tanke på eventuella skadeståndsansvar. Vad som är tillräckligt ska bedömas i förhållande till certifieringsverksamhetens omfattning. Även om certifikatutfärdaren har en tillräckligt omfattande ansvarsförsäkring för att täcka skadeståndsansvar, ska utfärdaren också i övrigt förfoga över tillräckliga ekonomiska resurser för att bedriva en tillförlitlig certifieringsverksamhet.

Enligt 2 mom. 3 punkten ska certifikatutfärdaren se till att sådana uppgifter om certifikaten och certifikatverksamheten som be-

hövs för att bedöma certifikatutfärdarens verksamhet och tillförlitlighet hålls allmänt tillgängliga. Certifikatutfärdarens kunder samt de instanser som förlitar sig på certifikaten ska ha tillgång till tillräckliga uppgifter om certifikatutfärdarens verksamhet för att på basis av dem kunna bedöma om certifikatet är tillräckligt tillförlitligt för deras behov. Kravet i 3 punkten kan uppfyllas med hjälp av t.ex. certifikatpolicy och ett meddelande om certifieringsstandard.

Certifikatpolicyn består av ett dokument med stöd av vilket certifikatutfärdaren utfärdar certifikat och som användaren ska känna till och godkänna. I dokumentet fastställs reglerna för certifikatutfärdarens verksamhet och utgående från dem kan det bedömas hur certifikatet lämpar sig för en viss tillämpning. Dokumentet över certifikatpolicyn svarar på vad en certifikatutfärdare gör och ställer sålunda krav på certifikatutfärdarens verksamhet och ledning. Flera certifikatutfärdare kan ha en gemensam certifikatpolicy. Exempelvis har European Telecommunications Standards Institute (ETSI) fastställt en miniminivå för den grundläggande certifikatpolicyn för de certifikatutfärdare som tillhandahåller kvalificerade certifikat.

Certifikatutfärdaren ska också tillhandahålla dokumentation över den certifieringsstandard (Certificate Practise Statement, nedan CPS) som tillämpas inom den egna organisationen. Standarden är en mera detaljerad beskrivning av hur certifikatutfärdaren tillämpar certifikatpolicyn inom sin organisation. Med hjälp av certifieringsstandarden kan t.ex. utomstående instanser kontrollera om certifikatutfärdaren uppfyller de krav som anges i policyn.

De uppgifter som föreslås i 3 punkten ska finnas allmänt tillgängliga. Uppgifterna anses finnas allmänt tillgängliga bl.a. då de kan hämtas på certifikatutfärdarens verksamhetsställe eller finns att tillgå på certifikatutfärdarens webbplats på Internet.

Enligt den föreslagna 4 punkten ska certifikatutfärdaren säkerställa att signaturframställningsdata är konfidentiella då certifikatutfärdaren själv framställer dem. Certifikatutfärdaren ska försäkra sig om att signaturframställningsdata överlåts endast till personer som är berättigade att förfoga över dem.

Enligt 3 mom. får certifikatutfärdaren inte heller lagra eller kopiera de signaturframställningsdata som överlåtits till en undertecknare. Att signaturframställningsdata förvaras endast hos undertecknaren är väsentligt för att tillförlitligheten hos den elektroniska signaturen ska kunna bibehållas. Därför föreskrivs det att certifikatutfärdaren inte får lagra eller kopiera signaturframställningsdata. Om signaturframställningsdata förkommer eller förstörs kan undertecknaren alltid begära att få nya signaturframställningsdata av certifikatutfärdaren. I sådana fall ligger det i undertecknarens intresse att utan dröjsmål göra en sådan anmälan som avses i 36 §.

Genom bestämmelsen genomförs punkterna a, e, g, h och j i bilaga II till direktivet. Bestämmelsen motsvarar i regel 10 § i lagen om elektroniska signaturer. I den föreslagna paragrafen har man dock slopat de delar som innehöll hänvisningar till offentliga förvaltningsuppgifter.

34 §. *Tillförlitliga maskinvaror och programvaror*. De system samt maskinvaror och programvaror som en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat använder ska enligt paragrafens 1 mom. vara tillräckligt säkra och tillförlitliga samt skyddade mot ändringar och mot förfalskning. Med tillräckligt säker och tillförlitlig avses en så stor tillförlitlighet som möjligt som kan uppnås genom användning av de bästa möjliga tekniska lösningarna. Systemen och deras delar ska vara skyddade på så sätt att endast sådan personal som certifikatutfärdaren särskilt utsett kan göra ändringar i dem. Ändringarna ska dessutom registreras automatiskt och uppgifterna om dem bevaras även i sådana fall att ändringarna eventuellt orsakas av utomstående eller av fel i maskinvaran.

I 2 mom. föreskrivs att en maskinvara eller programvara som överensstämmer med de allmänt erkända standarder som har fastställts av Europeiska gemenskapernas kommission och publicerats i Europeiska gemenskapernas officiella tidning alltid ska anses uppfylla kraven i 1 mom.

Genom bestämmelsen genomförs artikel 3.5 i direktivet och punkt f i bilaga II till direktivet. Bestämmelsen motsvarar 11 § i lagen om elektroniska signaturer.

35 §. *Utgivning av kvalificerade certifikat*. Enligt 1 mom. ska en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat omsorgsfullt och på ett tillförlitligt sätt kontrollera den sökandes identitet och andra uppgifter som gäller sökandens person och som är relevanta för utgivningen och upprätthållandet av det kvalificerade certifikatet. Uppgifter som hänför sig till sökandens person kan vara åtminstone sökandens namn och adressuppgifter samt de uppgifter enligt 30 § 2 mom. som finns i datainnehållet i ett kvalificerat certifikat, inklusive särskilda uppgifter som eventuellt hänför sig till en viss användning av certifikatet. Terminologin i den föreslagna paragrafen har ändrats jämfört med den gällande lagen så, att kvalificerade certifikat inte beviljas utan i stället ges ut. Ändringen beror på att kvalificerade certifikat inte längre är förknippade till utövning av offentlig makt.

Certifikatutfärdare som tillhandahåller kvalificerade certifikat ska identifiera sökanden personligen. Med att identifiera sökanden personligen avses att sökanden, då denne ansöker om det kvalificerade certifikatet, personligen ska besöka certifikatutfärdaren för identifiering. Kontrollen av sökandens identitet på ett tillförlitligt sätt kan ske med hjälp av en tillförlitlig handling som sökanden lägger fram. Som tillförlitliga handlingar kan betraktas de handlingar som avses i den föreslagna 17 §. I den förslagna 6 § föreskrivs om behandling av personuppgifter.

En certifikatutfärdare som tillhandahåller kvalificerade certifikat bekräftar genom en avancerad elektronisk signatur som tas in i det kvalificerade certifikatet att uppgifterna i det kvalificerade certifikatet gäller en viss person. Efter att certifikatet överlåtits kontrolleras undertecknarens identitet i allmänhet inte. Då certifikatet ges ut överlåts också unika signaturframställningsdata till undertecknaren. Den som verifierar signaturen känner nödvändigtvis inte den undertecknare som använder signaturframställningsdata, utan förlitar sig på certifikatutfärdarens identifiering och på de uppgifter som certifikatutfärdaren infört i det kvalificerade certifikatet. Därför är det särskilt viktigt att sökandens identitet kontrolleras på ett tillförlitligt sätt och att man försäkrar sig om att de uppgifter som tagits in i det kvalificerade certifikatet är korrekta samt att det kvalificerade certifikatet överlåts till en person som är berättigad att förfoga över det. Certifikatutfärdaren ansvarar enligt bestämmelserna i den föreslagna 41 § bl.a. för att de uppgifter som införts i det kvalificerade certifikatet är korrekta vid den tidpunkt då certifikatet utfärdades och att det kvalificerade certifikatet överlåts till en person som är berättigad att förfoga över det. Tidpunkten för certifikatets utfärdade anses enligt detaljmotiveringen till 41 § vara den tidpunkt då det överlåts till sökanden.

Innan ett avtal ingås ska certifikatutfärdaren enligt det föreslagna 2 mom. informera sökanden om villkoren för användning av certifikatet, inbegripet eventuella begränsningar av användningen, och om frivilliga ackrediteringssystem, myndighetstillsynen över verksamheten samt förfarandena för klagomål och avgörande av tvister. Uppgifter som ska ingå i villkoren för användning av certifikatet är bl.a. uppgifter om användning av eventuella katalogtjänster samt i synnerhet återkallande av kvalificerade certifikat och införande av certifikat på spärrlistan. Villkoren för användningen ska också omfatta uppgifter om certifikatutfärdarens skadeståndsansvar och andra skyldigheter.

Den som ansöker om ett certifikat ska också informeras om den tillsyn Kommunikationsverket och dataskyddsombudsmannen utövar över certifikatutfärdaren samt om sökandens rätt att hänskjuta ett ärende som gäller verksamhet som bedrivs av en i lagen avsedd certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat till Kommunikationsverket.

Uppgifterna ska ges den som ansöker om ett kvalificerat certifikat skriftligen i sådan form att sökanden utan svårighet förstår dem. Det kan anses att information i elektronisk form som är allmänt läsbar och kan lagras har getts skriftligen.

Genom bestämmelsen genomförs punkterna d och k i bilaga II till direktivet. Bestämmelsen motsvarar i regel 12 § i lagen om elektroniska signaturer, men i bestämmelsen har slopats de delar som innehåller hänvisningar till utövning av offentlig makt.

36 §. *Återkallande av kvalificerat certifikat*. Med tanke på certifieringsverksamhetens sä-

kerhet och tillförlitlighet är det viktigt att obehörig användning av ett kvalificerat certifikat kan förhindras i ett så tidigt skede som möjligt. Om signaturframställningsdata t.ex. har stulits eller förkommit, är det viktigt att undertecknaren omedelbart begär att certifikatutfärdaren återkallar det kvalificerade certifikatet. Skadorna blir då så små som möjligt.

Det föreslås att det i 1 mom. ska föreskivas om en uttrycklig skyldighet för undertecknaren att begära att certifikatutfärdaren återkallar ett kvalificerat certifikat, om undertecknaren har grundad anledning att anta att signaturframställningsdata kan användas på obehörigt sätt. Certifikatutfärdaren ska enligt 2 mom. omedelbart återkalla ett kvalificerat certifikat, om undertecknaren begär det. Certifikatutfärdaren ska återkalla ett kvalificerat certifikat genom att införa uppgifter om certifikatet på en spärrlista som avses i 37 § 3 mom. Undertecknaren behöver inte motivera sin begäran.

En begäran om återkallande anses ha inkommit då begäran finns tillgänglig för certifikatutfärdaren i en sådan form att den kan behandlas. När det gäller ett meddelande i elektronisk form innebär detta den tidpunkt då begäran är tillgänglig i den mottagarapparat eller i det datasystem som certifikatutfärdaren använder.

Certifikatutfärdaren kan enligt det föreslagna 3 mom. också återkalla ett certifikat om det finns särskild anledning till det. En särskild anledning kan vara t.ex. undertecknarens död eller något annat tvingande skäl. En sådan särskild anledning kan också vara att certifikatutfärdarens verksamhet upphör. Dessutom kan certifikatutfärdaren återkalla ett certifikat om undertecknaren bryter mot det avtal som ingåtts med certifikatutfärdaren eller använder certifikatet i strid med dess syfte.

Enligt 3 mom. ska undertecknaren alltid underrättas om att ett kvalificerat certifikat har återkallats och om tidpunkten för återkallandet. Detta är nödvändigt för att undertecknaren ska kunna försäkra sig om att begäran om återkallande har lyckats eller om ett eventuellt återkallande som gjorts på certifikatutfärdarens initiativ.

I 40 och 41 § föreskrivs om det skadeståndsansvar som gäller certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat och om obehörig användning av signaturframställningsdata.

Bestämmelsen motsvarar 13 § i lagen om elektroniska signaturer.

37 §. *Register som ska föras av certifikatutfärdare som tillhandahåller kvalificerade certifikat*. En certifikatutfärdare som tillhandahåller kvalificerade certifikat har enligt punkt b i bilaga II till direktivet om ett gemenskapsramverk för elektroniska signaturer ålagts skyldighet att garantera driften av ett snabbt och säkert system för registrering och för säkert och omedelbart återkallande. I punkt i i bilaga II till direktivet förutsätts dessutom att en certifikatutfärdare som tillhandahåller kvalificerade certifikat ska registrera all relevant information om ett kvalificerat certifikat under en lämplig tidsperiod, särskilt för att vid rättsliga förfaranden kunna lägga fram bevis om utfärdande av certifikatet.

Genom bestämmelsen om register som förs av certifikatutfärdare som tillhandahåller kvalificerade certifikat strävar man efter att garantera att de tjänster som på ett betydande sätt hänför sig till användningen av kvalificerade certifikat ska vara tillgängliga på ett så effektivt och tillförlitligt sätt som möjligt. Det är uttryckligen med hjälp av dessa tjänster som certifikatutfärdaren handlar som en tillförlitlig tredje part genom att med ett kvalificerat certifikat för mottagaren av meddelandet verifiera giltigheten hos de signaturframställningsdata som gäller den som sänt meddelandet och den som undertecknat det. I den föreslagna paragrafen samt i den föreslagna 38 § föreskrivs också om de uppgifter som ska lagras och om förvaringen av uppgifterna.

En certifikatutfärdare som tillhandahåller kvalificerade certifikat ska enligt 1 mom. föra register över utfärdade certifikat (certifikatregister). I registret ska utöver det datainnehåll i ett kvalificerat certifikat som anges i 30 § 2 mom. införas de uppgifter om sökandens person som avses i 35 § 1 mom., inbegripet en uppgift om det förfarande för identifiering av sökanden som tillämpats då det

kvalificerade certifikatet utfärdades. I registret ska dessutom föras in de i 39 § avsedda uppgifter om kontroll av certifikatets giltighet som gjorts på spärrlistan, om en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat utnyttjar rätten att registrera kontrolluppgifterna på spärrlistan enligt 39 §.

En certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat kan således lagra t.ex. uppgifter om vilken handling som använts vid identifieringen och även lagra de relevanta uppgifterna i denna handling. En sådan relevant uppgift kan utgöras av t.ex. passets nummer eller personbeteckningen. En certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat kan även t.ex. ta fotokopior av de handlingar som använts vid identifieringen. Det väsentliga vid lagringen av uppgifter är det krav på verifiering av en omsorgsfull och tillförlitlig identifiering som ställs på certifikatutfärdare som tillhandahåller kvalificerade certifikat. Eftersom certifikatutfärdare har ett i 41 § definierat strängt skadeståndsansvar för att uppgifterna i de kvalificerade certifikat som utfärdats är korrekta, ska certifikatutfärdarna också ha möjlighet att vid behov bevisa att de har handlat på ett omsorgsfullt sätt. Det är nödvändigt att uppgifterna om kontroll av ett kvalificerat certifikat lagras med tanke på t.ex. faktureringen av användningen av certifikatet och utredningen av eventuella tvister. Närmare bestämmelser om användningen av uppgifterna om kontroll finns i 39 §.

En certifikatutfärdare som tillhandahåller kvalificerade certifikat ska enligt 2 mom. säkerställa att den som förlitar sig på en avancerad elektronisk signatur som är baserad på ett kvalificerat certifikat har tillgång till certifikatets datainnehåll enligt vad som anges i 30 § 2 mom. Avsikten är inte att närmare bestämma på vilket sätt uppgifterna ska vara tillgängliga för de parter som förlitar sig på signaturen. Certifikatutfärdaren kan beroende på vilka tekniska tillämpningar som används uppfylla kravet på det ändamålsenligaste sättet. Om man i ett avtal mellan undertecknaren och certifikatutfärdaren har kommit överens om att undertecknaren själv tillsammans med ett meddelande även lämnar ut det kvalificerade certifikatet, kommer certifikatets innehåll till den parts kännedom som förlitat sig på det utan att certifikatutfärdaren behöver vidta några särskilda åtgärder. I sådana fall behövs det inte några särskilda tjänster som tillhandahålls av certifikatutfärdaren. Certifikatutfärdaren och undertecknaren kan också komma överens om att certifikatutfärdaren ur certifikatregistret överlåter de uppgifter i datainnehållet som anges i 30 § 2 mom. till den instans som förlitar sig på signaturen. Det som är väsentligt med tanke på tillförlitligheten hos elektroniska signaturer är att den part som förlitar sig på signaturen får kännedom om uppgifterna i datainnehållet i det kvalificerade certifikatet.

En certifikatutfärdare som tillhandahåller kvalificerade certifikat ska enligt det föreslagna 3 mom. också se till att på spärrlistan införs på ett lämpligt sätt och utan dröjsmål uppgifter om certifikat som återkallats och om den exakta tidpunkten för återkallandet. Undertecknarens ansvar för obehörig användning av signaturframställningsdata upphör i regel när han eller hon hos certifikatutfärdaren har begärt att det kvalificerade certifikatet återkallas i enlighet med den föreslagna 36 §. Ansvaret för användningen av signaturframställningsdata under tiden från det att undertecknaren begär att ett certifikat återkallas fram till det att certifikatet införs på spärrlistan vilar på certifikatutfärdaren. Därför torde det ligga i certifikatutfärdarens eget intresse att snabbt föra in uppgifterna på spärrlistan. Närmare bestämmelser om obehörig användning av signaturframställningsdata finns i 40 §.

Spärrlistan ska vara ett offentligt register, eftersom den part som förlitar sig på en signatur endast har spärrlistan att tillgå för att kunna konstatera att ett certifikat har återkallats. På spärrlistan kan t.ex. föras in endast identifieringskoden för ett kvalificerat certifikat. I sådana fall kommer spärrlistan inte att innehålla uppgifter som hänför sig till den person som besitter den avancerade elektroniska signatur som baserar sig på ett kvalificerat certifikat. Om uppgifter som hänför sig till undertecknarens person förs in på spärrlistan, ska av undertecknaren inhämtas hans eller hennes uttryckliga samtycke till att uppgifterna förs in. Med tanke på den part som förlitar sig på ett visst kvalificerat certifikat

räcker det om parten med hjälp av det kvalificerade certifikatets identifieringskod kan kontrollera om det kvalificerade certifikatet i fråga har återkallats.

