RP 197/2001 rd

Regeringens proposition till Riksdagen med förslag till lagar om elektroniska signaturer och om ändring av 2 § lagen om kommunikationsförvaltningen

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås att en lag skall stiftas om elektroniska signaturer. Genom lagen om elektroniska signaturer och produkter och tjänster som behövs när sådana signaturer används främjas konsumenternas och andra användares förtroende för nätaffärsverksamhet och elektronisk kommunikation. Meningen är att lagen skall främja utvecklingen inom en ny och växande affärssektor, dvs. certifieringen. Lagen kommer att öka den elektroniska handeln och kommunikationen samt användningen av de tjänster som IT-samhället tillhandahåller.

Meningen är att lagen skall reglera elektroniska signaturer och deras rättsverkan. En avancerad elektronisk signatur som gjorts med hjälp av en säker anordning för signaturframställning och ett kvalificerat certifikat, vilka definieras i lagen, garanteras samma ställning som en traditionell handskriven namnteckning.

Lagen kommer inte att gälla annat tillhandahållande av produkter och tjänster än sådant som ansluter sig till elektroniska signaturer. Enligt förslaget skall tillhandahållandet av produkter och tjänster i anslutning till elektroniska signaturer vara en fri näring. Dessutom är det meningen att i behövlig utsträckning lagstifta om tillhandahållandet av certifikat för elektronisk signering, om skyldigheterna och ansvaret för dem som tillhandahåller dessa certifikat samt om skyddet för personuppgifter.

I lagen skall föreskrivas om skyldigheterna för certifikatutfärdare som tillhandahåller kvalificerade certifikat av hög kvalitet. Dessa skyldigheter syftar till större tillförlitlighet hos elektroniska signaturer, och gäller bl.a. tillförlitlig identifiering av den som ansöker om certifikat, användning av säkra system, tillräckliga tekniska och ekonomiska resurser samt personalens kompetens. I lagen skall också ingå minimikrav angående innehållet i kvalificerade certifikat. En certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat är med vissa begränsningar som anges i lagen ansvarig för skador som felaktiga kvalificerade certifikat åsamkar dem som har förlitat sig på en elektronisk signatur som är baserad på ett kvalificerat certifikat.

Den som tillhandahåller kvalificerade certifikat skall göra en anmälan om sin verksamhet till Kommunikationsverket, som övervakar tillhandahållandet av kvalificerade certifikat. I propositionen ingår också ett förslag till ändring av lagen om kommunikationsförvaltningen. Genom ändringen fogas till Kommunikationsverkets uppgifter de uppgifter som ankommer på verket enligt lagen om elektroniska signaturer.

Genom de föreslagna lagarna genomförs Europaparlamentets och rådets direktiv om ett gemenskapsramverk för elektroniska signaturer.

De föreslagna lagarna är avsedda att träda i kraft så snart som möjligt efter det att de har antagits och blivit stadfästa.

Anmäld enligt Europaparlamentets och rådets direktiv 98/34/EG, ändr. 98/48/EG.

219361S

INNEHÅLLSFÖRTECKNING

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL 1

INNEHÅLLSFÖRTECKNING 2

ALLMÄN MOTIVERING 4
1. Inledning 4
2. Nuläge 7
2.1. Lagstiftning och praxis 7
2.2. Europeiska gemenskapernas direktiv om elektroniska signaturer 8
2.3. Den internationella utvecklingen och lagstiftningen i utlandet 10
2.4. Bedömning av nuläget 12
3. Propositionens mål och de viktigaste förslagen 13
4. Propositionens verkningar 15
4.1. Ekonomiska verkningar 15
4.2. Verkningar i fråga om organisation och personal 15
4.3. Miljökonsekvenser 15
4.4. Verkningar för olika medborgargrupper 15
5. Beredningen av propositionen 16
5.1. Beredningsskeden och beredningsmaterial 16
5.2. Utlåtanden 17
6. Andra omständigheter som inverkat på propositionens innehåll 17

DETALJMOTIVERING 19
1. Lagförslag 19
1.1. Lag om elektroniska signaturer 19
1 kap. Allmänna bestämmelser 19
2 kap. Tillhandahållande av kvalificerade certifikat 23
3 kap. Elektroniska signaturers rättsverkan och behandlingen av personuppgifter 36
4 kap. Allmän styrning och tillsyn 38
5 kap. Särskilda bestämmelser 39
1.2. Lag om kommunikationsförvaltningen 40
2. Närmare stadganden och bestämmelser 40
3. Ikraftträdande 40
4. Lagstiftningsordning 40

LAGFÖRSLAGEN 44
om elektroniska signaturer 44
om ändring av 2 § lagen om kommunikationsförvaltningen 52

BILAGA.....53

PARALLELLTEXTER.....53
om ändring av 2 § lagen om kommunikationsförvaltningen.....53

ALLMÄN MOTIVERING

1. Inledning

Utvecklingen på kommunikations- och IT-området har medfört tillväxt inom den elektroniska handeln och nätaffärsverksamheten i allmänhet. Verksamheten på området har knappast reglerats alls och utvecklingen har i stor utsträckning styrts av marknadskrafterna. I enlighet med den finska politiken på området har det allmänna inte använt lagstiftning för att ingripa i den i och för sig positiva utvecklingen inom nätaffärsverksamheten.

Den viktigaste tillväxthämmande faktorn inom nätaffärsverksamheten är konsumenternas och andra användares bristande förtroende för verksamheten. Man har inte känt trygghet i fråga om rättsliga handlingar eftersom den personliga kontakten mellan parterna saknas. Nya tjänster och medel har efterfrågats för att kunna identifiera parterna och garantera att informationen inte ändras. Frågan om den elektroniska underskriftens ställning i förhållande till den traditionella namnteckningen har också medfört osäkerhet.

Den nya teknologin erbjuder hela tiden mer och mer avancerade hjälpmedel som kan användas för att på ett tillförlitligt sätt uttrycka och bekräfta viljeyttringar med elektroniska signaturer. Ingen metod möjliggör en fullständig eliminering av risker. De nya kvalificerade certifikaten av hög kvalitet står dock för en mycket hög säkerhetsnivå och stor trygghet.

Lagstiftningen borde inte få hindra rättshandlingar över datanäten. I stället bör lagstiftningen skapa ett nytt och gynnsamt författningsklimat för detta tillvägagångssätt. Användningen av ny teknologi och tillförlitligare tjänster bör främjas, vilket förutsätter specialregler om elektroniska signaturer och certifikat i anslutning till dem. Det finns redan ett direktiv av Europeiska gemenskapen om detta, dvs. Europaparlamentets och rådets direktiv 1999/93/EG om ett gemenskapsramverk för elektroniska signaturer, nedan direktivet om elektroniska signaturer. Direktivet måste införlivas med den nationella lagstiftningen senast den 19 juli 2001.

Den elektroniska signaturen bör uppfattas som vilket som helst undertecknande på teknisk väg, oberoende av använd teknik. Den bör betraktas som en signatur som gör det möjligt att verifiera undertecknarens identitet och att sammanställa personen i fråga med den viljeyttring som skall styrkas med ett undertecknande. Samtidigt bör dock särskild hänsyn tas till elektroniska signaturer som gjorts med mer avancerad teknik, eftersom denna teknik kan öka de elektroniska signaturernas säkerhet och tillförlitlighet märkbart. Bl.a. de digitala underskrifterna som utnyttjar den s.k. öppna nyckelns infrastruktur är signaturer som använder sig av den nya tekniken. I framtiden blir också elektroniska underskrifter som bygger på biometrisk identifikation - t.ex. fingeravtryck – allmännare som en del av signaturframställningsprocessen.

Att signera elektroniskt är mer komplicerat än att personligen underteckna ett meddelande. I den virtuella verkligheten finns ingen ”handstil” som kunde användas som jämförelseobjekt för att fastställa vem underskriften tillhör. Den s.k. certifikatutfärdaren spelar en viktig roll vid elektronisk signering. Tillförlitligheten hos en elektronisk underskrift bygger på att någon instans (certifikatutfärdaren) 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 med hjälp av vilken det är möjligt att öka tillförlitligheten hos den elektroniska kommunikationen. Nedan eftersträvar man genom en beskrivning av metoden med öppna nycklar att klarlägga certifikatutfärdarens ställning i

användningen av elektroniska signaturer.

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

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 s.k. hashvärde. Den elektroniska signeringen genomförs så att den person som skall underteckna informationen kondenserar datamängden och krypterar denna med hjälp av sin hemliga 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 hemliga nyckel som hör samman med den öppna nyckeln. Eftersom den öppna nyckeln är certifierad (dvs. en tredje part har utfärdat undertecknaren ett certifikat och verifierat att den öppna nyckeln i fråga motsvaras endast och uteslutande av den hemliga 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 hemliga nyckeln förblir hemlig. Den hemliga nyckeln finns i allmänhet på något slags plattform, t.ex. ett smartkort, som skyddats med t.ex. en PIN-kod eller ett lösenord när det gäller bankkort. I framtiden kommer biometrisk identifikation såsom fingeravtryck att delvis ersätta användningen av lösenord som baserar sig på användarens minne. Den hemliga nyckeln kan t.ex. också finnas på mobiltelefonens SIM-kort eller som program i den anordning som undertecknaren använder, t.ex. hans eller hennes PC. De hjälpmedel som undertecknaren behöver består huvudsakligen av ett aktivkort som innehåller nycklarna, en kortläsare i datorn samt programvaran i arbetsstationen.

Den öppna nyckelns infrastruktur är förknippad med en mängd olika funktioner som bestämmer hur tillförlitlig signeringen blir. Certifikatutfärdarens agerande är väsentligt med hänsyn till kvalitet och tillförlitlighet.

Certifikatutfärdaren verifierar att en öppen nyckel tillhör en bestämd person. För detta ändamål utfärdar certifikatutfärdaren ett certifikat till undertecknaren.

Certifikaten finns på olika säkerhetsnivå. Vissa certifikat kan beställas direkt över nätet. I detta fall granskas identiteten inte särskilt noggrant. Tillförlitligheten hos dessa certifikat är tillräcklig för vissa ändamål. När certifikat som är säkrare och mer tillförlitliga utfärdas är det mycket viktigt att man försäkrar sig om den sökandes identitet på ett så

tillförlitligt sätt som möjligt. Att identiteten fastställs är av avgörande betydelse för certifikatets tillförlitlighet. Vid elektronisk kommunikation kan parterna inte fysiskt försäkra sig om varandras identitet.

Beroende på användningsändamålet innehåller ett certifikat förutom den öppna nyckeln även annan nödvändig information om undertecknaren. Certifikat kan också utfärdas som s.k. rollcertifikat, varvid certifikatet endast används då man t.ex. agerar för ett affärsföretags räkning.

Certifikaten utfärdas i allmänhet för en bestämd tid. I vissa fall kan det även bli nödvändigt att återkalla certifikaten. Med anledning härav är det viktigt att certifikatutfärdare upprätthåller ett allmänt tillgängligt offentligt register (spärrlista) över de certifikat/öppna nycklar som inte längre är i kraft. De certifikat/öppna nycklar som upptagits på spärrlistan är sålunda inte tillförlitliga. Så långt som möjligt uppdateras spärrlistan online av certifikatutfärdaren.