Uppgifterna enligt 30 § 2 mom. i det kvalificerade certifikatet samt spärrlistan ska enligt det föreslagna 4 mom. vara tillgängliga dygnet runt, eftersom datanäten möjliggör elektronisk kommunikation oberoende av tidpunkt på dygnet. Om certifikatutfärdaren ger ut de uppgifter som avses i 30 § 2 mom., ska tjänsten vara tillgänglig dygnet runt. Om undertecknaren själv ger ut det kvalificerade certifikatet finns det inget behov av några särskilda tjänster av certifikatutfärdaren, utan då kan det anses att datainnehållet i det kvalificerade certifikatet enligt 30 § 2 mom. är tillgängligt dygnet runt då det ges ut av undertecknaren. En spärrlista som förs av en certifikatutfärdare som tillhandahåller kvalificerade certifikat ska dock alltid vara tillgänglig dygnet runt.

Genom bestämmelsen genomförs punkterna b och c i bilaga II till direktivet. Bestämmelsen motsvarar 14 § i lagen om elektroniska signaturer.

38 §. *Förvaring av uppgifterna i certifikatregistret*. Enligt paragrafen är en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat skyldig att på ett tillförlitligt och ändamålsenligt sätt förvara de uppgifter som enligt det föreslagna 37 § 1 mom. ska införas i certifikatregistret i 10 år från det att det kvalificerade certifikatet upphörde att gälla. Uppgifterna kan också förvaras i elektronisk form.

Den långa förvaringstid på tio år som föreslås för uppgifterna i certifikatregistret är fortfarande nödvändig eftersom det är omöjligt att exakt uppskatta de eventuella problem som kan uppstå i anslutning till bevisningsfrågor och tillgången till bevisning, t.ex. i fråga om skador till följd av missbruk.

Vid förvaringen av uppgifter ska tillförlitliga system användas. Uppgifterna får registreras och ändras endast av sådana pålitliga personer som certifikatutfärdaren har bemyndigat för uppgiften. Dessutom ska de tekniska ändringar som kan äventyra säkerheten hos de uppgifter som lagras noteras av den instans som förvarar uppgifterna. Behandlingen av personuppgifter ska ske i enlighet med bestämmelserna i personuppgiftslagen. I det föreslagna 6 § 4 mom. finns en informativ hänvisning om att personuppgiftslagen ska tillämpas på alla certifikatutfärdares verksamhet.

Syftet med bestämmelserna i det föreslagna 2 mom. är att försöka undvika att certifikat som tillhandahålls av en och samma tjänsteleverantör och de system som hänför sig till certifikaten ska utsättas för motstridiga krav. I det föreslagna 2 mom. konstateras att om en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat också tillhandahåller identifieringstjänster, kan tjänsteleverantören oberoende av vad som föreskrivs i 24 § förvara uppgifterna till alla delar på det sätt som avses i 1 mom.

Genom bestämmelsen genomförs punkterna i och l i bilaga II till direktivet. Paragrafens 1 mom. motsvarar 15 § i den gällande lagen om elektroniska signaturer.

39 §. *Registrering av uppgift om kontroll av certifikats giltighet.* Enligt paragrafen ska en certifikatutfärdare som tillhandahåller kvalificerade certifikat ha rätt att registrera uppgifter om kontroll av certifikatets giltighet. Uppgifterna kan användas endast för att fakturera användningen av certifikat eller för att verifiera rättshandlingar som företagits med hjälp av en elektronisk signatur som baserar sig på ett certifikat.

Det är nödvändigt att en uppgift om kontroll registreras i synnerhet med tanke på eventuella skadeståndskrav som riktas till certifikatutfärdarna. En certifikatutfärdare ska kunna registrera uppgifterna om kontroll av ett certifikats giltighet för att i synnerhet vid tvister om rättshandlingar kunna visa huruvida spärrlistan har kontrollerats och om det vid den tidpunkten har funnits uppgifter om återkallande av certifikatet på spärrlistan. Uppgiften om kontroll kan överlåtas åtminstone till undertecknaren och den som kontrollerat spärrlistan. De som vid eventuella tvister drar nytta av att uppgifterna registreras är förutom certifikatutfärdaren också parterna i en rättshandling, dvs. undertecknaren och den part som förlitat sig på signaturen.

Det är också möjligt att man för användningen av certifikat kommer att fakturera den part som kontrollerat certifikatets giltighet. Även i detta fall är det naturligtvis nödvän-

digt att den som tillhandahåller certifikat har uppgifter om att faktureringen har skötts på ett ändamålsenligt sätt.

Genom att begränsa användningen av uppgifter om kontroll av ett certifikats giltighet endast till de syften som nämns i paragrafen strävar man efter att förhindra att uppgifter om enskilda personers eller företags användning av certifikat samlas in.

I direktivet om ett gemenskapsramverk för elektroniska signaturer finns det inte någon bestämmelse som motsvarar den föreslagna paragrafen. Genom bestämmelserna i paragrafen preciseras behandlingen av uppgifter om kontroll av ett certifikats giltighet på nationell nivå. Den föreslagna paragrafen motsvarar 21 § i lagen om elektroniska signaturer.

40 §. *Ansvar för obehörig användning av signaturframställningsdata*. I den föreslagna paragrafen regleras undertecknarens ansvar för skada som orsakats av obehörig användning av signaturframställningsdata.

Som obehörig användning av signaturframställningsdata betraktas utöver användningen av förkomna eller stulna signaturframställningsdata även användningen av signaturframställningsdata i en sådan situation där den som förfogar över signaturframställningsdata ursprungligen har haft tillstånd att få signaturframställningsdata i sin besittning, men använder dem efter det att undertecknaren har förbjudit innehavaren att använda signaturframställningsdata eller när innehavarens rätt att använda signaturframställningsdata annars har upphört.

Obehörig användning av signaturframställningsdata kan delvis jämställas med obehörig användning av kreditkort eller någon annan motsvarande identifikation. Därför är det motiverat att man i lagen tar in ansvarsbestämmelser med principiellt samma innebörd. I praktiken är den största skillnaden i förhållande till t.ex. användningen av kreditkort den att användningen av signaturframställningsdata, beroende på vilken teknik som används, kommer att skyddas med t.ex. ett lösenord eller en identifieringskod, t.ex. en PIN-kod. I framtiden kan signaturframställningsdata skyddas med t.ex. fingeravtrycksidentifikation. Jämfört med användningen av kreditkort kommer användningen av signaturframställningsdata då att vara tryggare, vilket också försvårar obehörig användning.

Enligt huvudbestämmelsen i 1 mom. ansvarar undertecknaren för skada som orsakats av obehörig användning av signaturframställningsdata tills en begäran om återkallande har inkommit till certifikatutfärdaren i enlighet med 36 § 2 mom. Det har inte någon betydelse på vilket sätt någon som inte har rätt att använda signaturframställningsdata har fått nämnda data.

Eftersom det vore oskäligt att tillämpa den stränga huvudregel som anges i 1 mom. på konsumenter, föreskrivs det i 2 mom. om de begränsningar som ska tillämpas på konsumenter.

Enligt 2 mom. 1 punkten kan en konsument bli tvungen att ansvara för sådana rättshandlingar som någon annan person obehörigt har utfört med hans eller hennes signaturframställningsdata, om konsumenten har överlåtit signaturframställningsdata till någon annan. Med överlåtelse avses frivillig överlåtelse av besittningen, oberoende av i vilket syfte överlåtelsen sker.

Enligt 2 mom. 2 punkten kan en konsument bli ansvarig i ett sådant fall där signaturframställningsdata har åtkommits av någon som är obehörig att använda dem och detta beror på sådan vårdslöshet från konsumentens sida som inte är lindrig. Utgångspunkten är den att undertecknaren omsorgsfullt ska förvara signaturframställningsdata och det lösenord eller den identifieringskod som hänför sig till användningen av signaturframställningsdata. Vid bedömningen av vårdslöshet bör man fästa uppmärksamhet vid på vilket sätt signaturframställningsdata och lösenordet eller identifieringskoden har förvarats samt på vilket sätt besittningen av dem har förlorats. Vid bedömningen av vårdslöshet bör man också beakta syftet med den elektroniska signaturen samt de eventuella begränsningar av användningen som framgår av det kvalificerade certifikatet.

Eftersom det i princip är möjligt att utföra vilken rättshandling som helst med en avancerad elektronisk signatur som baserar sig på ett kvalificerat certifikat och som skapats med en säker anordning för signaturframställning, kan också ett eventuellt missbruk ha omfattande följder. Å andra sidan kan de

begränsningar av användningen som antecknats i det kvalificerade certifikatet vara av betydelse när konsumentens vårdslöshet bedöms. Ju färre begräsningar av användningen som har antecknats i det kvalificerade certifikatet, desto noggrannare kan förvaringen av konsumentens signaturframställningsdata förväntas vara. Vid bedömning av vårdslösheten ska det även beaktas att användningen av signaturen i princip hänför sig till flera t.o.m. dagligen återkommande åtgärder, och därför bör undertecknaren kunna ha signaturframställningsdata med sig. Därför bör det vara möjligt att t.ex. i plånboken ha med sig ett aktivkort med signaturframställningsdata.

Dessutom ska det vid bedömningen av undertecknarens vårdslöshet särskilt beaktas hans eller hennes agerande när det gäller att på ett omsorgsfullt sätt förvara det lösenord eller den kod som är avsedd att skydda användningen av signaturframställningsdata. Ett lösenord eller en kod får inte förvaras tillsammans med signaturframställningsdata. När det gäller att förhindra obehörig användning av signaturframställningsdata kommer det att vara ytterst viktigt att undertecknaren är omsorgsfull vid förvaringen av lösenordet eller koden.

I 2 mom. 3 punkten föreskrivs om sådana situationer där undertecknaren har förlorat besittningen till signaturframställningsdata på ett sådant sätt att undertecknaren inte över huvud taget kan anses ha gjort sig skyldig till vårdslöshet eller att hans eller hennes vårdslöshet har varit lindrig. Enligt 3 punkten kan undertecknaren bli ansvarig för skador som orsakats av sådana rättshandlingar som utförts av en person som obehörigt använt signaturframställningsdata endast om han eller hon har underlåtit att utan dröjsmål begära att det kvalificerade certifikatet ska återkallas så som anges i 36 § 1 mom. Syftet med bestämmelsen i den föreslagna 3 punkten är att skydda konsumenten, som kan anses ha gjort sig skyldig till högst lindrig vårdslöshet i och med att signaturframställningsdata har hamnat hos en person som inte har rätt att använda dem. I de fall som avses i 3 punkten ansvarar undertecknaren för skador som orsakats av obehörig användning av signaturframställningsdata med början från den tidpunkt då undertecknaren kan anses ha försummat den begäran om återkallande av ett kvalificerat certifikat som avses i 36 § 1 mom. Utgångspunkten är att undertecknaren ska begära att det kvalificerade certifikatet återkallas omedelbart när han eller hon upptäcker att signaturframställningsdata har försvunnit.

I direktivet om ett gemenskapsramverk för elektroniska signaturer finns det inte någon bestämmelse som motsvarar den föreslagna paragrafen. Genom bestämmelserna i paragrafen är det nödvändigt att på nationell nivå precisera riskfördelningen i fråga om obehörig användning av signaturframställningsdata. Paragrafen motsvarar 17 § i lagen om elektroniska signaturer.

41 §. *Skadeståndsansvar för certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat*. Användningen av elektroniska signaturer grundar sig i hög grad på att användaren har förtroende för certifikatutfärdarens verksamhet. I praktiken kan det vara svårt för andra än certifikatutfärdaren att lägga fram bevis i anslutning till eventuella problem som uppstår vid användningen av elektroniska signaturer samt orsaken till dessa. För den som har lidit skada kan det vara svårt eller t.o.m. omöjligt att bevisa vårdslöshet eller försummelse i certifikatutfärdarens verksamhet. I direktivet om ett gemenskapsramverk för elektroniska signaturer förutsätts det därför att det ansvar som ålagts en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat regleras så att det är strängare än det normala ansvaret vid vårdslöshet. Den uttryckliga bestämmelsen om grunderna för skadeståndsansvar underlättar även certifikatutfärdarens möjligheter att bedöma de skadeståndsrisker som hänför sig till verksamheten och att ordna verksamheten därefter.

Paragrafens bestämmelser gäller endast certifikatutfärdarens skadeståndsansvar i förhållande till en sådan person som förlitat sig på det kvalificerade certifikatet och som inte står i avtalsförhållande till certifikatutfärdaren. I fråga om förhållandet mellan certifikatutfärdaren och undertecknaren bestäms skadeståndsansvaret i regel enligt de allmänna principerna om avtalsrättsligt skadeståndsansvar. I den föreslagna 40 § föreskrivs särskilt om fördelningen av risken

mellan certifikatutfärdaren och undertecknaren i fall av obehörig användning av signaturframställningsdata.

I 1 mom. föreskrivs om de omständigheter som omfattas av det skadeståndsansvar för certifikatutfärdare som tillhandahåller kvalificerade certifikat som är strängare än det normala ansvaret för vårdslöshet. Certifikatutfärdaren är skyldig att ersätta skador som beror på omständigheter som anges i 1-5 punkten, om inte certifikatutfärdaren kan visa att skadan inte har orsakats av vårdslöshet hos utfärdaren själv eller någon som denne har anlitat. Någon som certifikatutfärdaren anlitar kan vara både en fysisk och en juridisk person. En certifikatutfärdares skadeståndsansvar gäller alla skador vilka står i orsakssamband med den omständighet som orsakat skadan i enlighet med de allmänna skadeståndsrättsliga principer som gäller skadans förutsebarhet.

Enligt 1 mom. 1 och 2 punkten är en certifikatutfärdare som tillhandahåller kvalificerade certifikat skyldig att ersätta en skada som uppkommit genom att de uppgifter som antecknats i det kvalificerade certifikatet var felaktiga vid den tidpunkt då certifikatet utfärdades eller att det kvalificerade certifikatet inte innehåller de uppgifter som nämns i 30 § 2 mom. Med tidpunkten för certifikatets utfärdande avses den tidpunkt då det kvalificerade certifikatet överlåts till sökanden. Det ligger i undertecknarens intresse att omedelbart underrätta certifikatutfärdaren om eventuella förändringar som skett i de uppgifter som lämnats vid tidpunkten för utfärdandet för att utfärdaren ska kunna utfärda ett nytt kvalificerat certifikat som motsvarar de förändrade uppgifterna.

Enligt 1 mom. 3 punkten svarar en certifikatutfärdare som tillhandahåller kvalificerade certifikat för skada som uppkommit genom att den person som anges i det kvalificerade certifikatet inte vid den tidpunkt då certifikatet utfärdades var i besittning av de signaturframställningsdata som motsvarar signaturverifieringsdata. Tillförlitligheten hos elektroniska signaturer grundar sig på det faktum att signaturframställningsdata endast används av den person vars namn anges i det kvalificerade certifikatet. I problemsituationer ska certifikatutfärdare som tillhandahåller kvalificerade certifikat för att undvika skadeståndsansvar kunna visa att de har förfarit omsorgsfullt då de på ett tillförlitligt sätt enligt 35 § 1 mom. har kontrollerat sökandens identitet. Dessutom ska de visa att de har överlåtit signaturframställningsdata till en person som är berättigad att besitta nämnda data. Om den som ansöker om ett kvalificerat certifikat eller någon annan än certifikatutfärdaren framställer signaturframställningsdata, och de signaturverifieringsdata som motsvarar dessa antecknas i det kvalificerade certifikatet, ska certifikatutfärdaren innan det kvalificerade certifikatet överlåts försäkra sig om att sökanden har nämnda signaturframställningsdata i sin besittning.

Enligt 1 mom. 4 punkten svarar certifikatutfärdaren för skada som orsakats av att signaturframställningsdata och signaturverifieringsdata inte kan användas som komplement till varandra. Kravet på att signaturframställningsdata och signaturverifieringsdata ska vara kompatibla med varandra är en nödvändig förutsättning för användningen av elektroniska signaturer. I punkten föreskrivs endast om sådana fall i vilka en certifikatutfärdare som tillhandahåller kvalificerade certifikat eller en person som denna anlitar har framställt både signaturframställningsdata och signaturverifieringsdata. Om den som ansöker om ett kvalificerat certifikat själv har framställt eller på något annat sätt inhämtat signaturframställningsdata och signaturverifieringsdata och endast anlitar certifikatutfärdaren för andra tjänster, är certifikatutfärdaren inte ansvarig för kompatibiliteten hos data.

Enligt 1 mom. 5 punkten svarar certifikatutfärdaren för skada som orsakats den som förlitat sig på ett kvalificerat certifikat, om certifikatet inte har återkallats på det sätt som anges i 36 §. Den tredje parten, dvs. den som verifierar den elektroniska signaturen, ska kunna lita på att certifikatet är giltigt och att det är i den persons besittning som är berättigad till det, om inte certifikatet har återkallats och införts på den spärrlista som certifikatutfärdaren upprätthåller över återkallade kvalificerade certifikat. Om signaturframställningsdata förkommer eller förstörs förhindrar ett omedelbart återkallande av det kvalificerade certifikatet effektivt uppkomsten av

skador. Det skadeståndsansvar som regleras i punkten gäller tiden efter det att undertecknarens begäran om återkallande av certifikatet har inkommit. Fram till dess att en begäran om återkallande har inkommit till certifikatutfärdaren ansvarar undertecknaren med de begränsningar som följer av 40 § för de skador som uppkommit.

Så som det har konstaterats ovan är det vid användningen av elektroniska signaturer och certifikat ytterst viktigt att spärrlistan är tillförlitlig. Av denna anledning kan det anses att det ligger i en sådan omsorgsfull parts intresse som förlitar sig på ett kvalificerat certifikat att försäkra sig om att spärrlistan kontrolleras. Eftersom en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat inför den som förlitar sig på ett certifikat enbart är ansvarig för att återkalla certifikatet, dvs. för att en uppgift om det kvalificerade certifikatet införs på spärrlistan, behöver den som förlitar sig på det kvalificerade certifikatet inom ramen för kravet på omsorgsfullhet endast kontrollera spärrlistan. Kontrollen av spärrlistan kan dock också göras automatiskt mellan de system som används av certifikatutfärdaren och den som förlitar sig på det kvalificerade certifikatet, vilket innebär att den som förlitar sig på certifikatet inte personligen kontrollerar spärrlistan. Den som förlitar sig på certifikatet ska även i detta fall hos den som upprätthåller det system som anlitas försäkra sig om att kontrollen av spärrlistan alltid sker automatiskt. Beroende på de tekniska tillämpningar som används kan olika förfaranden tillämpas för att kontrollera spärrlistan, men utgångspunkten är den att de som förlitar sig på ett kvalificerat certifikat ska se till att kontrollera spärrlistan för att de ska kunna försäkra sig om att det kvalificerade certifikatet är giltigt.

Enligt det föreslagna 2 mom. är en certifikatutfärdare som tillhandahåller kvalificerade certifikat befriad från det ansvar som anges i 1 mom., om utfärdaren kan visa att skadan inte har orsakats av vårdslöshet hos utfärdaren själv eller någon som denne har anlitat. Detta s.k. presumtiva ansvar för vållande innebär ett undantag från den skadeståndsrättsliga huvudregel enligt vilken den skadelidande är skyldig att visa att den som har orsakat skadan har handlat vårdslöst. Den omvända bevisbörda som anges i momentet gäller endast grunden för ansvaret, och därför är den skadelidande skyldig att på normalt sätt lägga fram bevis för ett orsakssamband mellan certifikatutfärdarens verksamhet och den skada han eller hon lidit.

Enligt det föreslagna 3 mom. ansvarar en certifikatutfärdare som tillhandahåller kvalificerade certifikat inte för skada som orsakats av att ett kvalificerat certifikat har använts i strid med de begränsningar av användningen som ingår i det. Användningen av ett kvalificerat certifikat kan begränsas av olika skäl. Ett kvalificerat certifikat kan t.ex. vara tillgängligt endast för vissa rättshandlingar eller endast för rättshandlingar som understiger ett visst penningbelopp. Exempelvis en arbetsgivare kan begränsa användningen av ett kvalificerat certifikat som utfärdats till en arbetstagare så att det endast gäller arbetsuppgifter.

Med tanke på certifikatutfärdarnas riskhantering är det viktigt att de inte blir ansvariga för sådan användning som står i strid med begränsningarna av användningen. För att begränsningarna av användningen ska vara effektiva i förhållande till tredje parter förutsätts det att begränsningen kommer till de tredje parternas kännedom. Begränsningarna av användningen ska enligt den föreslagna 30 § 2 mom. 8 punkten synas i det kvalificerade certifikatet på så sätt att de alltid förmedlar information även till den som verifierar signaturen.

På det skadeståndsansvar som föranleds av verksamheten hos en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat tillämpas utöver den föreslagna lagen dessutom skadeståndslagen (412/1974). För tydlighetens skull föreslås det att en bestämmelse om detta ska ingå i det föreslagna 4 mom.

Till den del ansvaret för en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat grundar sig på omständigheter som nämns i 1 mom., ska i skadeståndslagen tillämpas bl.a. bestämmelserna om jämkning av skadestånd, den skadelidandes medverkan, solidariskt ansvar då flera är ansvariga för skadan samt preskribering av skadeståndskravet.

Till övriga delar ska skadeståndsansvaret för certifikatutfärdare som tillhandahåller kvalificerade certifikat i förhållande till en sådan instans som har förlitat sig på det kvalificerade certifikatet och till vilken certifikatutfärdaren inte står i avtalsförhållande i sin helhet fastställas i enlighet med skadeståndslagen och de allmänna skadeståndsrättsliga principerna.

I det föreslagna 4 mom. föreskrivs också att skadeståndsregleringen enligt den föreslagna paragrafen ska utvidgas att gälla certifikatutfärdare som garanterar att ett certifikat är ett kvalificerat certifikat. I direktivet om ett gemenskapsramverk för elektroniska signaturer förutsätts det att medlemsstaterna åtminstone försäkrar sig om att det skadeståndsansvar som nämns i 1 mom. 1-4 punkten även utvidgas att gälla certifikatutfärdare som för allmänheten garanterar att ett certifikat är ett kvalificerat certifikat. I lagförslaget föreslås det att utöver ansvarsgrunderna enligt 1 mom. 1-4 punkten ska dessutom ansvarsgrunden enligt 5 punkten om underlåtenhet att återkalla ett certifikat tillämpas på certifikatutfärdare som för allmänheten garanterar att ett certifikat är ett kvalificerat certifikat. För att undvika missförstånd på ett svårt tekniskt område är det motiverat att reglera det ansvar som ålagts den som garanterar ett certifikat så att det i sin helhet är enhetligt med det ansvar som ålagts certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat.

Genom paragrafen genomförs artikel 6 i direktivet som gäller det skadeståndsansvar som ålagts certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat eller certifikatutfärdare som för allmänheten garanterar att ett certifikat är ett kvalificerat certifikat inför personer som har rimlig anledning att förlita sig på det kvalificerade certifikatet. Det i artikeln använda begreppet "som har rimlig anledning att förlita sig på" (who reasonably relies on) är ett okänt begrepp i den finländska gällande skadeståndslagen och skadeståndspraxisen. I den föreslagna paragrafen föreskrivs det sålunda om skadeståndsansvaret för certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat vad beträffar skada som orsakats den som förlitat sig på det kvalificerade certifikatet. Eftersom det i artikel 6 i direktivet endast bestäms om minimikrav för medlemsstaterna, är en nationell reglering i överensstämmelse med den föreslagna paragrafen möjlig. Med anledning av minimiregleringen enligt direktivet är det också möjligt att nationellt bestämma att ansvarsgrunden enligt 1 mom. 5 punkten även ska tillämpas på certifikatutfärdare som garanterar att ett certifikat är ett kvalificerat certifikat, fastän direktivet nödvändigtvis inte förutsätter detta. Bestämmelsen motsvarar 16 § i den gällande lagen om elektroniska signaturer.

5 kap. Myndighetstillsyn

42 §. *Allmän styrning och tillsyn*. Enligt det föreslagna 1 mom. omfattar kommunikationsministeriets allmänna styrnings- och utvecklingsrätt utöver elektroniska signaturer även elektronisk identifiering. I 22 § 1 mom. i den gällande lagen om elektroniska signaturer anges att den allmänna styrningen samt utvecklandet av certifikatverksamheten ankommer på kommunikationsministeriet. Den föreslagna ändringen i förhållande till nuläget är en naturlig följd av det förändrade tillämpningsområdet för den föreslagna lagen.

På samma sätt som i fråga om elektroniska signaturer innebär den allmänna styrningen och utvecklingen av elektronisk identifiering i första hand beredning av lagstiftningsprojekt som hänför sig till elektronisk identifiering samt deltagande i den verksamhet i anslutning till elektronisk identifiering som bedrivs inom Europeiska gemenskapernas institutioner.

Enligt 2 mom. ska Kommunikationsverket övervaka efterlevnaden av lagen med undantag av 1 § 3 mom. Kommunikationsverket meddelar vid behov tekniska föreskrifter om kraven på tillförlitlighet och informationssäkerhet i verksamhet som bedrivs av leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller kvalificerade certifikat. Föreskrifterna och rekommendationerna är förknippade med endast ringa tillämpning av prövningsrätten och genom dem preciseras vid behov innehållet i de krav som gäller tjänsteleverantörernas verksamhet enligt de föreslagna 3 och 4 kap. Möjligheten att utfärda närmare tekniska föreskrifter är

nödvändig eftersom det kan antas att branschen utvecklas kontinuerligt under de kommande åren.

Kommunikationsverket har med stöd av motsvarande bestämmelse i den gällande lagen om elektroniska signaturer den 29 januari 2003 meddelat en föreskrift om krav på tillförlitlighet och informationssäkerhet i verksamhet av certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat (8/2003 M). Enligt 50 § 2 mom. gäller också denna föreskrift till dess att Kommunikationsverket har utfärdat en ny föreskrift med stöd av lagen.

Enligt det föreslagna 4 mom. övervakar dataombudsmannen efterlevnaden av bestämmelserna om behandling av personuppgifter i den föreslagna lagen.

I 5 mom. konstateras det att konsumentombudsmannen ska övervaka tillhandahållande av tjänster enligt 1 § 2 mom. när en sammanslutning tillämpar en egen metod för stark autentisering för att identifiera sina egna kunder i de egna tjänsterna. Det är alltså fråga om sådant tillhandahållande av tjänster som inte egentligen hör till lagens tillämpningsområde. Enligt andra meningen i det föreslagna 1 § 2 mom. ska på sådan verksamhet dock tillämpas bestämmelserna i 3 §, 20 § 1 mom., 21-22 §, 23 § 1 mom., 25 § 1 mom. och sista meningen i 25 § 2 mom. samt 27 § 1 mom., 2 mom. 1 punkten och 3 mom. Bestämmelsen är en följd av behovet att skydda konsumenterna också i fråga om sådana tjänster. Därför är det naturligt att det är just konsumentmyndigheten som övervakar bestämmelsen. Konsumentombudsmannen ska vara behörig i ärendet också i enlighet med sina allmänna befogenheter, men det finns anledning att ta upp en tydlig bestämmelse om detta i lagen.

Genom 42-49 § genomförs också artikel 3.3 i direktivet om ett gemenskapsramverk för elektroniska signaturer. Den föreslagna 42 § motsvarar delvis 22 § i lagen om elektroniska signaturer.

43 §. *Rätt till information*. I paragrafen bestäms om tillsynsmyndigheternas rätt till information. I 1 mom. fastställs det att Kommunikationsverket utan hinder av bestämmelserna om tystnadsplikt har rätt att av leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller kvalificerade certifikat samt av dem som dessa leverantörer eller utfärdare anlitar få den information som behövs för att fullgöra de uppgifter som anges i 42 §. Med dem som leverantören eller utfärdaren anlitar avses både fysiska och juridiska personer.

Enligt 2 mom. har dataombudsmannen i sitt uppdrag rätt att få information enligt personuppgiftslagen. Enligt 39 § 1 mom. i personuppgiftslagen har dataombudsmannen utan hinder av sekretessbestämmelserna rätt att få information om de personuppgifter som är föremål för behandling samt all den information som behövs för att övervaka att behandlingen av personuppgifter sker i enlighet med lag.

I övrigt motsvarar bestämmelsen 23 § i lagen om elektroniska signaturer, men till den har även fogats en rättighet för dataombudsmannen att få all den information som denna behöver för att fullgöra sina uppgifter.

44 §. *Myndighetssamarbete och rätt att lämna ut information.* I paragrafen ges Kommunikationsverket och dataombudsmannen utan hinder av sekretessbestämmelserna i lagen om offentlighet i myndigheternas verksamhet (621/1999) rätt att lämna ut sådan information till Finansinspektionen som den behöver för att fullgöra sina uppgifter.

Kommunikationsverket har det tekniska kunnande som behövs om omständigheter som gäller elektronisk identifiering och elektroniska signaturer. Därför ska de egentliga identifieringstjänsterna och tjänsterna i anslutning till elektroniska signaturer uttryckligen övervakas av Kommunikationsverket. Däremot ska den verksamhet som reglerar det sätt på vilket bankerna använder identifieringskoder i sin bankverksamhet övervakas av Finansinspektionen.

För Finansinspektionens del är det inte möjligt och med tanke på helheten inte heller förnuftigt att den skaffar sig kunnande om stark autentisering och elektroniska signaturer i syfte att uppfylla sitt eget tillsynsansvar. Därför är det nödvändigt att det i den föreslagna paragrafen bestäms om myndighetssamarbetet i denna fråga.

I 24 § i lagen om offentlighet i myndigheternas verksamhet finns en förteckning med

32 punkter om handlingar som är sekretessbelagda. Av dessa kan t.ex. uppgifter som gäller skyddsarrangemang för data- och kommunikationssystem enligt 7 punkten och handlingar som innehåller uppgifter som en privat affärs- eller yrkeshemlighet enligt 20 punkten komma på fråga.

Enligt det föreslagna 2 mom. ska Kommunikationsverket och dataombudsmannen när de utför uppgifter enligt lagen samarbeta på lämpligt sätt med Finansinspektionen, Konkurrensverket och Konsumentverket. I lagstiftningen finns det ett stort antal motsvarande bestämmelser som förpliktar till myndighetssamarbete.

Den föreslagna paragrafen ersätter 25 § om tystnadsplikt i lagen om elektroniska signaturer. Ändringen är en följd av att ingenting i den föreslagna lagen kan betraktas som utövning av offentlig makt.

45 §. *Förvaltningstvångsmedel*. Enligt 1 mom. kan Kommunikationsverket i egenskap av den myndighet som övervakar efterlevnaden av lagen ålägga den som bryter mot lagen eller mot föreskrifter som har utfärdats med stöd av den att rätta sitt fel eller sin försummelse. Kommunikationsverket kan förena sitt beslut med vite, hot om avbrytande av verksamheten eller hot om tvångsutförande. Ett beslut om åläggande och ett beslut som förenas med hot kan meddelas samtidigt eller separat.

Kommunikationsverkets tillsynsbehörighet omfattar tillhandahållandet av identifieringstjänster, som också kan inbegripa tillhandahållandet av tjänster för elektroniska signaturer, tillhandahållandet av kvalificerade certifikat samt verksamhet som bedrivs av kontrollorgan som eventuellt utses senare. Ett hot om avbrytande av verksamheten kan gälla en del av eller hela den verksamhet som omfattas av lagen. Hot som förenas med ett åläggande ska alltid stå i proportion till det fel eller den försummelse som den som tillsynen gäller har gjort sig skyldig till. Vite eller tvångsutförande ska vara primära åtgärder som förenas med ett åläggande. Hot om avbrytande av verksamheten ska i regel enbart utnyttjas i sådana situationer där den som tillsynen gäller inte har rättat felet eller försummelsen trots vite eller hot om tvångsutförande.

Den tillsyn som utövas på dem som tillhandahåller identifieringstjänster för Kommunikationsverkets räkning består i tämligen hög grad av tillsyn i efterhand.

Paragrafens 2 mom. innehåller en sedvanlig bestämmelse om betalning av kostnaderna för en åtgärd som vidtagits på den försumliges bekostnad och som betalts av statens medel samt om indrivningen av dem.

46 §. *Inspektionsrätt*. I paragrafen föreskrivs om inspektion av leverantörer av identifieringstjänster och av certifikatutfärdare som tillhandahåller kvalificerade certifikat och av tjänster som dessa tillhandahåller. Inspektionerna skiljer sig på ett väsentligt sätt från varandra. Kommunikationsverket utför eller låter utföra inspektionen.

Enligt 1 mom. har Kommunikationsverket rätt att utföra eller låta utföra inspektioner av leverantörer av identifieringstjänster och av leverantörernas tjänster, om det finns skäl att misstänka att lagen eller de föreskrifter som har utfärdats med stöd av den inte iakttas. Med föreskrifter avses de föreskrifter som Kommunikationsverket meddelar med stöd av denna lag. Kommunikationsverkets tillsynsbehörighet, som riktar sig till bestämmelserna i det föreslagna 3 kap., verkställs sålunda i regel som tillsyn i efterhand.

Kommunikationsverket verkställer sin tillsynsbehörighet huvudsakligen med hjälp av de förvaltningstvångsmedel som anges i den föreslagna 45 §. Det nyaste och grövsta bland de olika medlen är den i det föreslagna momentet angivna rätten att utföra eller låta utföra en inspektion av leverantörer av tjänster för stark autentisering eller av deras verksamhet, om det under processens gång finns skäl att misstänka att bestämmelserna i lagen inte iakttas. En sådan inspektion utförs alltså inte varje år eller för säkerhets skull. Kommunikationsverket kan enligt den planerade bestämmelsen också låta arbetet utföras av någon utomstående. Förseelsen ska vara väsentlig för att en i momentet avsedd inspektion ska kunna vidtas.

Med stöd av 2 mom. ska Kommunikationsverket årligen utföra eller låta utföra inspektioner av certifikatutfärdare som tillhandahåller kvalificerade certifikat och av deras tjänster. Avsikten är att certifikatutfärdare som tillhandahåller kvalificerade certifikat

och deras verksamhet således ska inspekteras regelbundet varje år utan att det finns skäl att misstänka brister eller försummelser i deras verksamhet. Den föreslagna bestämmelsen motsvarar den nuvarande situationen.

Enligt 3 mom. ska Kommunikationsverket förordna en inspektör att utföra inspektionen. Den som utför inspektionen har rätt att hos tjänsteleverantörer samt hos dem som dessa anlitar undersöka sådana maskinvaror och programvaror som kan vara av betydelse vid tillsynen över efterlevnaden av lagen och föreskrifter som meddelats med stöd av lagen.

I 4 mom. anges att leverantörer av tjänster för stark autentisering, 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. Denna skyldighet gäller inte lokaler som omfattas av hemfriden.

I 5 mom. föreskrivs om handräckning. Enligt momentet kan Kommunikationsverket få handräckning av polisen för att utföra inspektioner. I paragrafen avses med sådana personer som leverantörer av identifieringstjänster eller certifikatutfärdare som tillhandahåller kvalificerade certifikat anlitar både fysiska och juridiska personer.

I 6 mom. anges att dataombudsmannen vid fullgörandet av sina uppgifter har rätt att utöva tillsyn enligt personuppgiftslagen. Enligt 39 § 2 mom. i personuppgiftslagen har dataombudsmannen rätt att inspektera personregister. Dataombudsmannen och de sakkunniga som anlitas vid inspektioner har för inspektionen rätt att få tillträde till lokaler som den registeransvarige och den som handlar på dennes uppdrag har i sin besittning och i vilka personuppgifter behandlas eller personregister förs. De skall även ha tillgång till sådana upplysningar och anordningar som behövs för inspektionen. I lokaler som omfattas av hemfriden får inspektioner utföras endast om det i det aktuella fallet finns en specifik orsak att misstänka att bestämmelserna om behandling av personuppgifter har överträtts eller överträds. En inspektion ska utföras så att den inte i onödan vållar den registeransvarige olägenhet eller kostnader.

Den föreslagna bestämmelsen motsvarar delvis 24 § i lagen om elektroniska signaturer.

47 §. *Avgifter som ska betalas till Kommunikationsverket.* Enligt 1 mom. ska de leverantörer av identifieringstjänster eller sammanslutningar av leverantörer som har gjort en anmälan enligt 10 § årligen till Kommunikationsverket betala en tillsynsavgift på 12 000 euro per tjänsteleveratör. En sammanslutning av tjänsteleverantörer som har gjort anmälan behöver alltså betala endast en avgift.