Den som skall signera information erbjuds ofta den nödvändiga programvaran och maskinvaran, dvs. signeringsredskapen, av certifikatutfärdaren. Certifikatutfärdaren gör nödvändigtvis inte själv allt som behövs utan använder sig av underleverantörer. En hemlig nyckel kan t.ex. överlämnas av en s.k. registrerare som utför uppgifter för certifikatutfärdarens räkning, t.ex. tillförlitlig identifikation av användaren. Underleverantörer kan också användas för att skapa hemliga och öppna nycklar på en bestämd plattform och katalogtjänster kan köpas i form av underleverans hos IT-företag som specialiserat sig på detta område.

Eftersom certifieringen är förknippad med flera delfunktioner och många instanser är det med tanke på ett certifikats tillförlitlighet viktigt att veta vem som i sista hand har ansvaret för certifieringen. Detta är särdeles viktigt när det gäller tillhandahållandet av de i lagförslaget definierade kvalificerade certifikaten som i fråga om tillförlitligheten är avancerade. I den föreliggande propositionen koncentreras ansvaret till en instans. Enligt förslaget skall en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat vara skyldig att ersätta de skador som åsamkats den instans som förlitat sig på certifikatet till följd av att uppgifterna i det kvalificerade certifikatet inte stämmer.

Certifikat används inte bara i kommunikation mellan personer utan också i kommunikation mellan system och anordningar, uttryckligen vid identifikation mellan dessa, för att förbättra tillförlitligheten hos tjänsterna. På Internet är det vanligt att olika servrar känner igen varandra med hjälp av certifikat. Också mobilnätet igenkänner apparaten med hjälp av en metod som bygger på certifieringsteknik. Dessa rent tekniska identifieringsmetoder har dock ingenting att göra med den egentliga signeringen. Den nu föreslagna lagen kommer därför endast att reglera certifikat som används i samband med elektronisk signering.

Elektronisk signering omfattar inte bara själva undertecknandet utan också verifieringen av underskriften. Anordningarna för signaturframställning (programvara och maskinvara) motsvaras av anordningar för signaturverifiering (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 katalogtjänst och spärrlista och det ligger i den tredje partens som förlitar sig på ett certifikat intresse att själv försäkra sig om certifikatets giltighet med hjälp av dessa. Den som verifierar elektroniska signaturer bör skaffa lämpliga och säkra verifieringsanordningar och använda certifikaten för att identifiera undertecknarna och försäkra sig om att informationen är oförvanskad. Genom ett omfattande internationellt standardiseringssamarbete, som beskrivs i punkt 2.3, försöker man garantera hög standard och kompatibilitet på redskap, anordningar och program.

Den kommersiella verksamheten kring produkter som hör samman med tillhandahållandet av certifikat och elektroniska signaturer utvecklas kraftigt. På det internationella planet erbjuds certifikat av flera företag. Företag som i Finland erbjuder tjänster i branschen är bl.a. Certall Finland Ab, Novotrust Ab, Sonera Smart Trust Ab, F-Secure Abp, SSH Communications Security Ab. Certifi-

kat tillhandahålls också av Befolkningsregistercentralen.

2. Nuläge

2.1. Lagstiftning och praxis

Den elektroniska signaturens rättsverkan

Frågor som hör samman med elektronisk kommunikation och elektronisk verifiering har i regel avgjorts med hjälp av reglering och rättslig praxis som varit i kraft sedan länge. De existerande formreglerna för privaträttsliga rättshandlingar känner inte till elektroniska signaturer. Beträffande privaträttsliga avtal innebär de i lagstiftningen oftast förekommande formkraven i regel att avtalet skall uppgöras skriftligen och att det skall undertecknas. Uttrycken ”skriftligen” och ”underteckna” har inte definierats närmare i lagstiftningen.

Den fria bevisprövning som gäller i Finland förutsätter inte någon bestämd form hos bevis. Enligt 17 kap. 2 § rättegångsbalken skall rätten efter samvetsgrann prövning av alla omständigheter som förekommit avgöra vad som skall anses vara sant i målet. Den fria bevisprövningen gäller naturligtvis också elektroniska signaturer och rättshandlingar som utförts med hjälp av dem.

Största delen av de privaträttsliga rättshandlingarna är fria från formkrav på basis av avtal. I fråga om dessa rättshandlingar ger avtalsfriheten och den fria bevisprövningen redan i dagens läge goda möjligheter att använda elektroniska signaturer och certifikat.

Användningen av elektroniska signaturer förutsätter naturligtvis att det både är tillåtet och möjligt att utföra en rättshandling elektroniskt. Det att rättsverkningarna av ett visst slags elektroniska signaturer och traditionella namnteckningar enligt denna proposition fullständigt jämställs med varandra inverkar t.ex. inte på när det skall förutsättas att en rättshandling utförs på papper.

För att formkravet på skriftliga avtal skall uppfyllas även elektroniskt är avsikten att reglera detta separat i en lag om tillhandahållande av informationssamhällets tjänster, för vars beredning justitieministeriet tillsatte en arbetsgrupp (arbetsgruppen för elektronisk handel). Arbetsgruppen tillsattes den 30 maj 2000 i justitieministeriet för att bereda den lagstiftning som behövs för genomförandet av Europaparlamentets och rådets direktiv om elektronisk handel (direktiv om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden 2000/31/EG). Ifrågavarande direktivet skall genomföras nationellt senast den 17 januari 2002. Utlåtanden inbegärdes före den 27 april 2001 om arbetsgruppens betänkande av den 8 mars 2001.

Certifiering av elektroniska signaturer

En reglering av tillhandahållandet av certifikattjänster har skett i samband med att den elektroniska kommunikationen inom förvaltningen har utvecklats. Genom ändringen av befolkningsdatalagen (507/1993) och ändringarna av lagen om registerförvaltningen (166/1996) reglerades Befolkningsregistercentralens ställning som den myndighet som handhar certifikattjänster inom statsförvaltningen. I befolkningsdatalagen inskrevs bl.a. bestämmelser om uppgifterna i certifikat för statsförvaltningens certifierade elektroniska kommunikation, om elektroniska kommunikationskoder och om Befolkningsregistercentralens möjligheter att producera certifikattjänster även för andra myndigheter, företag, samfund och privatpersoner.

I lagen om identitetskort (829/1999) ingår bestämmelser om identitetskort och om elektroniska identitetskort. Elektroniska identitetskort som används vid certifierad elektronisk kommunikation har alltid ett av Befolkningsregistercentralen utfärdat certifikat för elektronisk identifiering av personen i fråga, ett s.k. HST-certifikat. Även andra tillämpningar kan registreras på kortet. Den ändring av 23 § befolkningsdatalagen som gjordes i samband med att lagen om identitetskort stiftades föreskriver bl.a. om förfarandet vid utfärdande av certifikat och om Befolkningsregistercentralens möjligheter att utfärda certifikat även för andra plattformar än identitetskort. Dessa bestämmelser trädde i kraft den 1 december 1999.

Lagen om elektronisk kommunikation i förvaltningsärenden (1318/1999) trädde i kraft den 1 januari 2000. Lagen reglerar användningen av elektroniska dataöverföringsmetoder inom förvaltningen, ansvars-

frågor som gäller skickande och emottagande av elektroniska meddelanden och krav som hör samman med elektronisk verifiering och certifiering i förvaltningsärenden. Enligt lagen skall elektroniska signaturer godkännas vid anhängiggörande av ett förvaltningsärende om certifikatutfärdaren och certifikatet uppfyller kraven i 4 och 5 § i lagen. Enligt 7 § skall certifieringsverksamheten iaktta bl.a. lagen om förvaltningsförfarande (598/1982), språklagen (148/1922), lagen om offentlighet i myndigheternas verksamhet (621/1999) och arkivlagen (831/1994). Dessa krav gäller samtliga certifikatutfärdare som utfärdar certifikat som kan användas inom förvaltningen, även certifikatutfärdare inom den kommersiella sektorn. I praktiken har detta lett till att man genom avtal har uteslutit användningen av kommersiella certifikat vid kommunikation inom förvaltningen, vilket för sin del minskar antalet användare av tjänsterna inom elektronisk kommunikation. Enligt lagens 33 § godkänns dock alltid sådana certifikat av Befolkningsregistercentralen som ingår i elektroniska identitetskort. Enligt 40 § skall finansministeriet upprätthålla en förteckning över certifikat som uppfyller kraven i lagen. Med stöd av 41 § 1 mom. kan en certifikatutfärdare yrka att uppgifter om utfärdaren eller certifikatet skall införas i denna förteckning. Ett beslut i ett sådant ärende får överklagas enligt förvaltningsprocesslagen.

2.2. Europeiska gemenskapernas direktiv om elektroniska signaturer

Europeiska unionens kommission lade den 16 april 1997 fram ett meddelande om ett europeiskt initiativ inom elektronisk handel (KOM(97) 157 slutlig) som förutsatte att ett gemensamt regelverk skulle skapas för identifiering av digitala signaturer och att minimikrav skulle fastställas i fråga om certifikatutfärdare. Den 8 oktober 1997 lade kommissionen fram meddelandet Säkerhet och tillförlitlighet vid elektronisk kommunikation (KOM(97) 503 slutlig). Meddelandet syftade till att utveckla en europeisk modell för digitala signaturer och certifikattjänster. I meddelandet betonades behovet av att separera de elektroniska signaturerna och krypteringen.

Kommissionen lade i oktober 1998 fram ett förslag till Europaparlamentets och rådets direktiv om en gemensam ram för elektroniska signaturer (EGT C 325, 23.10.1998). Europaparlamentets och rådets direktiv om ett gemenskapsramverk för elektroniska signaturer, direktivet om elektroniska signaturer, utfärdades den 30 november 1999 och det trädde i kraft den 19 januari 2000.

Enligt direktivet om elektroniska signaturer är tillhandahållandet av certifikattjänster en fri näring. Det är dock endast certifikat som uppfyller höga, i direktivet definierade kvalitetskrav som kan betraktas som sådana kvalificerade certifikat som garanterar att avancerade elektroniska signaturer som framställts med säkra anordningar för signaturframställning 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 om elektroniska signaturer används termen kvalificerat certifikat. I det följande redovisas direktivets huvudsakliga innehåll artikel för artikel.

Artikel 1. Tillämpningsområde. Syftet med direktivet är 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.

Artikel 2. 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.

Artikel 3. Marknadstillträde. Tillhandahållandet av certifikattjänster får inte vara beroende av förhandstillstånd. Medlemsstaterna får dock införa eller behålla frivilliga ackrediteringssystem. Ackrediteringssystemen

skall vara objektiva, tydliga, proportionella och icke-diskriminerande.

Medlemsstaterna skall 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 skall avgöra om säkra anordningar för skapande av signaturer överensstämmer med kraven i bilaga III. Ett beslut som fattas av ett sådant organ skall erkännas av samtliga medlemsstater.

Sådana produkter för elektroniska signaturer som är förenliga med allmänt erkända standarder skall 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 skall vara objektiva, tydliga, proportionella och icke-diskriminerande. Dessutom skall de endast gälla de särskilda egenskaperna för tillämpningen i fråga. Dessa krav får inte utgöra ett hinder för gränsöverskridande tjänster för medborgaren.

Artikel 4. Principer för den inre marknaden. Varje medlemsstat skall 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, på de områden som omfattas av direktivet. Dessutom skall medlemsstaterna säkerställa att produkter för elektroniska signaturer har fri rörlighet på den inre marknaden.

Artikel 5. Rättslig verkan för elektroniska signaturer. Medlemsstaterna skall 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 skall 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.

Artikel 6. Skadeståndsansvar. 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 skall 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 skall 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. Internationella aspekter. Artikeln 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.

Artikel 8. Dataskydd. Medlemsstaterna skall 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 skall 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.

Bilaga I. Krav på kvalificerade certifikat. Ett kvalificerat certifikat skall 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.

Bilaga II. Krav på tillhandahållare av certifikattjänster vilka 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, tillräckliga medel och lämpliga försäkringar, förbud att lagra signeringsnyckeln, arkiveringsskyldighet och skyldighet att informera användarna när certifikat utfärdas.

Bilaga III. Krav på säkra anordningar för skapande av signaturer. Anordningarna skall 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 skall 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 skall signeras och inte heller förhindra att dessa uppgifter presenteras för undertecknaren före undertecknandet.

Bilaga IV. Rekommendationer för säker signaturverifiering. Enligt rekommendationerna skall 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.

2.3. Den internationella utvecklingen och lagstiftningen i utlandet

Sverige, Norge och Danmark

I Sverige har en lag om certifiering av elektroniska signaturer (regeringens proposition 1999/2000:117, lag om kvalificerade elektroniska signaturer, m.m.) trätt i kraft den 1 januari 2001. Lagen genomför bestämmelser av direktivet om elektroniska signaturer i Sverige.

Den norska regeringen avlät i september 2000 en proposition om elektroniska signaturer (lov om elektronisk signatur, Ot.prp.nr.82) till Stortinget. Den norska lagen trädde i kraft den 1 juli 2001. Den danska lagen (lov om elektroniske signaturer, lov nr. 417 af 31. maj 2000) har trätt i kraft den 1 oktober 2000. Dessa lagar genomför bestämmelser av direktivet om elektroniska signaturer i Norge respektive Danmark.

Den svenska, den norska och den danska

lagen liknar i stor utsträckning den finska lagen. Sverige, Norge och Danmark har i sina nationella bestämmelser gett avancerade elektroniska signaturer samma rättsliga verkan som den traditionella handskrivna namnteckningen har. I den svenska lagen ingår inte någon bestämmelse om att inte heller andra elektroniska signaturer får fråntas sin rättsverkan och sin godtagbarhet enbart till följd av att signaturen har gjorts i elektronisk form. I den danska lagen finns det inte heller något omnämnande av rättsverkan för andra signaturer än avancerade signaturer. I den norska lagen utsägs det däremot att även andra signaturer än avancerade signaturer kan jämställas med handskrivna underskrifter. I lagen i denna proposition har man för avsikt att inta en bestämmelse om elektroniska signaturer, en bestämmelse som i fråga om rättsliga verkningar skall jämställa åtminstone avancerade elektroniska signaturer med handskrivna underskrifter. Med anledning av den fria bevisprövning och princip om avtalsfrihet som iakttas vid finska domstolar är det klart att inte heller andra elektroniska signaturer fråntas sin rättsverkan och sin godtagbarhet i Finland enbart till följd av namnteckningens elektroniska form.

Den viktigaste skillnaden mellan den danska lagen och de andra nordiska lagarna är den granskare (revisor) som ingår i det danska systemet. Kvalificerade certifikatutfärdare skall utse en utomstående av staten auktoriserad inspektör för att inspektera systemen (revision). I särskilda fall kan den danska telestyrelsen avvika från kravet att det uttryckligen skall vara fråga om en av staten auktoriserad inspektör. Revisorn rapporterar till telestyrelsen, i enlighet med de närmare anvisningar som styrelsen utfärdar, om den kvalificerade certifikatutställarens system uppfyller lagens krav. Motsvarande system finns inte i de andra nordiska länderna och avses inte heller bli infört i den finska lagstiftningen.

I Sverige har man i fråga om kvalificerat certifikat utöver avancerad elektronisk signatur av certifikatutfärdaren dessutom godkänt en annan elektronisk signatur med motsvarande säkerhetsnivå.

Vissa andra länder

Den tyska lagen om digitala signaturer (Signaturgesetz) trädde i kraft redan den 1 augusti 1997 som en del av en större allmän lag om informations- och kommunikationstjänster (Informations- und Kommunikationsdienste Gesetz). I lagen ingår bestämmelser om bl.a. tillträde till branschen, informationsplikt, avslutande av verksamhet och tidsstämpling. Med stöd av lagen utfärdades dessutom en mängd tekniska författningar. I Tyskland har branschtillträdet kritiserats. Det har ansetts vara alltför dyrt till följd av de tunga förpliktelser som de olika författningarna föreskriver. Den nämnda lagen om digitala signaturer (Signaturgesetz) upphävdes den 22 maj 2001, när den nya lagen om elektroniska signaturer (Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderungen weiterer Vorschriften) trädde i kraft. I Tyskland pågår som bäst beredningen av en förordning i anslutning till lagen, genom vilken detaljerna i kraven på dem som tillhandahåller certifikattjänster preciseras.

I Förenta staterna trädde en federal lag om elektroniska signaturer i kraft den 30 juni 2000 (Electronic Signatures in Global and National Commerce Act, Public Law No: 106–229). Utgångspunkten är att elektroniska signaturer skall ha samma rättsverkan som egenhändiga namnunderskrifter. Lagen förutsätter ingen användning av några som helst certifikattjänster i samband med elektroniska signaturer, men lagen kräver ett uttryckligt medgivande av konsumenten för att elektroniska signaturer skall få användas. Dessutom kan tilläggskrav i annan lagstiftning, t.ex. i fråga om formkrav för vissa avtal eller rättsliga handlingar hindra att elektroniska signaturer används. Syftet med den amerikanska lagen är framför allt att möjliggöra användning av elektroniska signaturer och elektroniska dokument genom att förutsätta att rättsliga handlingar inte får fråntas rättsverkan enbart på den grund att rättshandlingen i fråga har utförts i elektronisk form.

Internationella organisationer

Arbetsgruppen för elektronisk handel inom Förenta Nationernas, nedan FN, kommission för internationell handelsrätt UNCITRAL, nedan UNCITRAL, har allt sedan januari 1998 arbetat med en modellag om elektroniska signaturer, nedan modellagen. Meningen är att modellagen och de instruktioner som hör samman med den (Guide to Enactment) skall godkännas slutligt vid UNCITRAL:s 34:e möte sommaren 2001.

Arbetet med UNCITRAL:s modellag har erbjudit ett behövligt internationellt debattforum för FN-staterna vid utvecklandet av regleringen rörande elektroniska signaturer. Förslaget till modellag har redan i sig fungerat som exempel för lagberedningen, särskilt i icke-europeiska länder. Lagstiftningsprojekt som beaktat problem och problemlösningar som aktualiserats i samband med arbetet på modellagen har varit under arbete eller slutförts i bl.a. Argentina, Australien, Brasilien, Indien, Kanada, Korea, Mexiko, Nya Zeeland, Rumänien, Thailand och Singapore. Resultaten av arbetet med UNCITRAL:s modellag användes också i arbetet med direktivet om elektroniska signaturer. Europeiska unionens kommission och medlemsstater har deltagit aktivt och påverkat modellagsarbetet i arbetsgruppen för elektronisk handel även sedan direktivet trätt i kraft.

Den senaste versionen av modellagen finns att tillgå på UNCITRAL:s webbsidor, adress http://www.uncitral.org/en-index.htm, dokument A/CN.9/WG.IV/WP.88. Den innehåller liknande bestämmelser som direktivet om elektroniska signaturer om bl.a. elektroniska signaturers rättsverkan, certifikatsinnehåll, certifikatutställaransvar och ömsesidigt godkännande av certifikat. Modellagen skiljer sig från direktivet om elektroniska signaturer sålunda att den betonar avtalsparternas rätt att genom avtal avvika från modellagens bestämmelser. Utgångspunkten som betonar avtalsparternas autonomi är närmast en följd av Förenta staternas starka inflytande i arbetet på modellagen. Till skillnad från direktivet innehåller modellagen också bestämmelser om undertecknarens ansvar. I modellagen föreskrivs bl.a. att undertecknaren är skyldig att uppbevara nyckeln omsorgsfullt och att undertecknaren är skyldig att underrätta certifikatutfärdaren omedelbart om nyckeln försvinner och om andra händelser som äventyrar signaturens säkerhet.

Standardisering

I syfte att genomföra de krav som uppställs i direktivet om elektroniska signaturer har ett samprojekt inrättats för europeisk industri och standardiseringsorgan, European Electronic Signature Standardization Initiative, nedan EESSI. Inom ramen för EESSI-projektet sker ett omfattande standardiseringsarbete vid European Telecommunications Standards Institute, nedan ETSI och European Committee for Standardization, nedan CEN för att ta fram standarder för produkter, system och tjänster som hör samman med elektroniska signaturer.

Standardiseringsarbetet bygger på s.k. PKI-infrastruktur (Public Key Infrastructure, nedan PKI) med hjälp av vilken man kan uppfylla kravet på säker kommunikation. De första resultaten av standardiseringsarbetet färdigställdes i slutet av 2000 och fler arbetsområden blir klara under 2001. Standardiseringsarbetet syftar också till att producera färdiga tillämpningar för fri distribution för att stödja marknadstillväxten och bidra till ökad standardisering.

Standardiseringsorganen och forumen utför också ett omfattande internationellt samarbete över de europeiska gränserna. Uppgiftsområden inom EESSI-projektet handhas av ETSI och CEN i samarbete med bl.a. IETF (International Engineering Task Force) och W3C (World Wide Web Consortium).

2.4. Bedömning av nuläget

Marknadsutsikterna för certifikaten bedöms vara goda. Certifikaten håller på att bli ett viktigt medel för att öka tillförlitligheten inom kommunikationen på nätet. Man räknar med att nätaffärsverksamheten skall öka kraftigt varvid även efterfrågan på certifikat ökar. Fastän marknaden för certifikat ännu inte funnit sin slutliga form utvidgas användningsområdet för certifikat hela tiden. Vid sidan av certifikaten tas olika tilläggstjänster fram, t.ex. tjänster för nyckelhantering och

notariattjänster.

Med stöd av principen om allmän avtalsfrihet kan parterna fritt välja om de vill utföra en rättshandling eller inte. Den grundläggande principen för rättsliga handlingar är formfrihet, vilket innebär att handlingen kan ske på det sätt som parterna önskar. I dagens läge råder oklarhet om de elektroniska signaturernas status och rättsverkan, även om den fria bevisprövningen och avtalsfriheten i Finland ger goda möjligheter att använda dem.

I syfte att främja nätaffärsverksamheten, särskilt öka dess tillförlitlighet, är det dock skäl att genom lag reglera tillhandahållandet av certifikat och de elektroniska signaturernas rättsverkan. Dessutom är det nödvändigt att utfärda en lag som införlivar bestämmelserna i direktivet om elektroniska signaturer med den finska lagstiftningen.