Som det konstateras ovan i motiveringen till 46 § består den tillsyn som Kommunikationsverket utövar över leverantörer av tjänster för stark autentisering i hög grad av tillsyn i efterhand. Den årliga inspektionsavgiften följer av att Kommunikationsverket är tvunget att kontinuerligt upprätthålla sitt kunnande om stark autentisering samt att bemöta sådana tjänsteleverantörer som använder identifieringstjänster och sådana innehavare av identifieringsverktyg som eventuellt kontaktar verket.

Den tillsynsavgift som fastställs i det föreslagna momentet föreslås vara lika stor för alla, oberoende av tjänsteleverantörens omsättning och antalet identifieringsverktyg. På så sätt bestraffar systemet inte en ökning av antalet identifikatorer på marknaden. Nämnda belopp är synnerligen rimligt ur aktörernas synvinkel. Beloppet är så litet att om en aktör inte klarar av att betala det, torde inte heller kravet i 13 § 2 mom. om att en tjänsteleverantör ska ha tillräckliga ekonomiska resurser för att bedriva verksamhet uppfyllas.

Dessutom ska de leverantörer av identifieringstjänster och sammanslutningar av tjänsteleverantörer som har gjort en anmälan enligt 10 § betala en registreringsavgift på 5 000 euro till Kommunikationsverket. Registreringsprocessen är den fas som föranleder Kommunikationsverket i egenskap av tillsynsmyndighet mest arbete. Därför är det befogat att det föreskrivs om en särskild avgift för registrering. Avgiften betalas endast en gång.

Enligt paragrafens 2 mom. ska certifikatutfärdare som tillhandahåller kvalificerade certifikat årligen betala en inspektionsavgift på 40 000 euro till Kommunikationsverket. Be-

loppet av den gällande certifikatavgiften har grundat sig på antalet kvalificerade certifikat i omlopp. Grunden har kritiserats eftersom den har ansetts utgöra ett hinder för att utveckla affärsverksamheten. Också Statens revisionsverk har fäst uppmärksamhet vid detta. I den föreslagna lagen torde kostnaderna för tillsynen komma att delas av även andra aktörer, varför Befolkningsregistercentralens andel klart kan minskas. Eftersom den verksamhet som bedrivs av certifikatutfärdare som tillhandahåller kvalificerade certifikat enligt 46 § 2 mom. ska inspekteras årligen, ska avgiften vara klart högre än den avgift som tas ut hos leverantörerna av identifieringstjänster. De kvalificerade certifikaten och certifikatutfärdarna omfattas av en tämligen strikt reglering enligt EU:s direktiv om ett gemenskapsramverk för elektroniska signaturer. Därför är det motiverat att verksamheten även framöver ska inspekteras varje år.

I 3 mom. konstateras att registreringsavgiften och tillsynsavgiften motsvarar Kommunikationsverkets kostnader för att utföra uppgifterna enligt lagen, med undantag för de uppgifter som avses i 46 § 1 mom. Enligt bestämmelsen ska tillsynsavgiften betalas till fullt belopp även under det första verksamhetsåret, även om verksamheten inleds under året. Tillsynsavgiften återbetalas inte fastän tjänsteleverantören upphör med sin verksamhet under året.

Det går inte att visa på något tydligt vederlag från Kommunikationsverkets sida för de registreringsavgifter och tillsynsavgifter som avses i 1 och 2 mom. Därför är det fråga om avgifter av skattenatur, och regleringen av sådana måste uppfylla de krav som anges i skattelagstiftningen. I fråga om avgifter av skattenatur ska både grunden för och beloppet av avgiften fastställas på lagnivå. Paragrafens 1, 2 och 3 mom. uppfyller dessa krav. Motsvarande avgifter som tillämpas är bl.a. kommunikationsmarknadsavgiften och dataskyddsavgiften.

I 4 och 5 mom. finns ytterligare bestämmelser om verkställigheten och indrivningen av avgifter. Enligt det föreslagna 4 mom. påförs registreringsavgiften och tillsynsavgiften av Kommunikationsverket. Ändring i Kommunikationsverkets beslut om att påföra avgift får sökas i enlighet med 49 § 1 mom. Närmare bestämmelser om verkställigheten av avgifterna kan utfärdas genom förordning av kommunikationsministeriet.

I 5 mom. konstateras det att registreringsavgiften och tillsynsavgiften får drivas in utan dom eller beslut i den ordning som föreskrivs i lagen om verkställighet av skatter och avgifter. Om avgifterna inte betalas senast på förfallodagen, tas på det obetalda beloppet ut en årlig dröjsmålsränta enligt den räntefot som avses i 4 § 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.

I 6 mom. framhålls att om den verksamhet som bedrivs av en leverantör av identifieringstjänster ska inspekteras med stöd av 46 § 1 mom., tas kostnaderna för inspektionen ut av tjänsteleverantören enligt lagen om grunderna för avgifter till staten. Den inspektionsrätt som avses i det föreslagna 46 § 1 mom. är en följd av att Kommunikationsverket har anledning att misstänka att bestämmelserna i lagen inte iakttas. En sådan inspektion utförs alltså inte varje år eller för säkerhets skull. Kostnaderna för inspektionen betalas helt och hållet av tjänsteleverantören. Enligt 46 § 1 mom. kan Kommunikationsverket också låta arbetet utföras av någon utomstående.

6 kap. Särskilda bestämmelser

48 §. *Straffbestämmelser.* Med tanke på tillförlitligheten i tillhandahållandet av tjänster enligt den föreslagna lagen utgörs den viktigaste faktorn av behandlingen av personuppgifter i fråga om såväl identifieringstjänster som tjänster för tillhandahållandet av kvalificerade certifikat. Av tjänsteleverantörerna förutsätts det att de behandlar personuppgifter på ett tillförlitligt sätt. I den föreslagna lagen ingår flera bestämmelser om behandlingen av personuppgifter.

I den föreslagna paragrafen hänvisas det till vad som föreskrivs om personregisterbrott och personregisterförseelser. Hänvisningen är av informativ karaktär. Bestämmelsen motsvarar 26 § i lagen om elektroniska signaturer.

49 §. *Ändringssökande.* I beslut som Kommunikationsverket har fattat med stöd av lagen ska ändring enligt det föreslagna 1 mom. sökas i enlighet med vad som bestäms i förvaltningsprocesslagen (586/1996). Enligt 8 § 2 mom. i förvaltningsprocesslagen kan besvär anföras hos förvaltningsdomstolen.

Enligt det föreslagna 2 mom. kan Kommunikationsverket i sitt beslut bestämma att beslutet ska iakttas redan innan det har vunnit laga kraft. Besvärsmyndigheten kan dock förbjuda verkställigheten av beslutet tills besvären har avgjorts.

I 3 mom. anges att bestämmelser om sökande av ändring när det gäller dataombudsmannens verksamhet finns i personuppgiftslagen. Enligt 45 § 1 mom. i personuppgiftslagen får ändring även i beslut som dataombudsmannen fattat sökas genom besvär med iakttagande av vad som bestäms i förvaltningsprocesslagen. I 45 § 2 mom. i personuppgiftslagen finns motsvarande bestämmelse som i 2 mom. om att Kommunikationsverkets beslut ska iakttas trots att ändring har sökts.

Bestämmelsen motsvarar 22 § 4 mom. i lagen om elektroniska signaturer. Det kan anses vara författningstekniskt motiverat att bestämmelsen tas in i den aktuella paragrafen. Innehållet i bestämmelsen ändras inte trots att den flyttas.

7 kap. Ikraftträdande

50 §. *Ikraftträdande.* Paragrafen innehåller en ikraftträdandebestämmelse. Lagen avses träda i kraft den 1 september 2009.

I det föreslagna 2 mom. anges att genom lagen upphävs lagen om elektroniska signaturer (14/2003). De föreskrifter som Kommunikationsverket har utfärdat med stöd av lagen är dock i kraft tills nya föreskrifter har utfärdats med stöd av den nya lagen.

I det föreslagna 3 mom. anges på sedvanligt sätt att åtgärder som verkställigheten av lagen förutsätter får vidtas innan lagen träder i kraft.

51 §. *Övergångsbestämmelse*. Enligt 1 mom. ska leverantörer av tjänster för stark autentisering göra en anmälan enligt 10 § till Kommunikationsverket inom sex månader från lagens ikraftträdande. Som tjänster för stark autentisering och leverantörer av identifieringstjänster betraktas under denna tid tjänster för elektronisk identifiering som omfattas av tillämpningsområdet enligt 1 § och leverantörer av tjänster för elektronisk identifiering som uppfyller de definitioner som avses i 2 § 1 och 4 punkten. Bestämmelserna i lagen ska sålunda inte ännu tillämpas under nämnda övergångstid på sex månader. Det finns inte heller några centrala uppgifter om vem som är tjänsteleverantörer. En övergångstid är emellertid nödvändig för att tjänsteleverantörerna ska kunna utveckla sina tjänster så att de motsvarar kraven i lagen, vilket är en förutsättning för att göra en anmälan enligt 10 §.

Enligt 2 mom. ska identifieringsverktyg som har getts ut innan lagen trädde i kraft betraktas som verktyg för stark autentisering efter det att en tjänsteleverantör som tillhandahåller identifieringstjänster har gjort en anmälan som avses i 10 §. I praktiken innebär detta framför allt att bankernas gällande identifieringskoder enligt lagen ska betraktas som verktyg för stark autentisering efter det att den bank som har gett ut dem har gjort en anmälan enligt 10 § till Kommunikationsverket. Detta är en praktisk lösning som följer av att bankerna har gett ut mer än fyra miljoner identifieringskoder. Om det inte vore möjligt att med hjälp av en övergångsbestämmelse fortsätta använda koderna liksom hittills t.ex. då man identifierar sig för en elektronisk tjänst som tillhandahålls av den offentliga sektorn, skulle detta innebära ett synnerligen stort bakslag för den finländska informationssamhällsutvecklingen.

Enligt 2 mom. ska tjänsterna och tjänsteleverantörerna, då de gör anmälan, uppfylla alla lagens bestämmelser om identifieringstjänster och tillhandahållande av identifieringstjänster, med undantag för bestämmelserna i 17 §. Således ska alla andra förutsättningar uppfyllas, inklusive villkoret i 20 § 3 mom. om att identifieringsverktyg ska vara personliga.

I 3 mom. finns en bestämmelse för sådana situationer där leverantörerna av identifieringstjänster har ingått ett avtal enligt 17 § 2 mom. om möjligheten att lita på en inledande identifiering som en annan leverantör har

gjort och den tjänsteleverantör som har gett ut de identifieringsverktyg som använts vid den inledande identifieringen inte gör en anmälan enligt 10 § inom den fastställda övergångstiden på sex månader. Den leverantör av identifieringstjänster som har litat på en annan tjänsteleverantörs identifieringsverktyg ska i fråga om de identifieringsverktyg som getts ut på detta sätt göra den inledande identifieringen utan dröjsmål på det sätt som avses i 17 §.

I 4 mom. bestäms om övergången i fråga om certifikatutfärdare som tillhandahåller kvalificerade certifikat. En certifikatutfärdare som tillhandahåller kvalificerade certifikat och som har gjort en anmälan om elektroniska signaturer enligt 9 § 1 mom. och fortsatt verksamheten utan avbrott fram till ikraftträdandet av lagen behöver inte göra en ny anmälan enligt 32 § 1 mom. En certifikatutfärdare som tillhandahåller kvalificerade certifikat kan då lämna en fritt formulerad skriftlig anmälan till Kommunikationsverket om att verksamheten fortsätter oförändrad. Om samma tjänsteleverantör också tillhandahåller identifieringstjänster, innebär bestämmelsen självfallet inte att leverantörer befrias från skyldigheten att göra en anmälan enligt 10 §.

I 5 mom. bestäms om en övergångstid för en handling som ska godkännas vid den inledande identifieringen. Enligt bestämmelsen får leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller kvalificerade certifikat till och med den 31 december 2012 vid den inledande identifieringen använda ett giltigt körkort som har utfärdats efter den 1 oktober 1990 av en myndighet i en medlemsstat inom Europeiska ekonomiska samarbetsområdet.

Statsrådet har den 17 augusti 2006 gett en förordning om identitetshandlingar som utfärdas av polisen. I 1 § i förordningen anges att identitetshandlingar som utfärdas av polisen och som godkänns som identifieringshandling vid ansökan om identitetskort och pass är giltigt identitetskort enligt 1 § 1 och 3 mom. i lagen om identitetskort (829/1999) och giltigt pass enligt 3 § i passlagen (671/2006). Det är självfallet att några andra handlingar inte kan godkännas för detta ändamål.

Det praktiska läget i Finland är för närvarande att det i många andra situationer går att visa sin identitet med körkort. Cirka fyra miljoner finländare har ett pass eller ID-kort men alla är nödvändigtvis inte vana vid att ha dem med sig.

Tidigare nationella erfarenheter, liksom även vissa exempel från utlandet, visar att en viktig faktor som påverkar viljan hos människor att skaffa sig identifieringsverktyg är huruvida detta upplevs vara lätt eller komplicerat. Kravet på att körkortet inte ska duga som identifieringsverktyg försvårar detta förfarande väsentligt. Personer som inte har pass eller identitetskort är då tvungna att t.ex. först ansöka om pass eller identitetskort för att kunna få ett identifieringsverktyg.

Det finns ingen skyldighet att godkänna sådana körkort. Därför kan tjänsteleverantörerna själva välja vilka av de körkort som beviljats av myndigheterna i sådana stater de anser sig kunna godkänna. Det är klart att riskerna ökar i fråga om sådana körkort. Tjänsteleverantören måste bedöma vilka risker leverantören förmår ta på sig.

De största problemen i körkorten hänger samman med svagheten i beviljandeprocessen och säkerhetsfaktorerna. Användningen av körkort i identifieringen kommer troligen att minska avsevärt under de kommande åren i och med körkortsdirektivet 2006/126/EG som verkställs nationellt före den 19 januari 2013 och beviljandeprocessen av körkort som kommer att reformeras.

Med anledning av det ovan nämnda möjliggörs det i bestämmelsen användningen av körkort i den inledande identifieringen, men endast under en övergångstid.

I bestämmelsen har man uteslutit användningen av sådana körkort som är förknippade med de största riskerna för missbruk. Begränsningen gäller papperskörkort som har utfärdats före utgången av september 1990, som är mycket lätta att förfalska. Valet av år 1990 som gräns har således sina nationella skäl.

1.2 Lag om elektronisk kommunikation i myndigheternas verksamhet

3 §. *Annan lagstiftning.* Det föreslås att paragrafens 2 mom. ändras, eftersom avsikten

är att lagen om elektroniska signaturer ska upphävas samtidigt som lagen om stark autentisering och elektroniska signaturer träder i kraft. Hänvisningen till lagen om elektroniska signaturer ändras till en hänvisning till lagen om stark autentisering och elektroniska signaturer.

9 §. *Krav på skriftlig form och underskrift.* Paragrafens 1 mom. ändras så att det i stället för till 18 § i lagen om elektroniska signaturer hänvisas till 5 § 2 mom. i lagen om stark autentisering och elektroniska signaturer.

16 §. *Elektronisk signering av beslutshandlingar.* Paragrafen ändras så att det i stället för till 18 § i lagen om elektroniska signaturer hänvisas till 5 § 2 mom. i lagen om stark autentisering och elektroniska signaturer.

18 §. *Bevislig elektronisk delgivning.* Paragrafens 2 mom. ändras så att till momentet fogas ett uttryckligt omnämnande av att som godtagbart identifieringsverktyg ska anses ett identifieringsverktyg som avses i lagen om stark autentisering och elektroniska signaturer.

1.3 Befolkningsdatalag

19 §. *Certifierad elektronisk kommunikation.* Paragrafens 3 mom. ändras så att hänvisningen till lagen om elektroniska signaturer ändras till en hänvisning till lagen om stark autentisering och elektroniska signaturer.

20 §. *Uppgifter i certifikat för certifierad elektronisk kommunikation.* Paragrafen ändras så att det i stället för till 7 § i lagen om elektroniska signaturer hänvisas till 30 § i lagen om stark autentisering och elektroniska signaturer.

1.4 Lag om elektronisk behandling av klientuppgifter inom social- och hälsovården

2 §. *Tillämpningsområde.* Paragrafens 3 mom. ändras så att hänvisningen till lagen om elektroniska signaturer ändras till en hänvisning till lagen om stark autentisering och elektroniska signaturer.

9 §. *Elektronisk signering av handlingar.* Hänvisningen till lagen om elektroniska signaturer ändras till en hänvisning till lagen om stark autentisering och elektroniska signaturer.

1.5 Lag om kommunikationsförvaltningen

2 §. *Kommunikationsverkets uppgifter.* Paragrafens 1 punkt ändras så att hänvisningen till lagen om elektroniska signaturer ändras till en hänvisning till lagen om stark autentisering och elektroniska signaturer.

1.6 Lag om förhindrande och utredning av penningtvätt och av finansiering av terrorism

18 §. *Skärpta krav på kontroll vid identifiering på distans.* Paragrafens 3 punkt ändras så att till momentet fogas ett uttryckligt omnämnande av att som godtagbart verktyg för styrkande av identiteten ska anses ett identifieringsverktyg som avses i lagen om stark autentisering och elektroniska signaturer.

1.7 Lag om överlåtelseskatt

56 b §. *Elektronisk kommunikation och signering.* Ordalydelsen i paragrafens 2 mom. som ska ändras är relativt svår att tolka, eftersom det i momentet förutsätts en sådan elektronisk signatur som uppfyller kraven i lagen om elektroniska signaturer, utan att någon paragraf anges. Det föreslås att paragrafens 2 mom. ändras så att meddelanden och övriga handlingar där det krävs en underskrift ska i den elektroniska kommunikationen certifieras med en avancerad elektronisk signatur som avses i lagen om stark autentisering och elektroniska signaturer eller på något annat godtagbart sätt. Med certifiering hänvisas i detta moment allmänt till olika certifierings- och identifieringsmetoder som Skatteförvaltningen har godkänt enligt paragrafens 3 mom.

1.8 Lag om beskattningsförfarande

93 a §. *Elektronisk kommunikation och signering.* Det föreslås att paragrafens 2 mom. ändras så att meddelanden och övriga handlingar där det krävs en underskrift ska i den elektroniska kommunikationen cer-

tifieras med en avancerad elektronisk signatur som avses i lagen om stark autentisering och elektroniska signaturer eller på något annat godtagbart sätt. Med certifiering hänvisas i detta moment allmänt till olika certifierings- och identifieringsmetoder som Skatteförvaltningen har godkänt enligt paragrafens 3 mom.