Genom lagen i lagförslaget jämställs en avancerad elektronisk signatur som överensstämmer med definitionerna i direktivet om elektroniska signaturer med den traditionella handskrivna namnteckningen. Eventuella andra formkrav som ställs på rättshandlingar regleras på annat håll i lagstiftningen. Med tanke på näthandelns och de elektroniska tjänsternas utveckling vore det ytterst viktigt att användningen av en avancerad elektronisk signatur som skapats med en säker anordning för signaturframställning och som är baserad på ett kvalificerat certifikat som uppfyller de krav som ställs i den föreslagna lagen skall vara möjlig inom såväl den privata som den offentliga sektorn. Detta vore en central faktor även med tanke på att de elektroniska tjänsterna skall vara lätta att använda.

När de författningar som gäller myndigheternas elektroniska kommunikation revideras kunde det hänvisas till den lag som stiftats i enlighet med detta lagförslag när det gäller sådan certifieringsverksamhet och sådana certifikat som godkänns inom förvaltningstjänsterna. I detta sammanhang bör man också bedöma ett eventuellt behov av att ändra bestämmelserna i befolkningsdatalagen om tjänster i anslutning till certifierad elektronisk kommunikation. Detta är nödvändigt i synnerhet beträffande det datainnehåll i ett certifikat för elektronisk kommunikation inom statsförvaltningen, utfärdat av Befolkningsregistercentralen, som definieras i 20 § befolkningsdatalagen.

En elektronisk signatur hör alltid nära samman med en viljeyttring som avser elektronisk information, t.ex. signering av ett avtal. Certifikattjänster som inte hör samman med ett bestämt innehåll används redan i stor utsträckning över nätet. Sådana tjänster är t.ex. identifiering av en användares anslutning för erbjudande av tjänster inom mobilkommunikation eller verifiering mellan servrarna med hjälp av certifikattjänster. Utbudet av dessa tjänster förutsätter inte att den föreslagna lagen skall utsträckas till att omfatta även dem.

3. Propositionens mål och de viktigaste förslagen

Att öka konsumenternas förtroende för nätkommunikation och elektronisk handel är viktigt för framgång i affärsverksamhet över nätet. Certifikaten spelar i detta avseende en betydande roll. För att öka konsumentens förtroende är det ändamålsenligt att lagfästa grunderna för certifiering av hög kvalitet, elektroniska signaturers rättsverkan och centrala ansvarsfrågor. Dessutom förutsätter direktivet om elektroniska signaturer detta.

Certifikatutfärdarna sysslar huvudsakligen med kommersiell verksamhet. En särskild sektor utgörs av den elektroniska kommunikationen inom förvaltningen, om vilken det finns särskild lagstiftning. Certifikatens användningsområde kommer huvudsakligen att gälla uttryckligen kommersiell verksamhet och detta kommer att betonas ytterligare då nätaffärsverksamheten ökar och certifikaten får större användning inom mobilkommunikationen. En tillförlitlig certifieringsverksamhet och utvecklingen på området tryggas bäst om man tillser att de som tillhandahåller tjänster kan konkurrera med varandra på lika villkor. Dessutom skall det vara så enkelt som möjligt att få tillträde till branschen.

Författningsramen skall inte genom bestämmelser om extra skyldigheter skapa onödiga kostnader för en affärsverksamhet vars existens och framgångar bygger på förtroende hos användarna. Meningen är att målet skall uppnås genom så lätt reglering som möjligt inom ramen för direktivet om elektroniska signaturer, en reglering som fokuse-

rar endast på det nödvändigaste. Denna tanke betjänas bl.a. av att regleringen koncentreras till att gälla den certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat. Meningen är att den direkta regleringen inte skall omfatta de för certifieringsverksamheten typiska instanserna som bistår certifikatutfärdaren, t.ex. upprätthållarna av spärrlista, tillverkarna av hemliga nycklar eller de s.k. registrerarna som ofta överlämnar certifikaten till användarna. En certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat skall genom avtal med de nämnda instanserna se till att skyldigheterna genomförs. En certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat skall likväl vara den instans som utåt skall svara för certifieringsverksamhetens tillförlitlighet. Detta förenklar situationen för användaren eftersom det i en problemsituation finns tydligare gränsytor för ansvaret. Dessutom förenklas och förtydligas tillsynen över certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat.

Den helhet som certifieringen bildar har flera delområden och nya tjänster utvecklas hela tiden. Syftet är att försöka skapa gynnsamma utvecklingsförutsättningar för de nya tjänsterna. Detta eftersträvas så att man inom ramen för direktivet om elektroniska signaturer koncentrerar bestämmelserna i den föreslagna lagen till att omfatta i synnerhet elektroniska signaturer och de kvalificerade certifikat som behövs för dessa. Andra tjänster i samband med certifiering, t.ex. tjänster som gäller tidsstämpling och notariattjänster, blir fria näringar som lyder under annan lagstiftning.

Avsikten med lagförslaget är också att öka antalet användare av tjänsterna inom den elektroniska kommunikationen. Till följd av besvärligheter och osäkerhet som beror på de gällande bestämmelserna om elektronisk kommunikation har i allmänhet tjänsterna inom den offentliga förvaltningen avgränsats från användningsområdet för kommersiella certifikat. Situationen kan inte anses ändamålsenlig med tanke på tjänsterna inom den elektroniska kommunikationen som helhet. Avsikten är att skapa förutsättningar för en helhet där medborgaren kan välja ett säkert certifikat och använda detta såväl för kommersiella tjänster som inom förvaltningen. Det vore ändamålsenligt att eftersträva en situation där de säkra certifikaten kunde fastställas på ett enda ställe så att användaren skulle kunna få så tydlig och exakt information som möjligt om certifikat för olika tjänster samt om deras tillförlitlighet. Hur helheten fungerar blir också beroende av ändringen av lagen om elektronisk kommunikation i förvaltningsärenden.

Avsikten är att med hjälp av lagförslaget klarlägga elektroniska signaturers rättsverkan. Såsom redan ovan har nämnts erbjuder den fria bevisprövningen och avtalsfriheten i Finland redan nu möjligheter att använda elektroniska signaturer. För att öka möjligheterna att förutse verkningarna vill man i enlighet med direktivet om elektroniska signaturer ge avancerade elektroniska signaturer som baserar sig på ett kvalificerat certifikat och som har skapats med en säker anordning för signaturframställning samma status som de traditionella handskrivna namnunderskrifterna. Också i fortsättningen skall parterna likväl fritt kunna avtala om användningen av andra elektroniska signaturer. Övriga eventuella formkrav som anknyter till rättshandlingar skall gälla i enlighet med vad som föreskrivs om dem eller vad som avtalats om dem.

Avsikten är även att med hjälp av förslaget förtydliga de ansvarsfrågor som hör samman med certifiering. Genom förslaget skall ansvaret för den som tillhandahåller allmänheten kvalificerade certifikat fastställas. En dylik certifikatutfärdare skall särskilt i lag angivna fall ansvara för skada som har åsamkats den som har förlitat sig på ett kvalificerat certifikat, om inte certifikatutfärdaren enligt omvänd bevisbörda kan påvisa att han har förfarit omsorgsfullt. Undertecknaren skall för sin del åläggas skyldighet att omedelbart begära att den certifikatutfärdare som utfärdat det kvalificerade certifikatet återkallar hans eller hennes kvalificerade certifikat, om undertecknaren har grundad anledning att anta att signaturframställningsdata används obehörigt.

4. Propositionens verkningar

4.1. Ekonomiska verkningar

Det anses att ett tillförlitligt och effektivt utbud av certifikat för sin del förbättrar villkoren för bedrivande av nätaffärsverksamhet på ett betydande sätt. Nätaffärsverksamhetens ekonomiska betydelse kommer att växa snabbt under de närmaste åren. Nätaffärsverksamheten förbättrar produktiviteten och propositionen kommer därför att ha en positiv betydelse för samhällsekonomin. Det är dock svårt att beräkna verkningsvolymen eftersom certifikatmarknaden är under utveckling och eftersom olika tjänster i anslutning till certifikat torde tillhandahållas som tilläggstjänster i samband med andra tjänster, t.ex. mobiltjänster. Därför är det också svårt att bedöma hur de ekonomiska verkningarna kommer att påverka företag av olika storlek.

Propositionens direkta effekter på sysselsättningen är små. Arbetsplatserna hos företag som tillhandahåller certifikat och hos underleverantörer kommer att öka. De indirekta sysselsättningseffekterna är svåra att bedöma.

Det antas att propositionen också kommer att leda till ökad användning inom förvaltningen av till buds stående tjänster inom elektronisk kommunikation då användningen av certifikat ökar.

Propositionen har inga verkningar på statsbudgeten.

4.2. Verkningar i fråga om organisation och personal

Det föreslås att övervakningen av certifieringsverksamheten skall skötas av Kommunikationsverket. Enligt preliminära beräkningar kommer personalbehovet att öka vid Kommunikationsverket med 2–3 personer. Behovet av personal kan bli större beroende dels på antalet företag som kommer att tillhandahålla certifikat i framtiden, dels på den allmänna marknadsutvecklingen. Kommunikationsverket finansierar sina utgifter med övervakningsavgifter som uppbärs hos de instanser som kontrolleras. De totala utgifterna beräknas uppgå till 340 tusen euro (2 miljoner mark) om året.

Då användningen av elektroniska signaturer ökar kommer den elektroniska kommunikationen sannolikt att öka också inom den offentliga förvaltningen. Med tiden kommer detta att ändra behovet av och uppgifterna för den personal som sköter kundbetjäning och kontorsuppgifter. I princip kan detta leda till större arbetslöshet, om man inte uppmärksammar frågan. Eftersom medborgarnas beredskap för elektronisk kommunikation ökar rätt långsamt, kommer också behovet av eventuella personalminskningar inom den offentliga sektorn att ske i långsam takt. Å andra sidan kan det antas att behovet av arbetskraft uttryckligen kommer att öka i uppgifter som gäller elektronisk kommunikation. Genom att överföra resurser från traditionell kundbetjäning till nya uppgifter och genom personalutbildning kommer man att kunna hantera eventuella verkningar på sysselsättningen. Att den elektroniska kommunikationen ökar inom den offentliga förvaltningen kommer sålunda inte att leda till större arbetslöshet, om man på förhand beaktar de effekter som strukturomvandlingen har på sysselsättningen.

4.3. Miljökonsekvenser

Man räknar inte med att lagen kommer att ha några direkta miljökonsekvenser. Att ärenden sköts på elektronisk väg kommer att minska användningen av pappersbaserade dokument. Det är dock omöjligt att bedöma vilka verkningar som användning av elektroniska signaturer kommer att ha på t.ex. konsumtionen av papper.

4.4. Verkningar för olika medborgargrupper

Då de elektroniska tjänsterna ökar och då handläggningen av ärenden automatiseras allt mer, kommer betydelsen av elektroniska signaturer att växa. Arbetet med att fylla i och skicka dokument i pappersformat minskar då man övergår till en allt mer omfattande elektronisk behandling. Medborgarnas beredskap och möjligheter till elektronisk kommunikation ökar hela tiden. Då ärenden inte längre sköts fysiskt i samma utsträckning som tidigare, blir det lättare att sköta olika ärenden

och vissa särskilda grupper, t.ex. rörelsehindrade personer, gagnas av den elektroniska kommunikationen. Man kan därför anse att allt fler tjänster blir tillgängliga för användarna på mer lika villkor än förut i och med att de elektroniska tjänsterna och den elektroniska kommunikationen ökar.

5. Beredningen av propositionen

5.1. Beredningsskeden och beredningsmaterial

Propositionen har utarbetats vid kommunikationsministeriet som tjänsteuppdrag. Ministeriet har hört olika parter i stor omfattning. Under behandlingen av direktivet om elektroniska signaturer och beredningen av lagen ordnades offentliga s.k. hearings om elektroniska signaturer i justitieministeriet och trafikministeriet.

Kommunikationsministeriet har under beredningen av förslaget samarbetat med justitieministeriet, som beredde lagen om elektronisk kommunikation i förvaltningsärenden. Justitieministeriet bereder som bäst en allmän lag om elektronisk kommunikation som gäller hela myndighetsfältet (lagen om elektronisk kommunikation i myndigheternas verksamhet). I samband med att den allmänna lagen träder i kraft upphävs lagen om elektronisk kommunikation i förvaltningsärenden. I det lagförslag som nu är under beredning skall inte tas in bestämmelser om certifikat och certifiering, utan när det gäller dem är avsikten att hänvisa till den lag som ingår i denna proposition.

När lagen om elektronisk kommunikation i förvaltningsärenden utarbetades och utfärdades visste man att den allmänna lagen som man avsåg att ge senare sannolikt skulle medföra behov av ändring av lagen om elektronisk kommunikation i förvaltningsärenden. När lagen gavs förutsatte riksdagen att regeringen skulle tillse att riksdagen får en från den allmänna lagen separat proposition om lagen behöver ändras. Dessutom förutsatte riksdagen en separat beredning av ett lagförslag om effektivare och närmare reglerade ackrediteringssystem för certifikatutfärdare inom den offentliga sektorn.

Om oförenlighet mellan lagarna skall kunna undvikas kräver den nu föreslagna allmänna lagen en ändring av lagen om elektronisk kommunikation i förvaltningsärenden, åtminstone i fråga om bestämmelserna om certifieringsverksamheten, sålunda att dessa ändringar kan träda i kraft samtidigt som den allmänna lagen. Målet är att lagen om elektronisk kommunikation i förvaltningsärenden upphävs i samband med ikraftträdandet av lagen om elektronisk kommunikation i myndigheternas verksamhet, vilken är under beredning i justitieministeriet, och att alla bestämmelser om certifiering och certifikat skall ingå i detta lagförslag. Det mest ändamålsenliga vore att det lagförslag som justitieministeriet bereder och föreliggande lagförslag behandlas och träder i kraft samtidigt. Eftersom notifieringsförfarandet, med stöd av Europaparlamentets och rådets direktiv 98/34/EG, ändr. 98/48/EG, om ett informationsförfarande beträffande tekniska standarder och föreskrifter (det s.k. transparensdirektivet), som gäller den proposition som bereds vid justitieministeriet inte har slutförts när denna proposition överlåts, torde behandlingen av denna proposition dock kunna inledas redan innan justitieministeriets proposition har blivit färdig.

Eftersom certifikatmarknaderna fortfarande är under utveckling och eftersom det samarbete som eventuellt behövs mellan aktörerna i branschen än så länge i regel håller på att utformas är det inte aktuellt att på lagnivå reglera status, struktur eller relation till övriga aktörer för eventuella ackrediteringssystem som behövs för att främja helheten.

För att certifieringsverksamheten skall bli vanligare vore det önskvärt att alla instanser som förlitar sig på elektroniska signaturer godkänner åtminstone sådana avancerade elektroniska signaturer som skapats med en säker anordning för signaturframställning och som är baserade på ett sådant kvalificerat certifikat som definierats i den allmänna lagen. På detta sätt behöver certifikatutfärdarna inte separat överväga huruvida det kvalificerade certifikat som de tillhandahåller uppfyller de krav som den offentliga förvaltningen ställer.

Lagförslaget har med stöd av Europaparlamentets och rådets direktiv 98/34/EG, ändr. 98/48/EG, om ett informationsförfarande be-

träffande tekniska standarder och föreskrifter (det s.k. transparensdirektivet) anmälts till Europeiska gemenskapernas kommission (Finlands anmälan 2001/125/FIN, 12.3.2001). I kommissionens meddelande SG(2001) D/50601 har de anförda anmärkningarna samt de genom kommissionens meddelande SG(2001) D/51365 anförda anmärkningarna av Sverige beaktats i den fortsatta beredningen av lagförslaget. De anmärkningar som gjorts om lagförslaget har inte förlängt väntetiden, som gick ut den 12 juni 2001.

5.2. Utlåtanden

Utlåtanden om utkastet till proposition har begärts av alla ministerier samt på ett omfattande plan av myndigheter och statliga ämbetsverk i olika branscher samt av företrädare för handeln och industrin inom företagssektorn.

Utlåtanden inlämnades av justitieministeriet, inrikesministeriet, handels- och industriministeriet, försvarsministeriet, undervisningsministeriet, social- och hälsovårdsministeriet, arbetsministeriet, finansministeriet, Ålands landsskapstyrelse, arkivverket, Försörjningsberedskapscentralen, centralkriminalpolisen, Konkurrensverket, Konsumentverket, huvudstaben, Finansinspektionen, Teleförvaltningscentralen (nuvarande Kommunikationsverket), Dataombudsmannens byrå, Skattestyrelsen och Befolkningsregistercentralen.

Utlåtanden inkom även av Certall Finland Ab, CSC-Tieteellinen laskenta Ab, Elisa Communications Abp, Ficom rf, Finnetförbundet rf, Gramex rf, Helsingfors handelskammare, Centralhandelskammaren, Kopiosto rf, Kuluttajat-Konsumenterna rf, ICL Invia Abp, Mainostajien Liitto-Annonsörernas Förbund rf, Markkinointiviestinnän Toimistojen Liitto MTL rf, Merita Bank Abp, Mätteknikcentralen, Niksu Ab, Novotrust Ab, Andelsbankscentralen-ABC andelslag, Päijät-Hämeen Puhelin Abp, Sampo Bank Abp, Sanoma-WSOY Abp, Siemens Ab, Sonera Smart Trust Ab, Forsknings- och utvecklingscentralen för social- och hälsovården STAKES, Suomen ATK-oikeudellinen yhdistys rf, Bankföreningen i Finland rf, Finska Patentombudsförening rf, Posten Finland Abp, Suomen Suoramarkkinointiliitto rf, Finska Försäkringsbolagens Centralförbund, Företagarna i Finland rf, Säveltäjäin Tekijänoikeustoimisto Teosto rf, Teknologiska utvecklingscentralen Tekes, Teollisuuden ja Työnantajain Keskusliitto-Industrins och Arbetsgivarnas Centralförbund rf, Utvecklingscentralen för Informationsteknologi TIEKE rf och Työeläkevakuuttajat TELA-Arbetspensionsförsäkrarna TELA rf.

Allmänt taget förhöll de tillfrågade sig positivt till utkastet och lagförslaget ansågs främja möjligheterna att tillhandahålla elektroniska tjänster.

Ålands landskapsstyrelse har i sitt utlåtande fäst uppmärksamhet vid vissa specialfrågor i anknytning till lagens tillämpningsområde inom landskapet, t.ex. svenska språkets ställning och personuppgiftslagens tillämplighet i landskapet. Landskapsstyrelsen har dessutom i sitt utlåtande fäst uppmärksamhet vid det faktum att anmälan om inledande av verksamhet till den övervakande myndigheten enligt förslaget krävs för att ett kvalificerat certifikat skall utfärdas. Enligt lagförslaget är Kommunikationsverket en sådan myndighet. Landskapsstyrelsen anser att regleringen av verksamheten med kvalificerade certifikat med stöd av självstyrelselagen för Åland likväl omfattas av Ålands landstings lagstiftningsbehörighet.

6. Andra omständigheter som inverkat på propositionens innehåll

Propositionen hänför sig till den tidigare nämnda lagen om elektronisk kommunikation i förvaltningsärenden. Som bäst bereder justitieministeriet en allmän lag om elektronisk kommunikation för hela myndighetsfältet (lagen om elektronisk kommunikation i myndigheternas verksamhet). I samband med att den allmänna lagen träder i kraft skall lagen om elektronisk kommunikation i förvaltningsärenden upphävas. I det lagförslag som nu är under beredning skall inte tas in bestämmelser om certifikat och certifiering, utan när det gäller dem är avsikten att hänvisa till lagen i detta lagförslag. Det mest än-

damålsenliga vore att det lagförslag som justitieministeriet bereder och det nu föreslagna lagförslaget behandlas och träder i kraft samtidigt. Eftersom notifieringsförfarandet, med stöd av Europaparlamentets och rådets direktiv 98/34/EG, ändr. 98/48/EG, om ett informationsförfarande beträffande tekniska standarder och föreskrifter (det s.k. transparensdirektivet), som gäller den proposition som bereds vid justitieministeriet inte har slutförts när denna proposition överlåts, torde behandlingen av denna proposition dock kunna inledas redan innan justitieministeriets proposition har blivit färdig.

Propositionen har också samband med den lag om tillhandahållande av informationssamhällets tjänster som justitieministeriet bereder. För beredningen av lagen tillsattes den 30 maj 2000 vid justitieministeriet en separat arbetsgrupp (arbetsgruppen för elektronisk handel). I det lagförslag som bereds föreskrivs bl.a. om att kravet på skriftlig form på avtal skall uppfyllas elektroniskt. Arbetsgruppen för elektronisk handel tillsattes för att bereda den lagstifning som behövs för genomförandet av Europaparlamentets och rådets direktiv om elektronisk handel (direktiv om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden 2000/31/EG). Ifrågavarande direktivet skall genomföras nationellt senast den 17 januari 2002. Utlåtanden om arbetsgruppens betänkande av den 8 mars 2001 har inbegärts före den 27 april 2001.

DETALJMOTIVERING

1. Lagförslag

1.1. Lag om elektroniska signaturer

1 kap. **Allmänna bestämmelser**

1 §. *Lagens syfte*. Syftet med lagen är att underlätta användningen av elektroniska signaturer och tillhandahållandet av produkter för elektroniska signaturer och tjänster i anslutning till dem. Ytterligare ett syfte med lagen är att främja datasekretessen och dataskyddet vid elektronisk handel och elektronisk kommunikation.

Användningen av elektroniska signaturer skall underlättas genom att en i lag definierad avancerad elektronisk signatur som är baserad på ett kvalificerat certifikat och som har skapats med en säker anordning för signaturframställning skall få samma rättsliga ställning som egenhändigt utförda namnteckningar.

Tillhandahållandet av produkter för och tjänster i anslutning till elektroniska signaturer underlättas bl.a. genom att produkterna och tjänsterna garanteras fri rörlighet inom Europeiska ekonomiska samarbetsområdet på det sätt som framgår av lagens 4, 5 och 8 §.

Datasekretessen och dataskyddet vid elektronisk handel och elektronisk kommunikation samt företagens och konsumenternas förtroende för certifikaten främjas genom lagens bestämmelser om egenskaperna för kvalificerade certifikat, certifikatutfärdarens skyldigheter och skadeståndsskyldighet samt myndighetstillsynen över certifikatutfärdare.

Genom lagens 1 och 3 § genomförs artikel 1.1 i direktivet.