1.9 Mervärdesskattelag

165 §. Det föreslås att paragrafens 3 mom. ändras så att meddelanden och övriga handlingar där det krävs en underskrift ska i den elektroniska kommunikationen certifieras med en avancerad elektronisk signatur som avses i lagen om stark autentisering och elektroniska signaturer eller på något annat godtagbart sätt. Med certifiering hänvisas i detta moment allmänt till olika certifierings- och identifieringsmetoder som Skatteförvaltningen har godkänt enligt paragrafens 4 mom.

1.10 Lag om förskottsuppbörd

6 a §. *Elektronisk kommunikation och signering.* Det föreslås att paragrafens 2 mom. ändras så att meddelanden och övriga handlingar där det krävs en underskrift ska i den elektroniska kommunikationen certifieras med en avancerad elektronisk signatur som avses i lagen om stark autentisering och elektroniska signaturer eller på något annat godtagbart sätt. Med certifiering hänvisas i detta moment allmänt till olika certifierings- och identifieringsmetoder som Skatteförvaltningen har godkänt enligt paragrafens 3 mom.

1.11 Blodtjänstlag

11 §. *Uppgifter som hänför sig till blodgivare.* Paragrafen ändras så att hänvisningen till lagen om elektroniska signaturer ändras till en hänvisning till lagen om stark autentisering och elektroniska signaturer.

2 Närmare bestämmelser och föreskrifter

Enligt 47 § 4 mom. i propositionen kan det genom förordning av kommunikationsministeriet utfärdas närmare bestämmelser om verkställigheten av tillsynsavgifter och registreringsavgifter om vilka det föreskrivs i 47 §.

Enligt 8 § 3 mom. i propositionen kan Kommunikationsverket vid behov utfärda närmare tekniska föreskrifter om uppfyllandet av de krav som gäller identifieringsmetoder och om vilka det föreskrivs i 8 § 1 mom.

Enligt 10 § 5 mom. i propositionen kan Kommunikationsverket meddela för tillsynen behövliga föreskrifter om det närmare innehållet i de uppgifter som ska anmälas och inlämnandet av dem till Kommunikationsverket.

I fråga om elektroniska signaturer har Kommunikationsverket motsvarande rättigheter att meddela föreskrifter som i lagen om elektroniska signaturer. Enligt 32 § 1 mom. i propositionen kan Kommunikationsverket meddela för tillsynen behövliga föreskrifter om det närmare innehållet i de uppgifter som ska lämnas och inlämnandet av dem till Kommunikationsverket.

Vidare enligt 42 § 2 mom. i lagförslaget meddelar Kommunikationsverket vid behov tekniska föreskrifter om kraven på tillförlitlighet och informationssäkerhet i verksamhet som bedrivs av leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller kvalificerade certifikat.

3 Ikraftträdande

Lagarna föreslås träda i kraft den 1 september 2009. Åtgärder som verkställigheten av lagarna förutsätter får vidtas innan lagarna träder i kraft. I 51 § i lagförslaget om stark autentisering och elektroniska signaturer ingår en övergångsbestämmelse där det sägs att leverantörer av identifieringstjänster ska göra en anmälan enligt 10 § till Kommunikationsverket inom sex månader från lagens ikraftträdande.

4 Förhållande till grundlagen samt lagstiftningsordning

4.1 Förhållande till grundlagen

Utövning av offentlig makt

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.

Grundlagsutskottet har behandlat överföringen av förvaltningsuppgifter på andra än myndigheter i t.ex. följande utlåtanden: GrUU 23/2000 rd (lotterilagen), GrUU 28/2001 rd (lagen om privata säkerhetstjänster), GrUU 52/2001 rd (lagen om tillsyn över finans- och försäkringskonglomerat), GrUU 53/2001 rd (lagen om affärsbanker och andra kreditinstitut), GrUU 2/2002 rd (lagen om elektroniska signaturer) samt GrUU 67/2002 rd (lagen om finansinspektionen).

Uppfattningen om att tillhandahållandet av certifieringstjänster bör anses som utövning av offentlig makt kommer troligen från regeringens proposition med förslag till lag om elektronisk kommunikation i förvaltningsärenden (RP 153/1999 rd). I propositionen ansågs det att verksamheten av en privat eller offentlig certifikatutfärdare ska likställas med verksamheten av den medelbara offentliga förvaltningen. Denna ståndpunkt motiverades med att beviljande av certifikatet gäller den sökandens intresse på det sätt som föreskrivs i regeringsformens 16 §. I förvaltningsutskottets betänkande (FvUB 10/1999 rd) godkände man den i regeringens proposition framförda synpunkten på certifieringsverksamhetens offentligrättsliga karaktär även om hörande av experter gav också motsatta opinioner.

I överensstämmelse med denna linje ansågs det i regeringens proposition om elektroniska signaturer att också verksamheten av privata tillhandahållare av kvalificerade certifikat handlar om utövning av offentlig makt. I grundlagsutskottets utlåtande (GrUU 2/2002 rd) har det enligt regeringens proposition konstaterats att på grund av sin rättsverkan måste tillhandahållande av kvalificerade certifikat betraktas som en offentlig förvaltningsuppgift i den mening som 124 § i grundlagen avser. I utlåtandet ansågs det att ett kvalificerat certifikat kan jämställas med ett identitetsbevis utfärdat av en myndighet, t.ex. med pass eller ID-kort. Certifieringsverksamheten ansågs således ha betydelse för parterna i elektronisk handel och annan elektronisk kommunikation och deras rättsliga ställning.

Synpunkterna som framfördes i de ovan nämnda regeringspropositionerna återger klart det sättet på vilket man uppfattade saken på 1990-talet då de elektroniska signaturerna hade utvecklats. Sedermera har både den praktiska utvecklingen och sättet att uppfatta fenomenet med vilket man nu hanterar förändrats.

I praktiken är situationen för närvarande den att marknaden för den elektroniska signaturen inte har börjat fungera i Finland och inte heller någon annanstans i världen. I Finland är det endast Befolkningsregistercentralen som tillhandahåller tjänster för den elektroniska signaturen och kvalificerade certifikat. De har ändå inte utbretts mycket.

På grund av denna faktiska situation har utvecklingen i stället för elektroniska signaturer gått mot utvecklingen av verktyg för elektronisk identifiering. I Finland tillhandahålls verktyg för stark autentisering av Befolkningsregistercentralen med sina certifikat som bygger på systemet med öppen nyckel och bankerna med sina bankkoder. Ca 99 % av alla identifieringar görs med bankkoder. Med anledning av detta utfärdade finansministeriet redan 2002 en anvisning att bankkoder kan användas också i statsförvaltningens elektroniska ärendehantering. Möjligheten till elektronisk ärendehantering hos en myndighet är således inte längre bunden till användningen av certifikat eller kvalificerade certifikat.

Även sättet att uppfatta detta fenomen har förändrats. Det sägs att den elektroniska identifieringen och den elektroniska signaturen handlar om skapande av en elektronisk identitet. För närvarande anser man att var och en kan ha bara en identitet. Denna identitet skapas när en människa föds och de personuppgifter som fogats till henne antecknas i befolkningsdatasystemet. I Finland är det polisen som fogar identiteten som tillkommit på detta sätt till officiella handlingar som visar identiteten. Med ett verktyg för stark au-

tentisering kan man verifiera personens identitet i en elektronisk värld men verktyget för stark autentisering kan ändå inte jämföras med ett officiellt ID-kort eller pass som utfärdas av polisen. Detta utreds som bäst djupgående i inrikesministeriets projekt för skapande av identitet, dvs. identitetsprogrammet.

Tillhandahållande av en tjänst för stark autentisering och certifikat är privat serviceutbud och det är inte nödvändigt att foga utövning av offentlig makt enligt grundlagens 124 § till dem. Inte ens verksamheten med kvalificerade certifikat är utövning av offentlig makt. Däremot är Befolkningsregistercentralens tillhandahållande av medborgarcertifikat utövning av offentlig makt. Denna verksamhet regleras i egen lag, lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster. Regeringens proposition om denna är som bäst i riksdagens behandling. I lagen föreskrivs bl.a. om ett speciellt förfarande för beviljande av medborgarcertifikat. En väsentlig del i detta förfarande är verifiering av identiteten som utförs av polisen. Även Statens revisionsverk har i sin rapport (161/2008) Utvecklandet och användningen av identifieringstjänster i den offentliga förvaltningen ansett att Befolkningsregistercentralens verksamhet med medborgarcertifikat handlar om myndighetsverksamhet medan annan utgivning av kvalificerade certifikat eller andra certifikat inte är det.

Den ovan beskrivna ändringen i betraktelsesättet klarlägger verksamhetsfältet väsentligt. I den föreslagna lagen föreskrivs det enbart om privat tjänstetillhandahållande. Utövningen av offentlig makt i tillhandahållandet av tjänster för elektroniska signaturer regleras i den nya befolkningsdatalagen. Jämfört med lagen om elektroniska signaturer stryks det samtidigt ur den föreslagna lagen vissa detaljer som hänvisar till utövning av offentlig makt. Sådana är t.ex. sekretessbestämmelser. I den föreslagna lagens terminologi kallas utgivningen av verktyg för stark autentisering eller kvalificerade certifikat inte heller beviljande utan utgivning.

Behandling av personuppgifter

Enligt grundlagens 10 § utfärdas bestämmelser om skydd för personuppgifter genom lag. Enligt regeringens proposition om reform av de grundläggande fri- och rättigheterna hänvisar bestämmelsen till behovet att genom lagstiftning trygga individens rättsskydd och skydd för privatlivet i behandlingen, registreringen och användningen av personuppgifter (RP 309/1993 rd, s. 53). Bestämmelsens laghänvisning om skydd för personuppgifter förutsätter enligt syftet med reformen av de grundläggande fri- och rättigheterna (GrUB 25/1994 rd, s. 6/I) att lagstiftarna utfärdar bestämmelser om denna rättighet, men den överlåter detaljerna i bestämmelserna på lagstiftarna.

Grundlagsutskottet har behandlat skyddet för personuppgifter bl.a. i sina utlåtanden GrUU 47/1996 rd (telemarknadslagen), GrUU 28/1997 rd (lagen om godkännande av vissa bestämmelser i konventionen om upprättandet av en europeisk polisbyrå och i protokollet till konventionen), GrUU 29/1997 rd (lagen om polisens personregister), GrUU 26/1998 rd (lagen om dataskydd i telekommunikation), GrUU 27/1998 rd och GrUU 27a/1998 rd (lagen om integritetsskydd i arbetslivet) och GrUU 25/1998 rd (personuppgiftslagen).

Utskottet har i sina utlåtanden allmänt betonat viktigheten av att lagens detaljerade bestämmelser är exakta. Enligt utskottets utlåtandepraxis omfattas även frågan om lagringstider för uppgifter som lagrats i personregister av kravet om lagstiftning som avses i det nämnda lagrummet i grundlagen. Viktiga frågor som ska regleras är åtminstone syftet med registreringen, innehållet i personuppgifter som registreras, tillåtna användningsändamål för dem inklusive möjligheten till överlåtelse och lagringstiden i personregistret samt den registrerades rättsskydd och omfattningen och utförligheten av bestämmelser som gäller detta på lagnivån.

Behandlingen av personuppgifter är naturligtvis en väsentlig faktor i tillhandahållandet av identifieringstjänsten och tjänster för elektronisk signatur. Grundläggande bestämmelser om behandlingen av personuppgifter finns i lagförslagets 6 och 7 §. De gäller alla

certifikatutfärdare som tillhandahåller elektroniska signaturer, dvs. också andra certifikatutfärdare än dem som tillhandahåller kvalificerade certifikat och även tillhandahållare av tjänster för stark autentisering. Bestämmelserna baserar sig på personuppgiftslagen och artikel 8.1 och 8.2 i direktivet om ett gemenskapsramverk för elektroniska signaturer.

Enligt den föreslagna 6 § 1 mom. får leverantörer av identifieringstjänster vid utgivningen och upprätthållandet av identifieringsverktyg samt vid identifieringstransaktioner behandla de personuppgifter som behövs. På samma grunder får certifikatutfärdare som tillhandahåller elektroniska signaturer behandla de personuppgifter som behövs vid utfärdandet och upprätthållandet av certifikat. Det föreslagna momentet uppfyller de krav om ändamålsbundenhet som ställs i 7 § i personuppgiftslagen.

Enligt det nämnda 6 § 1 mom. får behandlingen ske på de grunder som anges i 8 § 1 mom. 1 och 2 punkten i personuppgiftslagen. Detta innebär att personuppgifter endast får behandlas med den registrerades entydiga samtycke och på uppdrag av den registrerade eller för att fullgöra ett sådant avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.

Enligt paragrafens 1 mom. får leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller elektroniska signaturer dessutom inhämta personuppgifter från personen själv. Syftet med inhämtandet ska vara detsamma som annars i behandlingen.

Enligt paragrafens 2 mom. får personuppgifter behandlas i andra syften endast på de grunder som avses i 8 § 1 mom. i personuppgiftslagen. Orsaken till detta är att det i uppdragsgivandet eller avtalet inte är möjligt att förbereda sig för andra syften med tillräcklig noggrannhet.

I paragrafens 3 mom. föreskrivs om användningen av personbeteckningen. Enligt 13 § 1 mom. i personuppgiftslagen får en personbeteckning behandlas med personens entydiga samtycke eller när behandlingen regleras i lag. Dessutom får en personbeteckning behandlas, om det är nödvändigt att entydigt individualisera den registrerade för att uppfylla den registrerades eller den registeransvariges rättigheter och skyldigheter.

Behandlingen av personbeteckningen i samband med en identifieringstjänst och en certifieringstjänst som anknyter till elektroniska signaturer är nödvändigt därför att ett pålitligt utförande av tjänsterna uttryckligen förutsätter att personer kan med säkerhet skiljas från varandra. Detta är i och för sig en i 13 § 1 mom. i personuppgiftslagen nämnd omständighet som berättigar till behandlingen av personbeteckningen också utan en uttrycklig bestämmelse i lagen. Man har ändå velat ha klara bestämmelser om ärendet i paragrafen.

Enligt det föreslagna momentet får leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller elektroniska signaturer behandla personbeteckningar i sina register. Ändamålet för behandlingen ska vara detsamma som i 1 mom. Verktyg för stark autentisering och certifikat får innehålla personbeteckning enbart om verktygets eller certifikatets innehåll är tillgängligt endast för dem som nödvändigt behöver den för att tillhandahålla tjänsten. Personbeteckningen får ändå inte vara tillgänglig i en offentlig katalog.

I den föreslagna lagens 7 § föreskrivs om användningen av uppgifter i befolkningsdatasystemet. Enligt paragrafens 1 mom. får leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller elektroniska signaturer på de grunder som avses i 8 § 1 mom. 1 och 2 punkten i personuppgiftslagen inhämta och kontrollera de personuppgifter som har lagrats i befolkningsdataregistret om en sökande eller innehavare. Syftet med behandlingen är detsamma som i 6 §. Leverantörer av identifieringstjänster får vid utgivningen och upprätthållandet av identifieringsverktyg och vid identifieringstransaktioner alltså behandla de personuppgifter som behövs och certifikatutfärdare som tillhandahåller elektroniska signaturer får behandla de personuppgifter som behövs vid beviljandet och upprätthållandet av certifikat.

Behandlingen av uppgifter får också för denna del ske på de grunder som anges i 8 § 1 mom. 1 och 2 punkten i personuppgiftslagen. Det är alltså fråga om den registrerades entydiga samtycke, uppdrag av den registre-

rade, fullgörande av ett sådant avtal i vilket den registrerade är part eller vidtagande av åtgärder på begäran av den registrerade innan ett sådant avtal ingås.

I fråga om identifieringstjänster är 24 § en väsentlig paragraf beträffande behandlingen av personuppgifter. I den bestäms om registreringen och användningen av uppgifter om identifieringstransaktioner och om identifieringsverktyg. I paragrafens 1 mom. föreskrivs om uppgifter som ska registreras. Dessa uppgifter är de uppgifter som behövs för att verifiera en enskild identifieringstransaktion och elektronisk signering, de uppgifter som behövs om den inledande identifiering av en sökande och om den handling som anlitats för identifieringen, uppgifter om eventuella hinder och begränsningar för användningen av verktyget för stark autentisering, och i fråga om certifikat uppgifter om certifikatets innehåll.

I paragrafens 2 mom. föreskrivs om förvaringstiden. I fråga om uppgifter om identifieringstransaktioner är tiden fem år från identifieringstransaktionen och i fråga om övriga registrerade uppgifter 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 enligt 3 mom. förstöras efter transaktionen, om det inte är nödvändigt att registrera dem för att verifiera en enskild identifieringstransaktion.

I paragrafens 4 mom. föreskrivs om syftet med behandlingen. 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 stark autentisering eller en innehavare av ett identifieringsverktyg. Dessutom föreskrivs det i momentet om förvaring av logguppgifterna om behandlingen.

Motsvarande bestämmelser för certifikatutfärdare som tillhandahåller kvalificerade certifikat ingår i förslagets 37 och 38 §. I 37 § föreskrivs det om uppgifter som tjänstetillhandahållaren ska registrera i certifikatregistret och på spärrlistan. I den föreslagna 38 § bestäms det att förvaringstiden för uppgifterna i certifikatregistret är 10 år. Paragraferna motsvarar de gällande bestämmelserna i lagen om elektroniska signaturer.

Behandling av personuppgifter ingår också i 19 och 30 § där det föreskrivs om certifikatens innehåll.

Om behandlingen av personuppgifter har det föreskrivits med den noggrannhet som förutsätts i 10 § i grundlagen. Bestämmelserna strider inte mot 10 § i grundlagen.

Näringsfrihet

Förslaget bör granskas också med tanke på den i 18 § 1 mom. i grundlagen föreskrivna näringsfriheten. Enligt 18 § 1 mom. i grundlagen har var och en rätt att i enlighet med lag skaffa sig sin försörjning genom arbete, yrke eller näring som han eller hon valt fritt. Grundlagsutskottet har tidigare behandlat frågor som gäller näringsfrihet bl.a. i utlåtandena GrUU 47/1996 rd (telemarknadslagen), GrUU 19/1998 rd (lagen om televisions- och radioverksamhet), GrUU 28/2001 rd (lagen om privata säkerhetstjänster), GrUU 61/2002 rd (kommunikationsmarknadslagen) och GrUU 67/2002 rd (lagen om finansinspektionen).