2 §. *Definitioner*. Enligt paragrafens 1 punkt betyder en elektronisk signatur data i elektronisk form som är fogade eller knutna till andra elektroniska data och som används som en metod för verifiering av undertecknarens identitet. En elektronisk signatur uppstår genom att elektroniska data i elektronisk form fogas till varandra på ett sådant sätt att de bildar en unik kombination som gör det möjligt att verifiera undertecknaren.

Användningen av en elektronisk signatur i ett system som utnyttjar en teknik med öppen nyckel (det öppna nyckelsystemet) för underskrift och identifiering går till så att undertecknaren med sin hemliga nyckel krypterar det kondensat av meddelandet som framställts med hjälp av en algoritm. Det krypterade kondensatet av meddelandet fungerar som en elektronisk signatur, som skickas tillsammans med det elektroniska meddelandet.

I punkt 2 i paragrafen definieras en avancerad elektronisk signatur. Den elektroniska signaturen skall uppfylla de särskilda kraven i underpunkterna a-d i punkt 2 för att det skall vara fråga om en avancerad elektronisk signatur.

En avancerad elektronisk signatur skall enligt underpunkt a 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 punkt 4.

En avancerad elektronisk signatur skall enligt underpunkt b göra det möjligt att identifiera undertecknaren. Certifikatutfärdaren kan därmed inte utfärda identiska certifikat till två olika personer. De personer till vilka certifikat utfärdats skall kunna skiljas från varandra genom särskilda kännetecken eller åtminstone genom certifikatens serienummer.

De medel med vilka en avancerad elektronisk signatur är skapad skall enligt underpunkt c 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 hemliga nyckeln.

Enligt den sista underpunkten skall en avancerad elektronisk signatur vara knuten till andra elektroniska data på ett sådant sätt att förvanskningar av dessa data kan upptäckas. Signaturen skall 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.

Med en undertecknare avses enligt 3 punkten en fysisk person som lagligen innehar signaturframställningsdata. En undertecknare kan enligt definitionen i punkt 3 aldrig vara en juridisk person, men undertecknaren kan dock representera en fysisk eller en juridisk person och agera i dennas ställe. Därmed är även signaturer framställda inom ramen för s.k. rollcertifikat, då en fysisk person representerar det företag i vars namn personen agerar, omfattas av definitionen på en undertecknare. En laglig representant för ett företag kan t.ex. införas i certifikatet för signaturen enligt förutsättningarna i 7 § 2 mom. 9 punkten. I samma syfte kan även ett tillägg fogas till certifikatet av vilket framgår personens rätt att agera i företagets ställe.

Med signaturframställningsdata avses enligt 4 punkten de unika data som används för att skapa en elektronisk signatur. Inom det öppna nyckelsystemet är signaturframställningsdata undertecknarens hemliga 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 hemliga nyckeln.

En anordning för signaturframställning är enligt 5 punkten maskin- eller programvara som används som hjälpmedel för att skapa en elektronisk signatur. 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 hemliga nyckel. Dessutom innehåller anordningen för signaturframställning särskild programvara för skapande av den elektroniska signaturen.

Med signaturverifieringsdata avses enligt 6 punkten data som används av mottagaren för att verifiera en elektronisk signatur. Inom det öppna nyckelsystemet är dessa data den s.k. öppna nyckeln.

Enligt 7 punkten avses med certifikat ett intyg i elektronisk form som kopplar ihop signaturverifieringsdata med en undertecknare och bekräftar undertecknarens identitet.

En certifikatutfärdare är enligt 8 punkten en fysisk eller juridisk person som tillhandahåller sådana certifikat som krävs för användning av elektroniska signaturer.

Med en produkt för elektroniska signaturer avses enligt 9 punkten maskinvara eller programvara, eller relevant del i sådant system, som är avsedd att användas av dem som tillhandahåller tjänster vid tillhandahållande av tjänster i anslutning till elektroniska signaturer eller som är avsedd att användas för att skapa eller verifiera elektroniska signaturer.

Med tjänster i anslutning till elektroniska signaturer avses enligt 10 punkten tillhandahållande av certifikat samt andra produkter för elektroniska signaturer och tjänster i anslutning till dem. Som dylika tjänster betraktas sålunda andra tjänster i anslutning till certifikaten, t.ex. tjänster som avser registrering, tidsstämpling, fakturering och rådgivning.

3 §. *Tillämpningsområde*. Lagen skall tillämpas på elektroniska signaturer samt på dem som tillhandahåller allmänheten produkter för elektroniska signaturer och tjänster i anslutning till dem.

Lagen skall uttryckligen tillämpas på tillhandahållandet av produkter för och tjänster i anslutning till elektroniska signaturer. Utgångspunkten skall vara fri rörlighet för produkter för och tjänster i anslutning till elektroniska signaturer på EU:s inre marknad i enlighet med 4 § i lagförslaget. I lagen skall likväl ges de bestämmelser som behövs för genomförande av direktivet om elektroniska signaturer i synnerhet om tillhandahållandet av certifikat för elektroniska signaturer. I lagen regleras särskilt skyldigheterna för certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat samt om myndighetsövervakningen.

Lagen skall inte tillämpas på utfärdandet av certifikat som används uteslutande för andra ändamål än elektroniska signaturer, eftersom denna användning av certifikat är annorlunda till sin karaktär. Användningssyften för certifikat som faller utanför lagens tillämpningsområde är bl.a. användningen av certifikat uteslutande för identifiering eller kryptering.

I fråga om certifikat som används för identifiering har parterna i allmänhet ingått ett

separat affärs- eller avtalsförhållande. Certifikatet utgör härvid ett hjälpmedel för uppfyllandet av avtalet. Ett certifikat för identifiering kan autentisera användaren t.ex. då det gäller sådana avgiftsbelagda tjänster om vilka ett särskilt avtal med den som erbjuder tjänsterna har ingåtts. Också olika slag av anläggningar och system inom nätverk för elektronisk kommunikation känner igen varandra med hjälp av certifieringsteknik.

Certifikat som i tekniskt hänseende är likadana kan användas för olika ändamål. Certifikat som används för verifiering av elektroniska signaturer kan bl.a. användas också enbart för identifiering. Identifiering av personer är ett av användningssyftena då det gäller elektroniska signaturer. Även uppgifter om framställning och verifiering av signaturen, såsom hemliga och öppna nycklar, kan användas också för identifierings- och krypteringsändamål. Såvida det är fråga om ett certifikat som används för verifiering av elektroniska signaturer tillämpas bestämmelserna i lagen på certifikatutfärdare och certifikat.

Lagen skall tillämpas på tillhandahållandet av för allmänheten avsedda produkter för och tjänster i anslutning till elektroniska signaturer. Med allmänheten avses en användargrupp som inte på förhand är begränsad på basis av ett arbets-, tjänste- eller kundförhållande. Lagen tillämpas därmed inte på en sluten användargrupp. Lagen omfattar inte utfärdandet av certifikat för intern användning inom t.ex. en företagskoncern. Lagen skall inte tillämpas för elektroniska signaturer som endast används inom användargrupp som grundar sig på frivilliga civilrättsliga avtal mellan ett bestämt antal deltagare. En användargrupp borde däremot anses vara öppet i de fall de mottaggare som skall förlita på certifikatet saknar varje form av avtal med undertecknaren eller certifikatutfärdaren. Den närmare tolkningen av begreppet ”allmänheten” får överlämnas till rättstillämpningen.

Den föreslagna lagen skall vara en allmän lag som gäller elektroniska signaturer och tillhandahållandet av produkter för och tjänster i anslutning till elektroniska signaturer. I fråga om användningen av elektroniska signaturer inom förvaltningen skall därtill gälla vad som bestäms särskilt. Lagstiftningen om elektronisk kommunikation i myndigheternas verksamhet bereds i justitieministeriet. Avsikten är att lagen om elektronisk kommunikation i förvaltningsärenden upphävs i detta sammanhang. Avsikten är att bestämmelserna om certifikat och certifikatutfärdare i detta lagförslag även skall lämpa sig för myndighetskommunikation inom förvaltningen. Lagen om elektronisk kommunikation i myndigheternas verksamhet skall närmast koncentrera sig på regleringen av själva kommunikationsprocessen.

Det är dessutom möjligt att de elektroniska tjänsterna inom något visst förvaltningsområde måste regleras separat till följd av dessa tjänsters särdrag. Detta kan vara möjligt när det gäller t.ex. elektronisk kommunikation inom social- och hälsovårdstjänsterna samt försvarsförvaltningen.

4 §. *Fri rörlighet för tjänster och produkter*. Paragrafen skall innehålla bestämmelser om fri rörlighet på den inre marknaden för produkter för elektroniska signaturer och tjänster i anslutning till dem. Genom denna paragraf genomförs principerna för den inre marknaden enligt artikel 4 i direktivet.

5 §. *Säkra anordningar för signaturframställning*. I paragrafen skall ingå bestämmelser om de krav som en anordning för signaturframställning skall uppfylla för att den skall kunna betraktas som en säker anordning för signaturframställning. Enligt 18 § i lagförslaget uppfyller en avancerad elektronisk signatur som baserar sig på ett kvalificerat certifikat enligt definitionen i lagens 7 § och har skapats med en säker anordning för signaturframställning formkraven på en elektronisk signatur enligt lag.

En säker anordning för signaturframställning skall tillräckligt tillförlitligt säkerställa att kraven i 1 mom. 1-5 punkten är uppfyllda. 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 skall en säker anordning för signaturframställning tillförlitligt säkerställa att signaturframställningsdata kan förekomma endast en gång och förblir konfidentiella. Den programvara och den utrustning som finns i undertecknarens dator eller någon annan anordning skall 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 skall 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 därmed inte ge tillgång till unika signaturframställningsdata. Detta kan åstadkommas med hjälp av bl.a. programinställningar samt genom hur utrustningen och dess delar är konstruerade. Därutöver skall den krypteringsalgoritm som används i anordningen för signaturframställning vara tillräckligt kraftfull och nyckeln tillräckligt lång för att signaturframställningsdata, såsom den hemliga nyckeln, inte skall kunna härledas ur resultatet av krypteringen, dvs. ur den elektroniska signaturen.

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

Enligt 4 punkten i momentet skall 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 genom lösenord eller biometriska identifieringsmetoder.

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

Ett omfattande standardiseringsarbete pågår i fråga om säkra anordningar för signaturframställning. Ett av målen för direktivet är att koordinera och samla det europeiska standardiseringsarbetet så att Europeiska gemenskapernas kommission kan fastställa och offentliggöra referensnumren för allmänt erkända standarder gällande anordningar för framställning av elektroniska signaturer i Europeiska gemenskapernas officiella tidning, nedan EGT. Kommissionen biträds enligt artikel 9.1 i direktivet av en kommitté för elektroniska signaturer, som enligt artikel 10 i direktivet har till uppgift att klargöra de kriterier som avses i artikel 3.4 (kriterier enligt vilka medlemsstaterna avgör huruvida ett organ bör utses) samt de allmänt erkända standarder som fastställts och offentliggjorts i enlighet med artikel 3.5 (standarder för produkter för elektroniska signaturer).

Enligt 5 § 2 mom. 1 punkten i lagförslaget anses en anordning för signaturframställning alltid uppfylla kraven i 5 § 1 mom. om den överensstämmer med de allmänt erkända standarder som kommissionen har fastställt och som har publicerats i EGT. Enligt punkt 2 i paragrafens 2 mom. 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 skall ha utsetts särskilt för den ifrågavarande prövningsuppgiften samt finnas i Finland eller en annan stat inom EES-området. I artikel 3.4 andra stycket i direktivet förutsätts att ett beslut om anordningens säkerhet som fattats av ett sådant organ skall erkännas av samtliga medlemsstater. I lagförslagets 6 § ingår bestämmelser om kontrollorganet.

Genom 1 mom. i paragrafen genomförs bilaga III till direktivet. Genom bestämmelsen i paragrafens 2 mom. 1 punkt samt genom 11 § 2 mom. genomförs artikel 3.5 i direktivet. Genom bestämmelsen i paragrafens 2 mom. 2 punkt genomförs artikel 3.4 andra stycket i direktivet.

6 §. *Kontrollorgan*. Enligt det föreslagna 1 mom. kan Kommunikationsverket vid behov utse kontrollorgan som skall bedöma om en anordning för signaturframställning uppfyller kraven i 5 § 1 mom. Kontrollorganet kan vara antingen ett privat eller ett offentligt organ.

Den ovan i motiveringen till 5 § nämnda kommittén för elektroniska signaturer enligt artikel 9 i direktivet har kommit överens om de minimikrav som skall uppställas för kontrollorganen och som Europeiska gemenskapernas kommission har fastställt genom sitt beslut av den 6 november 2000 (Kommissionens beslut 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 skall 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. Detta gäller även certifikatutfärdare och deras auktoriserade representanter. Om organet är en del av en organisation som även utför annan än i denna paragraf avsedd kontrollverksamhet, skall organet kunna identifieras som en separat enhet i organisationen och de olika funktionerna inom organisationen skall tydligt kunna skiljas från varandra.

Kontrollorganets verksamhet skall vara ändamålsenlig och organet får t.ex. inte diskriminera någon som önskar använda sig av dess tjänster. Kontrollorganet skall arbeta öppet med överensstämmelsebedömningen av säkra anordningar för signaturframställning och det skall dokumentera all relevant information beträffande detta arbete. Vem som helst skall ha rätt att använda kontrollorganets tjänster.

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

Kommunikationsverket utnämner kontrollorganen på basis av ansökan. Ansökan skall utöver sökandens kontaktuppgifter och handelsregisterutdrag eller motsvarande utredning dessutom omfatta en utredning av huruvida de villkor som avses i 2 mom. uppfylls då det gäller sökandens verksamhet. Kommunikationsverket meddelar även vid behov anvisningar om de uppgifter som skall ingå i ansökan och hur de skall skickas till Kommunikationsverket.

Kommunikationsverket övervakar kontrollorganets verksamhet. Kontrollorganet skall underrätta Kommunikationsverket om sådana ändringar i verksamheten som inverkar på förutsättningarna för utnämning till kontrollorgan. Om kontrollorganet inte längre uppfyller fastställda krav eller om det bryter mot bestämmelserna, skall Kommunikationsverket återkalla utnämningsbeslutet.

Vid bedömningen av anordningar kan kontrollorganet anlita utomstående personer. Med person avses här både en fysisk och en juridisk person. Kontrollorganet svarar också för det arbete som dessa utför. Kontrollorganet skall säkerställa och kunna påvisa att dessa personer är kompetent för uppgifterna i fråga.

Genom denna bestämmelse genomförs artikel 3.4 första stycket i direktivet samt det ovan nämnda beslutet av kommissionen om de minimikriterier som gäller för kontrollorgan (Bryssel, 06/11/2000, K(2000) 3179 slutlig.).

2 kap. Tillhandahållande av kvalificerade certifikat

7 §. *Kvalificerade certifikat.* Med kvalificerat certifikat avses ett certifikat som uppfyller kraven i paragrafens 2 mom. och som har utfärdats av en certifikatutfärdare som uppfyller kraven i 10-15 §. I det finska lagförslaget

används benämningen ”laatuvarmenne” för kvalificerat certifikat, vilket motsvarar ”hyväksytty varmenne” enligt definitionen i artikel 2.10 i den finska versionen av direktivet. På svenska används benämningen ”kvalificerat certifikat” i såväl lagförslaget som direktivet. Paragrafen innehåller minimikraven i fråga om ett kvalificerat certifikat.

Ett kvalificerat certifikat skall enligt 2 mom. 1 punkten innehålla uppgift om att certifikatet är ett kvalificerat certifikat och enligt 2 punkten skall det innehålla uppgift om certifikatutfärdaren och etableringsstat. Etableringsstaten bestäms enligt var det faktiska utövandet av den ekonomiska verksamheten från ett fast verksamhetsställe försiggår. Om certifikatutfärdaren har många etableringsställen betraktas den stat som etableringsstat där centret för certifikatutfärdarens certifieringsverksamhet ligger.

Undertecknarens namn skall enligt 3 punkten ingå i det kvalificerade certifikatets datainnehåll. Om namnet är en pseudonym, skall det klart framgå av certifikatet att det är fråga om en pseudonym.

Signaturverifieringsdata som motsvarar signaturframställningsdata som undertecknaren innehar skall enligt 4 punkten utgöra en del av innehållet i det kvalificerade certifikatets datainnehåll. Inom det öppna nyckelsystemet innebär detta att det kvalificerade certifikatets datainnehåll skall omfatta en öppen nyckel som svarar mot den hemliga nyckeln.

Ett kvalificerat certifikat skall enligt 5 punkten innehålla uppgifter om certifikatets giltighetstid. Dessa uppgifter skall omfatta både tidpunkt för när certifikatet börjar gälla och tidpunkt för när det upphör att gälla.

Ett kvalificerat certifikat skall enligt 6 punkten innehålla dess identifieringskod. En säker certifieringsverksamhet förutsätter att certifikaten kan skiljas från varandra. Identifieringskoden kan vara ett löpande serienummer eller annan teckensträng som fungerar som identifieringskod.

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

Eventuella begränsningar av certifikatets användningsområde eller av värdet på de transaktioner för vilka certifikatet kan användas skall enligt 8 punkten framgå av det kvalificerade certifikatet. Begränsningen kan gälla t.ex. värdet av penningbeloppet i fråga om en rättshandling eller vara av liknande art. Genom en sådan begränsning kan användningen av certifikatet t.ex. begränsas till enbart vissa rättshandlingar.

Enbart namnet identifierar inte nödvändigtvis undertecknaren tillräckligt entydigt. Särskilda uppgifter om undertecknaren skall enligt 9 punkten framgå av det kvalificerade certifikatet om de behövs för ändamålet med det kvalificerade certifikatet. Sådana uppgifter kan vara t.ex. en uppgift om rätten att handla i något företags namn. Särskilda uppgifter kan vara någon av undertecknarens personuppgifter, t.ex. en av certifikatutfärdaren utfärdad identifieringskod. I ett certifikat som utfärdats av t.ex. Befolkningsregistercentralen utgörs dylik information av den kod för elektronisk kommunikation som finns lagrad i befolkningsdatasystemet. Undertecknarens personbeteckning skall dock inte kunna vara en sådan särskild uppgift som avses i denna punkt.

Genom bestämmelsen genomförs definitionen i artikel 2.10 i direktivet och bilaga I till direktivet. Genom 2 mom. 3 punkten genomförs dessutom artikel 8.3 i direktivet.

8 §. *Kvalificerade certifikat som tillhandahålls av en certifikatutfärdare som inte är etablerad i Finland.* I paragrafen skall ingå bestämmelser om de förutsättningar under vilka certifikat tillhandahålls av en certifikatutfärdare som inte är etablerad i Finland anses uppfylla kraven i 7 §. Som kvalificerat certifikat kan endast ett sådant certifikat betraktas vars datainnehåll är relevant. Certifikatet skall uppfylla åtminstone fordringarna i 7 § 2 mom.

Enligt 1 punkten i momentet skall som kvalificerade certifikat erkännas sådana certifikat som tillhandahållits av en certifikatutfärdare etablerad i en annan stat inom EES-området. Ytterligare en förutsättning är att det certifikat som certifikatutfärdaren tillhandahållit uppfyller etableringsstatens krav på ett kvalificerat certifikat.

Enligt 2 punkten i momentet skall som kvalificerade certifikat erkännas sådana certifikat som tillhandahållits av en certifikatut-

färdare 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 direktiv 1999/93/EG om elektroniska signaturer. Det finns många frivilliga ackrediteringssystem och det är inte obligatoriskt att ansluta sig till och tillhöra sådana. Ackrediteringssystem håller på att upprättas i bl.a. Nederländerna (TTP Netherlands) och Storbritannien (TScheme).

Som kvalificerade certifikat skall enligt 3 punkten erkännas sådana certifikat som garanteras av en certifikatutfärdare som är etablerad i en annan stat inom EES-området och uppfyller de nationella krav som i denna stat föreskrivits för genomförande av direktivet om elektroniska signaturer.

Genom bestämmelsen i 4 punkten i momentet anses det certifikat som certifikatutfärdaren tillhandahållit uppfylla kraven på ett kvalificerat certifikat enligt 7 § om certifikatet eller certifikatutfärdaren har erkänts enligt ett bilateralt eller multilateralt avtal mellan Europeiska gemenskapen och tredje länder eller internationella organisationer.

Genom bestämmelsen genomförs artikel 7.1 i direktivet.

9 §. *Anmälan om inledande av verksamhet*. Enligt paragrafens 1 moment skall en certifikatutfärdare som avser att tillhandahålla allmänheten kvalificerade certifikat innan sådana certifikat börjar tillhandahållas göra en anmälan till Kommunikationsverket. Anmälan skall göras skriftligen. Av anmälan skall framgå certifikatutfärdarens namn och adressuppgifter samt de uppgifter som behövs för att säkerställa att kraven i 7 § och 10-15 § uppfylls. Kommunikationsverket kunde meddela nödvändiga föreskrifter eller rekommendationer om hur de uppgifter som skall uppges skall sändas till verket och om närmare innehåll i dem. Genom Kommunikationsverkets föreskrifter och rekommendationer kunde senare preciseras de uppgifter som är behövliga för att de i lag fastställda förutsättningarna skall konstateras och kontrolluppdraget utföras. Genom föreskrifterna och rekommendationerna skall inte uppställas nya skyldigheter för dem som tillhandahåller kvalificerade certifikat. Möjligheten att senare meddela närmare föreskrifter och rekommendationer är nödvändig till följd av att certifieringsverksamheten fortfarande är under utveckling och standardiseringsverksamheten inte är slutförd.

Inledande av verksamhet förutsätter inte något förhandsgodkännande av Kommunikationsverket, men Kommunikationsverket kunde efter att ha fått anmälan utan dröjsmål förbjuda certifikatutfärdaren att tillhandahålla certifikat som anges vara kvalificerade, om certifikaten inte uppfyller kraven i 7 § 2 mom. eller certifikatutfärdaren inte uppfyller kraven i 10-15 §. Förbudet gäller endast rätten att tillhandahålla certifikat som kvalificerade certifikat. Ett kvalificerat certifikats datainnehåll får t.ex. inte innefatta uppgifter om det kvalificerade certifikatet. I övrigt kan certifikatutfärdaren fortsätta verksamheten trots förbudet och tillhandahålla andra än kvalificerade certifikat.