Utskottet har i sin utlåtandepraxis konstaterat att näringsfriheten inte får begränsas utan synnerligen giltigt skäl. Ett sådant skäl kan vara t.ex. skydd av personers hälsa och säkerhet eller andra viktiga och starka samhälleliga intressen. Begränsningarna ska framgå på lagnivå, eftersom det gäller begränsning av en grundläggande rättighet.

Utskottet har i sin utlåtandepraxis ansett att det i undantagsfall är möjligt att införa tillståndsplikt för näringsverksamhet. Det ska dock alltid föreskrivas om tillståndsplikten i lag och lagen ska uppfylla de krav på precisering och exakthet som gäller vid begränsning av en grundläggande fri- eller rättighet.

I propositionens 10 § föreskrivs det om skyldigheten för leverantörer av tjänster för stark autentisering att göra en anmälan om sin verksamhet till Kommunikationsverket. Enligt 12 § ska Kommunikationsverket efter det att anmälan har inkommit förbjuda en tjänsteleverantör att tillhandahålla sina tjänster som stark autentisering, om tjänsterna eller tjänsteleverantören inte uppfyller kraven i

detta kapitel. Om bristfälligheten kan anses vara endast ringa, kan Kommunikationsverket uppmana tjänsteleverantören att avhjälpa bristfälligheten inom en utsatt tid. Dessutom föreskrivs det i 12 § 1 mom. att Kommunikationsverket ska föra ett offentligt register över de tjänsteleverantörer som har gjort en anmälan.

Att anmälan görs är viktigt för att Kommunikationsverket effektivt kan utöva den tillsynsbehörighet som ankommer på det. Med tanke på systemet som helhet är det också väsentligt att övriga tjänsteleverantörer och personer som överväger att skaffa ett verktyg för stark autentisering på ett lätt sätt kan få besked om vilka tjänsteleverantörer som kan anses vara pålitliga. Arrangemanget i 10 och 12 § innebär ingen tillståndsplikt eftersom tjänsteleverantören kan tillhandahålla helt samma tjänst utan att göra en anmälan. Då får tjänsteleverantören dock inte tillhandahålla sin tjänst som tjänst för stark autentisering.

I fråga om tjänster för elektroniska signaturer innehåller den föreslagna lagen motsvarande bestämmelser i 32 §.

I den föreslagna lagens 29 § föreskrivs det dessutom om kontrollorgan. Kontrollorganen utses av Kommunikationsverket på ansökan. I den nämnda paragrafen föreskrivs om vilka förutsättningar som ska finnas för att en inrättning kan utses till kontrollorgan. Paragrafen bygger på EU-direktivet om ett gemenskapsramverk för elektroniska signaturer.

Med undantag av bestämmelserna om utnämnandet av kontrollorganen som bygger på direktivet om ett gemenskapsramverk för elektroniska signaturer föreskrivs det i den föreslagna lagen inte om att tjänsteleverantörerna skulle förutsättas ha ett tillstånd som ges på förhand. Förslaget begränsar i någon mån ett helt fritt utövande av en näring men begränsningarna ska anses vara motiverade med hänsyn till verksamhetens karaktär. Enligt de ovan nämnda grunderna strider förslaget inte heller för denna del mot grundlagen.

Skatter och avgifter

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. Skattskyldighetens omfattning ska entydigt framgå av skattelagen. Bestämmelserna i lagen ska också vara på så vis exakta att de tillämpande myndigheterna har bunden prövning när de fastställer skatten. De allmänna grunderna för de statliga myndigheternas tjänsteåtgärder, tjänster och övriga verksamhet samt avgifternas storlek utfärdas med stöd av 81 § 2 mom. i grundlagen genom lag.

Grundlagsutskottet har behandlat gränsdragningen mellan skatter och avgifter åtminstone i sitt utlåtande GrUU 66/2002 rd om järnvägslagen, i sitt utlåtande GrUU 67/2002 rd om finansinspektionen samt i sina utlåtanden GrUU 61/2002 rd och GrUU 3/2003 rd, som båda gällde kommunikationsmarknadslagen. Ärendet har också behandlats i utlåtandet GrUU 9/2004 rd om lagen om dataskydd vid elektronisk kommunikation.

Enligt grundlagsutskottets vedertagna tolkningspraxis är det utmärkande för avgifter att de utgör ersättningar eller vederlag för service som tillhandahålls av det allmänna. Övriga betalningar till staten är däremot i konstitutionellt hänseende i allmänhet skatter.

Grundlagsutskottet har i sina utlåtanden skissat vissa villkor som avgiften bör uppfylla för att den i konstitutionellt hänseende ska vara avgift och inte skatt. De prestationer som det tas ut avgifter för bör gå att specificera på något vis. Om ett penningbelopp allmänt tas ut för finansiering av någon verksamhet, är det konstitutionellt snarare fråga om en skatt än en avgift. Även om förutsättningen för avgiftens natur inte ens är full kostnadsmotsvarighet ska emellertid avgiftens storlek och grunderna för bestämmande av den bevara något slag av samband med de kostnader som föranleds av produktionen av prestationen. Ju större skillnaden mellan en avgift och kostnaderna för produktion av en prestation är, inte minst i samband med en offentligrättslig uppgift, desto närmare ligger det till hands att betrakta prestationen som en skatt.

Det spelar också en viss roll om det är frivilligt eller obligatoriskt att ta emot prestationen. Det tyder på en skatt om det inte går att tacka nej till betalningar som det finns en skyldighet att betala och skyldigheten direkt

med stöd av lag gäller rättssubjekt som uppfyller vissa rekvisit.

Att en penningprestation möjligen har ett begränsat syfte spelar enligt grundlagsutskottets utlåtandepraxis ingen roll vid bedömningen av prestationens konstitutionella natur.

I propositionens 47 § föreskrivs det om avgifter som ska betalas till Kommunikationsverket. De leverantörer av identifieringstjänster och sammanslutningar av tjänsteleverantörer som har gjort en anmälan ska betala en registreringsavgift på 5 000 euro till Kommunikationsverket. Tjänsteleverantörerna och sammanslutningarna ska dessutom årligen betala en tillsynsavgift på 12 000 euro till Kommunikationsverket.

Certifikatutfärdare som tillhandahåller kvalificerade certifikat ska årligen betala en tillsynsavgift på 40 000 euro till Kommunikationsverket. Om en certifikatutfärdare som tillhandahåller kvalificerade certifikat även gör en anmälan om tillhandahållande av tjänster för stark autentisering, ska också registreringsavgiften betalas.

Genom avgifterna täcks de kostnader som föranleds för Kommunikationsverket för skötseln av vissa lagstadgade uppgifter. Detta tyder på att avgifterna är av skattenatur.

Förbindelsen mellan grunder för hur avgiften bestäms och kostnader som föranleds av produceringen av prestationen kan bedömas som följer: Avgifterna har bara en avgiftsklass. Betalningsskyldigheten bestäms alltså på allmänna grunder utan att fästa individuell vikt vid någon prestation som tjänsteleverantören har tagit emot. Avgiftsskyldigheten kopplas allmänt till finansiering av en viss verksamhet i Kommunikationsverket, och det är därmed inte fråga om ett vederlag som särskilt kan specificeras genom en prestation av Kommunikationsverket. Enligt detta kriterium ska avgifterna anses snarare som skatt än som avgift.

Att det är obligatoriskt att ta emot en prestation kan bedömas som följer: Avgifterna ska betalas om företaget gör en anmälan om inledande av verksamhet av visst slag och utövar verksamhet av visst slag. Också enligt detta kriterium ska avgifterna anses snarare som skatt än som avgift.

Den föreslagna bestämmelsen har gjorts upp så att av den framgår minst grunderna för skattskyldighet och skattens storlek, de skattskyldigas rättsskydd och vilken krets de skattskyldiga utgör på det sätt som förutsätts i 81 § i grundlagen. Om andra detaljer kan vid behov föreskrivas genom förordning av kommunikationsministeriet. Lagens 47 § 4 mom. föreslås ha en särskild fullmaktsbestämmelse om detta.

Rätt att meddela föreskrifter

Enligt 80 § 1 mom. i grundlagen ska bestämmelser om grunderna för individens rättigheter och skyldigheter utfärdas genom lag. 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 en sådan fullmakt ska vara exakt avgränsat. Av grundlagen följer dessutom att de frågor som ett bemyndigande omfattar ska fastställas noggrant i lag.

Grundlagsutskottet har behandlat ärendet bl.a. i utlåtandena GrUU 19/2002 rd (läkemedelslagen), GrUU 21/2001 rd (lagen om säkerhetsutredningar), GrUU 34/2000 rd (telemarknadslagen), GrUU 25/2000 rd (lagen om försäkringsbolag) och GrUU 23/2000 rd (lotterilagen).

Grundlagsutskottet har i sin utlåtandepraxis konstaterat följande om tillämpningen av 80 § 2 mom. i grundlagen: Jämfört med bemyndiganden att utfärda förordning ställs det större krav på exakt avgränsning av bemyndiganden att meddela föreskrifter, vilket betyder att de frågor som bemyndigandet gäller måste preciseras exakt genom lag. Bemyndigandet ska dessutom enligt en uttrycklig bestämmelse i grundlagen ha ett exakt avgränsat tillämpningsområde (se också t.ex. GrUU 46/2001 rd, s. 3/I). Sett ur ett grundlagsperspektiv är andra myndigheters normgivningsrätt ett undantag (GrUB 10/1998 rd, s. 23/II). I samband med grundlagsreformen nämndes som exempel på myndigheters rätt att utfärda rättsnormer en teknisk reglering av smärre detaljer som inte inbegriper prövningsrätt i

någon större utsträckning (RP 1/1998 rd, s. 133/II, se även GrUU 16/2002, s. 2/I).

Grundlagsutskottet har också upprepade gånger betonat att tolkningen av bestämmelserna om bemyndigande liksom också innehållet i bestämmelser som utfärdas med stöd av dem inskränks direkt av 80 § 1 och 2 mom. i grundlagen (se t.ex. GrUU 48/2001 rd, s. 4). Det går därmed inte att genom förordning eller myndighetsföreskrifter utfärda allmänna rättsregler om exempelvis grunderna för individens rättigheter och skyldigheter eller frågor som enligt grundlagen i övrigt hör till området för lag (GrUU 16/2002 rd, s. 2/II).

I fråga om stark autentisering föreskrivs det i 8 § 3 mom. i propositionen att Kommunikationsverket vid behov kan utfärda närmare tekniska föreskrifter om hurdana krav tjänsten för stark autentisering måste uppfylla för att den kan vara stark. Enligt 10 § 5 mom. i propositionen kan Kommunikationsverket dessutom meddela för tillsynen behövliga föreskrifter om det närmare innehållet i de uppgifter som ska anmälas och om inlämnandet av dem till Kommunikationsverket.

I fråga om elektroniska signaturer har Kommunikationsverket motsvarande rättigheter att meddela föreskrifter som i den gällande lagen om elektroniska signaturer. Enligt 32 § 1 mom. i den föreslagna lagen kan Kommunikationsverket meddela för tillsynen behövliga föreskrifter och rekommendationer om det närmare innehållet i de uppgifter som ska lämnas och inlämnandet av dem till Kommunikationsverket.

Vidare enligt 42 § 3 mom. i lagförslaget kan Kommunikationsverket vid behov meddela tekniska föreskrifter om kraven på tillförlitlighet och informationssäkerhet i verksamhet som bedrivs av leverantörer av tjänster för stark autentisering och certifikatutfärdare som tillhandahåller kvalificerade certifikat.

Fullmakten att utfärda normer har i lagförslaget definierats så avgränsat och exakt som möjligt. Utfärdandet av föreskrifter innehåller bara lite ändamålsenlighetsprövning. Meddelande av tekniska och närmare föreskrifter är nödvändigt med hänsyn till den tekniska karaktären, snabbheten av den tekniska utvecklingen som föremålet för regleringen har samt den specialsakkunnigheten som regleringen förutsätter.

På ovan nämnda grunder kan den föreslagna rätten att utfärda normer inte anses stå i strid med grundlagens 80 §.

4.2 Bedömning av lagstiftningsordningen

Med stöd av vad som anförts ovan kan lagförslaget behandlas i vanlig lagstiftningsordning. Det är trots allt önskvärt att grundlagsutskottets utlåtande om propositionen inbegärs.

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

Lagförslag

1.

Lag

om stark autentisering och elektroniska signaturer

I enlighet med riksdagens beslut föreskrivs:

1 kap.

Allmänna bestämmelser

1 §

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.

Lagen tillämpas inte på tillhandahållande av tjänster för stark autentisering eller elektroniska signaturer som sker internt inom en sammanslutning.

Lagen tillämpas inte heller om en sammanslutning tillämpar en egen metod för stark autentisering uteslutande för att identifiera sina egna kunder, med undantag för bestämmelserna i:

3 § om bestämmelsernas tvingande natur,

20 § 1 mom. om utgivning av identifieringsverktyg,

21 § om överlåtelse av identifieringsverktyg till innehavaren,

22 § om förnyelse av identifieringsverktyg,

23 § 1 mom. om skyldigheter för innehavare av identifieringsverktyg,

25 § 1 och 2 mom. om återkallande eller förhindrande av användning av identifieringsverktyg,

27 § 1 mom., 27 § 2 mom. 1 punkten och 27 § 3 mom. om innehavarens ansvar för obehörig användning av ett identifieringsverktyg, och

42 § 4 mom. om konsumentombudsmannens befogenheter.

Lagen tillämpas inte på tillverkning, import eller försäljning av verktyg för stark autentisering eller för elektroniska signaturer.

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 de följande tre alternativen:

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, 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 verifiera en enskild transaktion 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 ett identifieringsverktyg av en leverantör av identifieringstjänster,
6) *inledande identifiering* verifiering av identiteten hos den som ansöker om ett identifieringsverktyg 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 till eller logiskt knutna till andra elektroniska data och som används som en metod för verifiering av undertecknarens identitet,
10) *avancerad elektronisk signatur* en elektronisk signatur som
a) är knuten uteslutande till undertecknaren,
b) gör det möjligt att identifiera undertecknaren,
c) är skapad med medel 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, och
13) *signaturverifieringsdata* data, såsom koder eller öppna nycklar, som används för att verifiera en elektronisk signatur.

2 kap.

Rättsverkningar och behandling av personuppgifter

3 §

Bestämmelsernas tvingande natur

Ett avtalsvillkor som avviker från bestämmelserna i denna lag till konsumentens nackdel är utan verkan, om inte något annat föreskrivs nedan.

4 §

Elektroniska signaturer som skapas med identifieringsverktyg

Elektroniska signaturer och avancerade elektroniska signaturer kan skapas med identifieringsverktyg på det sätt som verktygens egenskaper tillåter, om något annat inte föreskrivs på något annat ställe i lag eller i 18 §.

5 §

Rättshandlingar

Identifieringsverktyg får användas vid rättshandlingar, om något annat inte föreskrivs på något annat ställe i lag eller i 18 §.
Om det beträffande en rättshandling i lag ställs krav på 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 §

Behandling av personuppgifter

Vid utgivningen och upprätthållandet av identifieringsverktyg samt vid identifierings-

transaktioner får leverantörer av identifieringstjänster behandla de personuppgifter som behövs för detta 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 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.

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.

När leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller elektroniska signaturer kontrollerar sökandens identitet får de kräva att han eller hon uppger sin personbeteckning. Leverantörer av identifieringstjänster och certifikatutfärdare 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 den för att tillhandahålla tjänsten. Personbeteckningen får inte vara tillgänglig i en offentlig katalog.

I övrigt föreskrivs om behandlingen av personuppgifter i 19, 24, 30, 37, och 38 § och i personuppgiftslagen.

7 §

Användning av uppgifter i befolkningsdatasystemet

Leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller elektroniska signaturer får på de grunder som avses i 8 § 1 mom. 1 och 2 punkten i personuppgiftslagen och för de syften som nämns i 6 § 1 mom. inhämta personuppgifter ur befolkningsdataregistret och i registret kontrollera de personuppgifter som en sökande eller innehavare har uppgett.

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

3 kap.

Stark autentisering

8 §

Krav som gäller identifieringsmetoden

Identifieringsmetoden ska uppfylla följande krav:

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

2) med metoden kan innehavaren av identifieringsverktyget entydigt identifieras,

3) med metoden är det möjligt att med tillräckligt hög tillförlitlighet säkerställa att endast innehavaren av identifieringsverktyget kan använda verktyget, och

4) metoden är 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 endast meddelar den tjänsteleverantör som använder en identifieringstjänst den pseudonym som innehavaren av identifieringsverktyget använder eller ett begränsat antal personuppgifter.

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

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 bolags-

män eller andra personer i motsvarande ställning ska uppfylla följande krav:

1) de har uppnått myndighetsålder,
2) de får inte vara försatta i konkurs, och
3) de har inte begränsad handlingsbehörighet.

En leverantör av identifieringstjänster ska vara tillförlitlig. En leverantör av identifieringstjänster betraktas inte som tillförlitlig om en sådan person som avses i 1 mom. genom en lagakraftvunnen dom under de senaste fem åren har dömts till fängelsestraff eller under de senaste tre åren har dömts till böter för ett brott som kan anses visa att personen i fråga är uppenbart olämplig att tillhandahålla tjänster för stark autentisering.

En leverantör av identifieringstjänster betraktas inte heller som tillförlitlig, om en sådan person som avses i 1 mom. i övrigt genom sin tidigare verksamhet har visat sig vara uppenbart olämplig som leverantör av identifieringstjänster.

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

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

11 §

Leverantör av identifieringstjänster som är etablerad i en annan medlemsstat inom Europeiska ekonomiska samarbetsområdet

Vad som föreskrivs i 10 § hindrar inte att en leverantör av identifieringstjänster som är etablerad i en annan medlemsstat inom Europeiska ekonomiska samarbetsområdet gör en anmälan enligt nämnda paragraf.

12 §

Register över leverantörer av identifieringstjänster

Kommunikationsverket ska föra ett offentligt register över de leverantörer av identifieringstjänster som har gjort en anmälan enligt 10 § och om de tjänster som de tillhandahåller.

Efter det att anmälan enligt 10 § har inkommit ska Kommunikationsverket förbjuda en tjänsteleverantör att tillhandahålla sina tjänster som stark autentisering, om tjänsterna eller tjänsteleverantören inte uppfyller kraven i detta kapitel. Om bristfälligheten kan anses vara endast ringa, kan Kommunikationsverket uppmana tjänsteleverantören att avhjälpa bristfälligheten inom en utsatt tid.

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.

Leverantören av identifieringstjänster ska ha med tanke på verksamhetens omfattning

tillräckliga ekonomiska resurser för ordnande av verksamheten och täcka ett eventuellt skadeståndsansvar. Leverantören får också vidta andra nödvändiga åtgärder för att täcka ett eventuellt skadeståndsansvar.

Leverantören av identifieringstjänster ska dessutom ansvara för skyddet av uppgifterna enligt 32 § i personuppgiftslagen och för en tillräcklig informationssäkerhet i fråga om sina tjänster.

Leverantören av identifieringstjänster svarar för att tjänster och produkter som produceras av personer som tjänsteleverantören anlitar är tillförlitliga och fungerar.

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 av identifieringstjänster 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 om dem,
3) tjänsteleverantörens viktigaste samarbetsparter,
4) de kontroller som har utförts av utomstående bedömningsorgan, samt
5) andra omständigheter som är av betydelse för att tjänsteleverantörens verksamhet och tillförlitlighet ska kunna bedömas.

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

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 om identifieringstjänst lämna den andra avtalsparten uppgifter om

1) tjänsteleverantören,
2) de tjänster som tillhandahålls,
3) principerna för identifiering enligt 14 §,
4) parternas rättigheter och skyldigheter,
5) eventuella ansvarsbegränsningar,
6) förfarandena för klagomål och avgörande av tvister,
7) eventuella hinder för och begränsningar av användningen som avses i 18 §, och
8) övriga eventuella villkor för användning av identifieringsverktyget.

De uppgifter som avses i 1 mom. ska lämnas, skriftligen eller elektroniskt så att den som ansöker om ett identifieringsverktyg kan spara och återge dem i oförändrad form. Om ett avtal på begäran av den som ansöker om ett identifieringsverktyg ingås genom distanskommunikation så att uppgifter och avtalsvillkor inte kan lämnas på det sätt som avses ovan innan avtalet ingås, ska uppgifterna utan dröjsmål lämnas på det nämnda sättet efter det att avtalet har ingåtts.

Bestämmelser om skyldigheten att lämna uppgifter vid behandlingen av personuppgifter finns i personuppgiftslagen.

16 §

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

Leverantören av identifieringstjänster ska anmäla 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 personupppgiftslagen, ska leverantören av identifieringstjänster förutom till de aktörer som

avses i 1 mom. även anmäla saken till dataombudsmannen.

I anmälan ska redogöras för de åtgärder som de olika aktörerna kan vidta för att avvärja hoten eller störningarna, och för de beräknade kostnaderna för dessa åtgärder.

17 §

Inledande identifiering av den som ansöker om ett identifieringsverktyg

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

Den inledande identifieringen behöver inte göras personligen, om leverantörer av identifieringstjänster sinsemellan har avtalat om möjligheten att lita på en inledande identifiering som en avtalspart har gjort. Då kan ansökan om identifieringsverktyg göras elektroniskt. I avtalet ska leverantörerna av identifieringstjänster fastställa hur ansvaret fördelas mellan dem, om den ursprungliga identifieringen är felaktig. Den tjänsteleverantör av identifieringstjänster som litar på en inledande identifiering som gjorts av en annan avtalspart bär ansvaret i förhållande till den skadelidande.

Ansökan om identifieringsverktyg kan också göras elektroniskt, om sökanden har ett gällande identifieringsverktyg som har getts ut av samma leverantör av identifieringstjänster. Då behöver den inledande identifieringen inte göras på nytt.

Om identiteten hos den som ansöker om ett identifieringsverktyg inte kan verifieras på ett tillförlitligt sätt, ska polisen utföra den inledande identifieringen i samband med ansökan. De kostnader som polisens identifiering orsakar den som ansöker om ett identifieringsverktyg är en offentligrättslig prestation. I fråga om avgiften för en prestation föreskrivs i lagen om grunderna för avgifter till staten.

18 §

Förhindrande eller begränsning av användningen av identifieringsverktyg i samband med rättshandlingar

Användningen av verktyg för stark autentisering för att utföra rättshandlingar får förhindras genom avtal mellan leverantörer av identifieringstjänster, tjänsteleverantörer som använder tjänsterna och innehavare av identifieringsverktyg. Dessutom får utförandet av rättshandlingar begränsas både när det gäller användningsändamål och transaktionernas värde i pengar.

Leverantören av identifieringstjänster ska se till att alla parter känner till hindren eller begränsningarna eller att de är lätta upptäcka. Leverantören av identifieringstjänster får även införa hinder eller begränsningar med tekniska medel. Leverantören av identifieringstjänster svarar inte för de åtgärder som har vidtagits i strid med hindren eller begränsningarna trots att leverantören av identifieringstjänster har handlat på ett omsorgsfullt sätt.

Leverantören av identifieringstjänster ska se till att en tjänsteleverantör som använder identifieringstjänsterna har möjlighet att dygnet runt kontrollera de hinder och begränsningar som gäller identifieringsverktyget. Denna skyldighet föreligger dock inte om användning av identifieringsverktyget i strid med hindren och begränsningarna har förhindrats med hjälp av tekniska medel.

En tjänsteleverantör som använder stark autentisering ska i samband med användningen av ett identifieringsverktyg kontrollera eventuella hinder eller begränsningar i de system och register som leverantören av identifieringstjänster har. Detta behöver dock inte göras om användning av identifieringsverktyget i strid med hindren och begränsningarna har förhindrats med hjälp av tekniska medel.

19 §

Certifikatets innehåll

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

1) uppgifter om certifikatutfärdaren,
2) uppgifter om innehavaren av certifikatet,
3) innehavarens identifieringskod,
4) certifikatets giltighetstid,
5) certifikatets identifieringskod,
6) uppgifter om eventuella hinder och begränsningar som gäller användningen av certifikatet,
7) certifikatinnehavarens öppna nyckel och uppgifter om nyckelns användningsändamål, och
8) certifikatutfärdarens avancerade elektroniska signatur.

Den som tillhandahåller certifikattjänster ska för sin del försäkra sig om att en tjänsteleverantör som använder ett certifikat för elektronisk identifiering har tillgång till certifikatets innehåll.

20 §

Utgivning av identifieringsverktyg

Utgivningen av identifieringsverktyg grundar sig på ett avtal mellan den som ansöker om verktyget och leverantören av identifieringstjänster. Avtalet ska ingås skriftligen. Avtalet kan även ingås elektroniskt om dess innehåll inte kan ändras ensidigt och det hålls tillgängligt för parterna.

Avtalet kan gälla tills vidare eller för viss tid. Ett identifieringsverktyg kan ha en giltighetstid som är kortare än avtalets giltighetstid.

Identifieringsverktyg tillhandahålls endast fysiska personer. Identifieringsverktyg ska vara personliga. Till ett verktyg kan fogas en uppgift om att en person i enskilda fall även kan företräda en annan fysisk eller 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 av identifieringstjänster ska på ett tillräckligt sätt säkerställa att verktyget inte obehörigt kommer i någon annans besittning vid överlåtelsen.

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.

23 §

Skyldigheter för innehavare av identifieringsverktyg

Innehavaren av ett identifieringsverktyg ska använda identifieringsverktyget i enlighet med villkoren i avtalet. Innehavaren ska förvara identifieringsverktyget omsorgsfullt. Innehavaren är skyldig att ansvara för identifieringsverktyget efter det att verktyget har tagits emot.

Innehavaren av ett identifieringsverktyg får inte överlåta verktyget för att användas av någon annan.

24 §

Registrering och användning av uppgifter om identifieringstransaktioner och om 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 för stark autentisering 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 stark autentisering eller en innehavare av ett identifieringsverktyg. Leverantören av identifieringstjänster ska registrera uppgifter om behandlingen av identifieringstransaktionen, tidpunkt och orsak till transaktionen samt vem som utfört den.

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.

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, obehörigt 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 av identifieringstjänster ska omedelbart återkalla verktyget eller förhindra att det används efter det att anmälan har mottagits.

Leverantören av identifieringstjänster ska på lämpligt sätt och utan dröjsmål registrera uppgift om tidpunkten för återkallandet eller förhindrandet av användningen i systemet. 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.

Systemet ska vara sådant att en tjänsteleverantör som använder stark autentisering lätt kan kontrollera uppgifterna i systemet vilket tid på dygnet som helst. Skyldighet att ordna möjlighet att kontrollera uppgifterna föreligger dock inte om användning av identifieringsverktyget kan förhindras med hjälp av tekniska medel eller om verktyget kan spärras.

En tjänsteleverantör som använder en identifieringstjänst ska i samband med användningen av ett identifieringsverktyg kontrollera uppgifterna om eventuella hinder eller begränsningar i de system och register som leverantören av identifieringstjänster har. Detta behöver dock inte göras om användning av identifieringsverktyget i strid med hindren och begränsningarna har förhindrats med hjälp av tekniska medel.

Om en identifieringstjänst grundar sig på certifikat och uppgifter om återkallade certifikat ges med hjälp av en spärrlista, får den som tillhandahåller certifikattjänster registrera uppgifter om kontroll av certifikatens giltighet som gjorts på spärrlistan. Certifikatutfärdaren kan alternativt lagra spärrlistan.

26 §

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

Utöver vad som föreskrivs i 25 § får leverantören av identifieringstjänster återkalla el-

ler 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 identifieringsverktyget har äventyrats,

4) innehavaren av ett identifieringsverktyg använder identifieringsverktyget 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 av identifieringsverktyget om att identifieringsverktyget har återkallats eller användningen av det förhindrats och ange tidpunkten för återkallandet eller förhindrandet av användningen och orsakerna till det.

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

27 §

Innehavarens ansvar för obehörig användning av ett identifieringsverktyg

Innehavaren av ett identifieringsverktyg ansvarar för obehörig användning av identifieringsverktyget endast om:

1) innehavaren har överlåtit identifieringsverktyget till någon annan,

2) identifieringsverktyget har försvunnit, kommit i någon annans besittning obehörigt eller använts obehörigt på grund av innehavarens vårdslöshet, som inte är lindrig, eller

3) innehavaren har försummat att utan obefogat dröjsmål efter det att saken har upptäckts, anmäla till leverantören av identifieringstjänster eller någon annan aktör som denne har angett att identifieringsverktyget har försvunnit, kommit i någon annans besittning obehörigt eller använts obehörigt.

Innehavaren av ett identifieringsverktyg ansvarar dock inte för obehörig användning av identifieringsverktyget

1) till den del identifieringsverktyget har använts efter det att innehavaren har anmält till leverantören av identifieringstjänster att identifieringsverktyget har försvunnit, kommit i någon annans besittning obehörigt eller använts obehörigt,

2) om innehavaren av identifieringsverktyg inte utan obefogat dröjsmål efter det att saken har upptäckts har kunnat göra en anmälan om att identifieringsverktyget har försvunnit, kommit i någon annans besittning obehörigt eller använts obehörigt på grund av att leverantören av identifieringstjänster har åsidosatt skyldigheten enligt 25 § 2 mom. att se till att innehavaren av ett identifieringsverktyg alltid har möjlighet att göra en sådan anmälan, eller

3) om en tjänsteleverantör som använder stark autentisering har åsidosatt sin skyldighet enligt 18 § 4 mom. och 25 § 5 mom. att kontrollera om det finns begränsningar för användningen av identifieringsverktyget eller uppgift om spärrning av verktyget.

4 kap.

Elektroniska signaturer

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, samt

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 publicerats 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 som en säker anordning för signaturframställning.

29 §

Kontrollorgan

Kommunikationsverket kan utse kontrollorgan med uppgift att bedöma om anordningar för signaturframställning uppfyller 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 ett ändamålsenligt ordnande av verksamheten och täckande av ett eventuellt ersättningsansvar,

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

5) den har tillgång till sådana lokaliteter 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.

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,

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 tjänster för stark autentisering enligt 2 kap., anses kraven i 1 mom. alltid också uppfylla de krav som gäller certifikatets innehåll i 19 § 1 mom.

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, eller

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*, eller

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 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 tredje länder 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 meddela 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 certifikat som anges vara kvalificerade, 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 ändrats.

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 tjänster för stark autentisering.

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 verksamheten, även för att 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 ordnande av verksamheten och täckande av ett eventuellt skadeståndsansvar,

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

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

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

34 §

Tillförlitliga maskinvaror och programvaror

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

En 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 fastställt och som har publicerats 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.

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

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, samt

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 spärrlistan ska utan dröjsmål införas uppgift om att ett kvalificerat certifikat har återkallats samt 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 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.

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.

40 §

Ansvar för obehörig användning av signaturframställningsdata

Undertecknaren ansvarar för skada som orsakats av obehörig användning av signaturframställningsdata för skapande av 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) det beror på vårdslöshet från konsumentens sida, som inte är lindrig, att signaturframställningsdata åtkommits av någon som är obehörig att använda dem, eller

3) konsumenten på annat sätt än som nämns i 2 punkten har förlorat besittningen till signaturframställningsdata och har underlåtit att begära att det kvalificerade certifikatet ska återkallas så som anges i 36 § 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.,

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 certifi-

kat har använts i strid med de begränsningar av användningen som ingår i det.

I fråga om skadeståndsansvaret för certifikatutfärdare som tillhandahåller 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.

5 kap.

Myndighetstillsyn

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 meddelar 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.

Efterlevnaden av 1 § 3 mom. i denna lag i fråga om förhållandet mellan leverantörer av identifieringstjänster och konsumenten övervakas av konsumentombudsmannen.

43 §

Rätt till information

Trots bestämmelserna om sekretess har Kommunikationsverket rätt att av leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller kvalificerade certifikat samt av personer som dessa anlitar få den information som behövs för att fullgöra de uppgifter som anges i 42 §.

Dataombudsmannen har i sitt uppdrag rätt att få information enligt personuppgiftslagen.

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 lämna till Finansinspektionen den information som den behöver för att fullgöra sina uppgifter.

När Kommunikationsverket och dataombudsmannen utför uppgifter enligt denna lag ska de vid behov samarbeta på lämpligt sätt med Finansinspektionen, Konkurrensverket och Konsumentverket samt med varandra.

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).

Kostnaderna för en åtgärd som vidtagits på den försumliges bekostnad betalas av statens medel och indrivs hos den försumlige på det sätt som föreskrivs i lagen om verkställighet av skatter och avgifter (706/2007).

46 §

Inspektionsrätt

Kommunikationsverket har rätt att utföra eller låta utföra inspektioner av leverantörer av identifieringstjänster och av leverantörernas tjänster, om det finns skäl att misstänka att tjänsteleverantören på ett väsentligt sätt

har brutit mot denna lag eller mot föreskrifter som har utfärdats med stöd av den.

Kommunikationsverket ska årligen utföra eller låta 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 sådana maskinvaror och programvaror som kan vara av betydelse vid tillsynen över efterlevnaden av denna lag och föreskrifter som meddelats med stöd av den.

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 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.

47 §

Avgifter som ska betalas till Kommunikationsverket

De leverantörer av identifieringstjänster och sammanslutningar av tjänsteleverantörer som har gjort en anmälan enligt 10 § ska betala en registreringsavgift på 5 000 euro till Kommunikationsverket. Leverantörerna av identifieringstjänster och sammanslutningarna ska dessutom årligen betala en tillsynsavgift på 12 000 euro till Kommunikationsverket.

Certifikatutfärdare som tillhandahåller kvalificerade certifikat ska 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.

Registreringsavgiften 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. Tillsynsavgiften återbetalas inte även om tjänsteleverantören upphör med sin verksamhet under året.

Registreringsavgiften 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 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 på det obetalda beloppet ut en årlig dröjsmålsränta 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 tjänsteleverantören av identifieringstjänster enligt lagen om grunderna för avgifter till staten.

6 kap.

Särskilda bestämmelser

48 §

Straffbestämmelser

Bestämmelser om straff för personregisterbrott finns i 38 kap. 9 § i strafflagen (39/1889) och bestämmelser om straff för personregisterförseelse finns i 48 § 2 mom. i personuppgiftslagen.

49 §

Ändringssökande

Bestämmelser om sökande av ändring i beslut som Kommunikationsverket har fattat med stöd av denna lag finns i förvaltningsprocesslagen (586/1996).

Kommunikationsverket kan i sitt 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 dataombudsmannens beslut finns i personuppgiftslagen.

7 kap.

Ikraftträdande

50 §

Ikraftträdande

Denna lag träder i kraft den 20 .

Genom denna lag upphävs lagen av den 24 januari 2003 om elektroniska signaturer (14/2003). De föreskrifter som Kommunikationsverket har utfärdat med stöd av den lag som upphävs är dock i kraft tills nya föreskrifter utfärdas med stöd av denna lag.

Åtgärder som verkställigheten av lagen förutsätter får vidtas innan lagen träder i kraft.

51 §

Övergångsbestämmelse

Leverantörer av identifieringstjänster ska göra en anmälan enligt 10 § till Kommunikationsverket inom sex månader från lagens ikraftträdande. Som tjänster för stark autentisering och leverantörer av identifieringstjänster betraktas under denna tid sådana tjänster för elektronisk identifiering sådana leverantörer av tjänster för elektronisk identifiering som uppfyller de definitioner som omfattas av tillämpningsområdet för 1 § och som avses i 2 § 1 och 4 punkten.

Identifieringsverktyg som har getts ut före ikraftträdandet av denna lag och inom den övergångsperiod som avses i 1 mom. betraktas som verktyg för stark autentisering, om en leverantör av identifieringstjänster gör en anmälan enligt 10 § inom den tid som avses i 1 mom. Identifieringstjänsterna och leverantörerna av identifieringstjänster ska då uppfylla alla krav som i denna lag ställs på dem, med undantag för bestämmelserna i 17 §.

Om leverantörerna av identifieringstjänster har ingått ett avtal enligt 17 § 2 mom. om möjligheten att lita på en inledande identifiering som en annan leverantör har gjort, och den tjänsteleverantör som har gett ut de identifieringsverktyg som använts vid den inledande identifieringen inte har gjort en anmälan enligt 10 § inom den tid som avses i 1 mom., ska den inledande identifieringen göras utan dröjsmål på det sätt som avses i 17 § i fråga om de identifieringsverktyg som getts ut på detta sätt.

En sådan certifikatutfärdare som tillhandahåller kvalificerade certifikat och som har gjort en anmälan enligt 9 § 1 mom. i lagen om elektroniska signaturer och fortsatt verksamheten utan avbrott till ikraftträdandet av denna lag, behöver inte göra en ny anmälan enligt 32 § 1 mom. Certifikatutfärdaren kan då lämna en fritt formulerad skriftlig anmälan till Kommunikationsverket om att verksamheten fortsatt oförändrad.

Trots betsämmelserna i 17 § 1 mom. och 35 § 1 mom. kan leverantörer av identifieringstjänster och certifikatutfärdare som tillhandahåller kvalificerade certifikat till och med den 31 december 2012 vid den inledande identifieringen använda ett giltigt körkort som har utfärdats efter den 1 oktober 1990 av en myndighet i en medlemsstat inom Europeiska ekonomiska samarbetsområdet.

2.

Lag

om ändring av lagen om elektronisk kommunikation i myndigheternas verksamhet

I enlighet med riksdagens beslut

ändras i lagen av den 24 januari 2003 om elektronisk kommunikation i myndigheternas verksamhet (13/2003) 3 § 2 mom., 9 § 1 mom., 16 § och 18 § 2 mom. som följer:

3 §

Annan lagstiftning

— — — — — — — — — — — — — —

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 ().

9 §

Krav på skriftlig form och underskrift

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.

— — — — — — — — — — — — — —

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.

18 §

Bevislig elektronisk delgivning

— — — — — — — — — — — — — —

Parten eller dennes företrädare ska identifiera sig när beslutshandlingen hämtas. Vid identifieringen kan användas 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.

— — — — — — — — — — — — — —

_____

Denna lag träder i kraft den 20 .

_____

3.

Lag

om ändring av 19 och 20 § i befolkningsdatalagen

I enlighet med riksdagens beslut

ändras i befolkningsdatalagen av den 11 juni 1993 (507/1993) 19 § 3 mom. och 20 § 1 mom., sådana de lyder i lag 299/2003, som följer:

19 §	20 §
Certifierad elektronisk kommunikation	*Uppgifter i certifikat för certifierad elektronisk kommunikation*
— — — — — — — — — — — — — — —	
I fråga om tillhandahållande av sådana certifikat för elektroniska signaturer som utfärdas av Befolkningsregistercentralen, certifikatutfärdarens skyldigheter och ansvar samt behandlingen av personuppgifter gäller dessutom vad som föreskrivs i lagen om stark autentisering och elektroniska signaturer (/).	I fråga om innehållet i sådana certifikat för elektroniska signaturer som Befolkningsregistercentralen utfärdar för en person gäller vad som i 30 § i lagen om stark autentisering och elektroniska signaturer föreskrivs om innehållet i kvalificerade certifikat. Den elektroniska kommunikationskod som avses i 21 § utgör den identifieringsuppgift som anger innehavaren av ett sådant medborgarcertifikat som Befolkningsregistercentralen utfärdar. Ett medborgarcertifikat innehåller dessutom andra nödvändiga tekniska uppgifter som användningen av certifikatet kräver.
	— — — — — — — — — — — — — — —

Denna lag träder i kraft den 20 .

4.

Lag

om ändring av 2 och 9 § i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården

I enlighet med riksdagens beslut

ändras i lagen av den 9 februari 2007 om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) 2 § 3 mom. och 9 § som följer:

2 §

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 (/) och arkivlagen (831/1994) eller med stöd av dem.

9 §

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.

———

Denna lag träder i kraft den 20 .

———

5.

Lag

om ändring av 2 § i lagen om kommunikationsförvaltningen

I enlighet med riksdagens beslut

ändras i lagen av den 29 juni 2001 om kommunikationsförvaltningen (625/2001) 2 § 1 punkten, sådan den lyder i lag 520/2004, som följer:

2 §

Kommunikationsverkets uppgifter

Kommunikationsverket har till uppgift att

1) sköta de uppgifter som enligt kommunikationsmarknadslagen (393/2003), lagen om radiofrekvenser och teleutrustningar (1015/2001), lagen om posttjänster (313/2001), 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 (/) och lagen om domännamn (228/2003) ankommer på Kommunikationsverket, samt

— — — — — — — — — — — — — — —

_____

Denna lag träder i kraft den 20 .

_____

6.

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 av den 18 juli 2008 om förhindrande och utredning av penningtvätt och av finansiering av terrorism (503/2008) 18 § 3 punkten 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 eller ett kvalificerat certifikat som avses i lagen om stark autentisering och elektroniska signaturer (/), eller med hjälp av någon annan teknik för elektronisk identifiering som är informationssäker och bevislig.

_____

Denna lag träder i kraft den 20 .

_____

7.

Lag

om ändring av 56 b § i lagen om överlåtelseskatt

I enlighet med riksdagens beslut

ändras i lagen av den 29 november 1996 om överlåtelseskatt (931/1996) 56 b § 2 mom., sådant det lyder i lag 1085/2005, som följer:

56 b §	med en avancerad elektronisk signatur som avses i lagen om stark autentisering och elektroniska signaturer (/) eller på något annat godtagbart sätt.
Elektronisk kommunikation och signering	———————————————
———————————————	_____
Deklarationer och andra handlingar som får lämnas in till skattemyndigheten på elektronisk väg och som ska signeras, ska certifieras	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 av den 18 december 1995 om beskattningsförfarande (1558/1995) 93 a § 2 mom., sådant den lyder i lag 1079/2005, 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 avancerad elektronisk signatur som avses i lagen om stark autentisering och elektroniska signaturer (/) eller på något annat godtagbart sätt.

— — — — — — — — — — — — — — —

_____

Denna lag träder i kraft den 20 .

_____

9.

Lag

om ändring av 165 § i mervärdesskattelagen

I enlighet med riksdagens beslut

ändras i mervärdesskattelagen av den 30 december 1993 (1501/1993) 165 § 3 mom., sådant det lyder i lag 1083/2005, som följer:

165 §

— — — — — — — — — — — — — — —

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 (/) 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 av den 20 december 1996 om förskottsuppbörd (1118/1996) 6 a § 2 mom., sådant det lyder i lag 1082/2005, 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 avancerad elektronisk signatur som avses i lagen om stark autentisering och elektroniska signaturer (/) 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 av den 1 april 2005 (197/2005) 11 § som följer:

11 §

Uppgifter som hänför sig till blodgivare

Den som ger blod och blodkomponenter ska före blodgivningen ges nödvändiga 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 av betydelse när det gäller att bedöma blodgivarens lämplighet samt blodgivarens egenhändiga underskrift eller en avancerad elektronisk signatur enligt lagen om stark autentisering och elektroniska signaturer (/). Läkemedelsverket kan utfärda närmare föreskrifter om den information som ska ges till och inhämtas från blodgivare.

_____

Denna lag träder i kraft den 20 .

_____

Helsingfors den 27 mars 2009

Republikens President

TARJA HALONEN

Kommunikationsminister *Suvi Lindén*

Bilagor
Parallelltext

2.

Lag

om ändring av lagen om elektronisk kommunikation i myndigheternas verksamhet

I enlighet med riksdagens beslut
ändras i lagen av den 24 januari 2003 om elektronisk kommunikation i myndigheternas verksamhet (13/2003) 3 § 2 mom., 9 § 1 mom., 16 § och 18 § 2 mom. som följer:

Gällande lydelse	*Föreslagen lydelse*
3 §	3 §
Annan lagstiftning	*Annan lagstiftning*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
Bestämmelser om användningen av elektroniska signaturer och certifikattjänster i anslutning till dem finns i lagen om elektroniska signaturer (14/2003).	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* ( ).
9 §	9 §
Krav på skriftlig form och underskrift	*Krav på skriftlig form och underskrift*
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 18 § lagen om elektroniska signaturer.	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, *ska den undertecknas så som avses i 5 § 2 mom. i lagen om stark autentisering och elektroniska signaturer.*
	— — — — — — — — — — — — — — — —

Gällande lydelse	*Föreslagen lydelse*
16 §	16 §
Elektronisk signering av beslutshandlingar	*Elektronisk signering av beslutshandlingar*
En beslutshandling kan signeras elektroniskt. En myndighets elektroniska signatur skall uppfylla kraven i 18 § lagen om elektroniska signaturer.	En beslutshandling kan signeras elektroniskt. *En myndighet ska underteckna handlingen så som avses i 5 § 2 mom. i lagen om stark autentisering och elektroniska signaturer.*
18 §	18 §
Bevislig elektronisk delgivning	*Bevislig elektronisk delgivning*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
Parten eller dennes företrädare skall identifiera sig när beslutshandlingen hämtas. För identifieringen krävs ett certifikat som uppfyller de krav som ställs på kvalificerade certifikat i lagen om elektroniska signaturer eller någon annan motsvarande identifieringsteknik som är datatekniskt tillförlitlig och bevislig.	Parten eller dennes företrädare ska identifiera sig när beslutshandlingen hämtas. *Vid identifieringen kan användas 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.
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —

———

Denna lag träder i kraft den 20 .

———

3.

Lag

om ändring av 19 och 20 § i befolkningsdatalagen

I enlighet med riksdagens beslut
ändras i befolkningsdatalagen av den 11 juni 1993 (507/1993) 19 § 3 mom. och 20 § 1 mom., sådana de lyder i lag 299/2003, som följer:

Gällande lydelse	*Föreslagen lydelse*
19 §	19 §
Certifierad elektronisk kommunikation	*Certifierad elektronisk kommunikation*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
I fråga om tillhandahållande av sådana certifikat för elektroniska signaturer som utfärdas av Befolkningsregistercentralen, certifikatutfärdarens skyldigheter och ansvar samt behandlingen av personuppgifter gäller dessutom vad som föreskrivs i lagen om elektroniska signaturer (14/2003).	I fråga om tillhandahållande av sådana certifikat för elektroniska signaturer som utfärdas av Befolkningsregistercentralen, certifikatutfärdarens skyldigheter och ansvar samt behandlingen av personuppgifter gäller dessutom vad som föreskrivs *i lagen om stark autentisering och elektroniska signaturer (/).*
20 §	20 §
Uppgifter i certifikat för certifierad elektronisk kommunikation	*Uppgifter i certifikat för certifierad elektronisk kommunikation*
I fråga om innehållet i sådana certifikat för elektroniska signaturer som Befolkningsregistercentralen utfärdar för en person gäller vad som i 7 § lagen om elektroniska signaturer föreskrivs om innehållet i kvalificerade certifikat. Den elektroniska kommunikationskod som avses i 21 § utgör den identifieringsuppgift som anger innehavaren av ett sådant medborgarcertifikat som Befolkningsregistercentralen utfärdar. Ett medborgarcertifikat innehåller dessutom andra nödvändiga tekniska	I fråga om innehållet i sådana certifikat för elektroniska signaturer som Befolkningsregistercentralen utfärdar för en person gäller vad som *i 30 § i lagen om stark autentisering och elektroniska signaturer föreskrivs om innehållet i kvalificerade certifikat.* Den elektroniska kommunikationskod som avses i 21 § utgör den identifieringsuppgift som anger innehavaren av ett sådant medborgarcertifikat som Befolkningsregistercentralen utfärdar. Ett medborgarcertifikat innehåller dess-

Gällande lydelse	*Föreslagen lydelse*
uppgifter som användningen av certifikatet kräver.	utom andra nödvändiga tekniska uppgifter som användningen av certifikatet kräver.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —

_____

Denna lag träder i kraft den 20 .

_____

4.

Lag

om ändring av 2 och 9 § i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården

I enlighet med riksdagens beslut

ändras i lagen av den 9 februari 2007 om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) 2 § 3 mom. och 9 § 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 elektroniska signaturer (14/2003) och arkivlagen (831/1994) eller med stöd av dem.	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 (/)* och arkivlagen (831/1994) eller med stöd av dem.
9 §	9 §
Elektronisk signering av handlingar	*Elektronisk signering av handlingar*
Klientuppgifternas integritet, oförvanskade form och oavvislighet skall säkerställas med en elektronisk signatur vid elektronisk behandling, överföring och förvaring av uppgifterna. Vid elektronisk signering som görs av en fysisk person skall användas en avancerad elektronisk signatur enligt lagen om elektro-	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 au-*

Gällande lydelse	*Föreslagen lydelse*
niska signaturer. Vid signering som görs av en organisation och datatekniska enheter skall användas en elektronisk signatur av motsvarande tillförlitlighet.	*tentisering och elektroniska signaturer*. Vid signering som görs av en organisation och datatekniska enheter ska användas en elektronisk signatur av motsvarande tillförlitlighet.

_____

Denna lag träder i kraft den 20 .

_____

5.

Lag

om ändring av 2 § i lagen om kommunikationsförvaltningen

I enlighet med riksdagens beslut
ändras i lagen av den 29 juni 2001 om kommunikationsförvaltningen (625/2001) 2 § 1 punkten, sådan den lyder i lag 520/2004, som följer:

Gällande lydelse	*Föreslagen lydelse*
2 §	2 §
Kommunikationsverkets uppgifter	*Kommunikationsverkets uppgifter*
1) sköta de uppgifter som enligt kommunikationsmarknadslagen (393/2003), radiolagen (1015/2001), lagen om posttjänster (313/2001), 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 elektroniska signaturer (14/2003) och lagen om domännamn (228/2003) ankommer på Kommunikationsverket, samt	Kommunikationsverket har till uppgift att 1) sköta de uppgifter som enligt kommunikationsmarknadslagen (393/2003), lagen om radiofrekvenser och teleutrustningar (1015/2001), lagen om posttjänster (313/2001), 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 ()* och lagen om domännamn (228/2003) ankommer på Kommunikationsverket, samt
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —

———

Denna lag träder i kraft den 20 .

———

6.

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 av den 18 juli 2008 om förhindrande och utredning av penningtvätt och av finansiering av terrorism (503/2008) 18 § 3 punkten som följer:

Gällande lydelse	*Föreslagen lydelse*
18 §	18 §
Skärpta krav på kontroll vid identifiering på distans	*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 kvalificerat certifikat som avses i lagen om elektroniska signaturer (14/2003), eller med hjälp av någon annan teknik för elektronisk identifiering som är informationssäker och bevislig.	3) kontrollera kundens identitet med ett identifieringsverktyg eller ett kvalificerat certifikat som avses *i lagen om stark autentisering och elektroniska signaturer (/),* eller med hjälp av någon annan teknik för elektronisk identifiering som är informationssäker och bevislig.

_____

Denna lag träder i kraft den 20 .

_____

7.

Lag

om ändring av 56 b § i lagen om överlåtelseskatt

I enlighet med riksdagens beslut
ändras i lagen av den 29 november 2001 om överlåtelseskatt (931/1996) 56 b § 2 mom., sådant det lyder i lag 1085/2005, 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 på elektronisk väg och som skall signeras så som särskilt bestäms därom, anses vara signerade när de uppfyller kraven i lagen om elektroniska signaturer (14/2003).	Deklarationer och andra handlingar som får lämnas in på elektronisk väg och som ska signeras så som särskilt bestäms därom, anses vara signerade när *de har undertecknats med en avancerad elektronisk signatur som avses i lagen om stark autentisering och elektroniska signaturer (/) eller på något annat godtagbart sätt.*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —

_____

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 av den 18 december 1995 om beskattningsförfarande (1558/1995) 93 a § 2 mom., sådant den lyder i lag 1079/2005, 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 skall signeras skall certifieras på det sätt som anges i 18 § i lagen om elektroniska signaturer (14/2003) eller på något annat godtagbart sätt.	Deklarationer och andra handlingar som får lämnas in till skattemyndigheten på elektronisk väg och som ska signeras *anses vara signerade när de har undertecknats med en avancerad elektronisk signatur som avses i lagen om stark autentisering och elektroniska signaturer (/) eller på något annat godtagbart sätt.*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —

_____

Denna lag träder i kraft den 20 .

_____

9.

Lag

om ändring av 165 § i mervärdesskattelagen

I enlighet med riksdagens beslut
ändras i mervärdesskattelagen av den 30 december 1993 (1501/1993) 165 § 3 mom., sådant det lyder i lag 1083/2005, som följer:

Gällande lydelse	*Föreslagen lydelse*
165 §	165 §
Deklarationer och andra handlingar som får lämnas in till skattemyndigheten på elektronisk väg och som skall signeras skall certifieras på det sätt som anges i 18 § i lagen om elektroniska signaturer (14/2003) eller på något annat godtagbart sätt.	Deklarationer och andra handlingar som får lämnas in till skattemyndigheten på elektronisk väg och som ska signeras *anses vara signerade när de har undertecknats med en avancerad elektronisk signatur som avses i lagen om stark autentisering och elektroniska signaturer (/) 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 av den 20 december 1996 om förskottsuppbörd (1118/1996) 6 a § 2 mom., sådant det lyder i lag 1082/2005, 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 skall signeras skall certifieras på det sätt som anges i 18 § i lagen om elektroniska signaturer (14/2003) eller på något annat godtagbart sätt.	Deklarationer och andra handlingar som får lämnas in till skattemyndigheten på elektronisk väg och som ska signeras *anses vara signerade när de har undertecknats med en avancerad elektronisk signatur som avses i lagen om stark autentisering och elektroniska signaturer (/) 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 av den 1 april 2005 (197/2005) 11 § 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 skall före blodgivningen ges nödvändiga upplysningar som hänför sig till blodgivningen samt de uppgifter som avses i 24 § i personuppgiftslagen (523/1999). Blodgivaren skall informeras om sekretessen i fråga om uppgifterna. Av blodgivaren skall begäras identifieringsuppgifter, sådana uppgifter om hälsotillståndet som är av betydelse när det gäller att bedöma blodgivarens lämplighet samt blodgivarens egenhändiga underskrift eller en avancerad elektronisk signatur enligt lagen om elektroniska signaturer (14/2003). Läkemedelsverket kan utfärda närmare föreskrifter om den information som skall ges till och inhämtas från blodgivare.	Den som ger blod och blodkomponenter ska före blodgivningen ges nödvändiga 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 av betydelse när det gäller att bedöma blodgivarens lämplighet samt blodgivarens egenhändiga underskrift *eller en avancerad elektronisk signatur enligt lagen om stark autentisering och elektroniska signaturer (/).* Läkemedelsverket kan utfärda närmare föreskrifter om den information som ska ges till och inhämtas från blodgivare.

_____

Denna lag träder i kraft den 20 .

_____