En certifikatutfärdare som tillhandahåller allmänheten sina certifikat som kvalificerade certifikat ansvarar likväl alltid i egenskap av utfärdare av kvalificerade certifikat enligt detta lagförslag för eventuella skador som kan uppstå när ett certifikat som inte uppfyller kraven på kvalificerade certifikat likväl används som ett kvalificerat certifikat. Bestämmelser om skadeståndsansvaret för en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat ingår i 16 § i detta lagförslag. Kommunikationsverket skall med beaktande av anmälarens intressen och det ovan nämnda skadeståndsansvaret för den certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat agera omedelbart i ärendet för att certifikatutfärdaren så snabbt som möjligt skall få besked från Kommunikationsverket till stöd för sin affärsverksamhet. Certifikatutfärdaren skall också omedelbart underrätta Kommunikationsverket om ändringar i uppgifterna i anmälan. Enligt den föreslagna lagen skall Kommunikationsverket på det sätt som framgår av 4 kap. i lagförslaget utöva tillsyn över de certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat. För att kunna utföra sina tillsynsuppgifter behöver Kommunikationsverket få tillräckliga och korrekta uppgifter om de certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat.

Kommunikationsverket för ett offentligt register över certifikatutfärdare som utfärdar kvalificerade certifikat. Registret innehåller bl.a. uppgifter om certifikatutfärdarens namn och adress i samma form som utfärdaren har meddelat uppgifterna till Kommunikationsverket. Ur registret skall det vara möjligt att få uppgifter om de certifikatutfärdare som till Kommunikationsverket har anmält att de tillhandahåller kvalificerade certifikat i Finland. Uppgifterna i registret skall emellertid endast ha en informativ uppgift. Enligt 16 § i lagförslaget ansvarar en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat för eventuella skador som hans verksamhet åsamkat tredje part, oberoende av om certifikatutfärdaren i fråga har införts i Kommunikationsverkets register eller inte.

Genom bestämmelsen genomförs artikel 3.1 och delvis artikel 3.3 i direktivet. Det övervakningssystem som avses i artikel 3.3 i direktivet regleras i 22-28 § i lagen.

10 §. *Allmänna skyldigheter för certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat.* Paragrafen innehåller bestämmelser om de allmänna skyldigheterna för en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat. En certifikatutfärdare skall bedriva verksamheten omsorgsfullt, tillförlitligt och ändamålsenligt. Genom kraven på omsorgsfullhet, tillförlitlighet och ändamålsenlighet eftersträvar man att öka det offentliga förtroendet för säkerheten hos elektronisk kommunikation och därtill anknytande certifieringsverksamhet. Kravet på ändamålsenlighet avser huvudsakligen certifikatutfärdarens verksamhet inom kundbetjäningen. Innehållet i kravet på omsorgsfullhet och tillförlitlighet har behandlats inte bara i motiveringen till denna paragraf utan också i andra paragrafer i detta lagförslag och i motiveringen till dessa paragrafer.

En certifikatutfärdare skall dessutom vara skyldig att se till att de personer som eventuellt anlitas bedriver verksamhet på ett omsorgsfullt och tillförlitligt sätt. Med person avses här både en fysisk och en juridisk person. Den som tillhandahåller kvalificerade certifikat, dvs. den vars namn uppges i certifikatet, är ansvarig för alla verksamhetens delområden även om en del av de tjänster och produkter som han eller hon tillhandahåller köps av underleverantörer. Uppgifter som utförs av personer som certifikatutfärdaren anlitar kan t.ex. vara mottagande av certifikatansökningar, skapande av certifikat samt underhåll av spärrlistor.

Certifikatutfärdaren skall också ha tillräckliga tekniska kunskaper och ekonomiska resurser med tanke på verksamhetens omfattning. Som ett bevis på att verksamheten bedrivs omsorgsfullt och tillförlitligt skall certifikatutfärdaren bl.a. bedöma de tekniska och ekonomiska risker som ansluter sig till verksamheten och vidta nödvändiga åtgärder för att minimera dessa risker. Omsorgsfullhet och tillförlitlighet förutsätts också då det gäller certifikatutfärdarens dokumentation över de förfaranden som används.

Enligt 2 mom. 1 punkten i paragrafen skall en certifikatutfärdare ha personal med tillräcklig sakkunskap, erfarenhet och kompetens. Certifikatutfärdaren skall alltså se till att de anställda, och särskilt de som har ledande uppgifter, har sådan sakkunskap, erfarenhet och kompetens som certifieringsverksamheten kräver. Personalen skall ha tillräcklig sakkunskap bl.a. om framställning av elektroniska signaturer och datasäkerhetsfrågor.

Enligt 2 mom. 2 punkten skall certifikatutfärdaren se till att förfoga över tillräckliga ekonomiska resurser för ordnande av verksamheten och med tanke på eventuellt skadeståndsansvar. Vad som är tillräckligt skall bedömas i relation till certifieringsverksamhetens omfattning. Även om certifikatutfärdaren skulle ha en tillräckligt omfattande ansvarsförsäkring för täckande av skadestånden, skall utfärdaren även ha tillräckliga ekonomiska resurser för att bedriva en tillförlitlig certifieringsverksamhet.

Enligt 2 mom. 3 punkten skall certifikatutfärdaren se till att sådana uppgifter om certifikaten och certifikatverksamheten finns allmänt tillgängliga som behövs för bedömande av certifikatutfärdarens verksamhet och tillförlitlighet. Certifikatutfärdarens kunder samt de instanser som förlitar sig på certifikatutfärdarens tjänster skall ha tillgång till tillräckliga uppgifter om verksamheten för att på basis av dem kunna bedöma om certifikatet är tillräckligt tillförlitligt för deras behov. Kravet i momentets 3 punkt skall kunna uppfyllas genom att certifikatutfärdaren medde-

lar sina certifieringsprinciper och sin certifieringsstandard.

Certifieringsprinciperna framgår av det dokument som certifikatutfärdaren har sammanställt och som användaren skall känna till och godkänna. Dokumentet fastställer reglerna för certifikatutfärdarens verksamhet och utgående från dem kan det bedömas hur certifikatet lämpar sig för olika syften. Dokumentet över certifieringsprinciperna svarar på vad certifikatutfärdaren gör och ställer därmed krav på certifikatutfärdarens verksamhet och ledning. Flera certifikatutfärdare kan ha ett gemensamt dokument över sina certifieringsprinciper. European Telecommunications Standards Institute (ETSI) har fastställt en miniminivå för grundläggande certifieringsprinciper avsedda för certifikatutfärdare som tillhandahåller kvalificerade certifikat.

Certifikatutfärdaren skall också erbjuda dokumentation över den certifieringsstandard (Certificate Practise Statement, nedan CPS) som tillämpas inom den egna organisationen och som är en mera detaljerad beskrivning av hur certifikatutfärdaren tillämpar certifieringsprinciperna inom sin organisation. Med hjälp av certifieringsstandarden kan t.ex. utomstående instanser kontrollera om certifikatutfärdaren följer certifieringsprinciperna.

De uppgifter som avses i momentets 3 punkt skall finnas allmänt tillgängliga. Uppgifterna anses vara allmänt tillgängliga bl.a. då de kan hämtas på certifikatutfärdarens verksamhetsställe eller finns att tillgå på certifikatutfärdarens webbplats via Internet.

Enligt momentets 4 punkt skall certifikatutfärdaren trygga att signaturframställningsdata är konfidentiella då certifikatutfärdaren själv framställer dem. Certifikatutfärdaren skall försäkra sig om att han eller hon överlåter signaturframställningsdata endast till de personer som är berättigade att förfoga över dem.

Enligt 3 mom. får certifikatutfärdaren inte heller lagra eller kopiera signaturframställningsdata som överlåtits till en undertecknare. Att signaturframställningsdata uppbevaras endast för undertecknarens räkning är väsentligt för att tillförlitligheten hos den elektroniska signaturen skall kunna bibehållas. Av denna orsak föreskrivs att certifikatutfärdaren inte får lagra eller kopiera signaturframställningsdata. Om signaturframställningsdata förkommer eller förstörs kan undertecknaren alltid begära att få nya signaturframställningsdata av certifikatutfärdaren. Det ligger i undertecknarens intresse att i sådana situationer alltid göra en sådan anmälan som avses i 13 §.

Genom bestämmelsen genomförs punkterna a, e, g, h och j i bilaga II till direktivet.

11 §. *Tillförlitliga maskinvaror och programvaror*. De system samt den maskinvara och programvara som en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat använder skall vara tillräckligt säkra och tillförlitliga samt skyddade mot ändringar och förfalskningar. Med tillräckligt säker och tillförlitlig avses så stor tillförlitlighet som möjligt som kan uppnås genom användning av de bästa möjliga tekniska lösningarna. Systemen och deras delar skall vara skyddade så att endast personal som utsetts av certifikatutfärdaren kan företa ändringar i dem och så att förändringar, även sådana som eventuellt orsakas av utomstående och fel i maskinvaran, registreras och data om dem bevaras.

I paragrafens 2 moment föreskrivs att maskinvara eller programvara som överensstämmer med de allmänt erkända standarder som har fastställts av Europeiska gemenskapernas kommission och publicerats i EGT alltid skall anses uppfylla kraven i 1 mom.

Genom bestämmelsen genomförs artikel 3.5 och punkt f i bilaga II till direktivet.

12 §. *Utfärdande av kvalificerade certifikat*. En certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat skall omsorgsfullt och på ett tillförlitligt sätt kontrollera den sökandes identitet och andra uppgifter som hänför sig till sökandens person och som är relevanta för utfärdandet och upprätthållandet av det kvalificerade certifikatet. Uppgifter som hänför sig till sökandens person kunde vara åtminstone sökandens namn och adressuppgifter samt de uppgifter enligt 7 § 2 mom. som ingår i datainnehållet i ett kvalificerat certifikat, inbegripet särskilda uppgifter som eventuellt hänför sig till ett visst användningsändamål för certifikatet.

Certifikatutfärdaren som tillhandahåller allmänheten kvalificerade certifikat skall identifiera sökanden personligen. Att identi-

fiera sökanden personligen avser att sökanden, när denne ansöker om det kvalificerade certifikatet, personligen skall besöka certifikatutfärdaren för identifiering.

En certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat har rätt att kräva att sökanden uppger sin personbeteckning för att identiteten skall kunna kontrolleras. Detta är nödvändigt för att det skall kunna säkerställas att sökanden har identifierats på ett tillförlitligt sätt. En bestämmelse om yppande av personbeteckningen ingår i lagförslagets 19 § 2 mom., som berättigar alla certifikatutfärdare att kräva att sökanden uppger sin personbeteckning. I detta fall är det självklart att även en certifikatutfärdare som tillhandahåller kvalificerade certifikat har samma rättighet. Ett förbud som gäller alla certifikatutfärdare är även förbudet enligt 19 § 2 mom. mot att en personbeteckning tas in i certifikatet. Personbeteckningen får således inte heller tas in i ett kvalificerat certifikat.

Kontrollen av sökandens identitet på ett tillförlitligt sätt kan ske med hjälp av en tillförlitlig handling som sökanden företer. Såsom tillförlitliga handlingar kan åtminstone betraktas av polisen utfärdad identitetshandling, pass, identitetskort eller körkort utfärdat efter september 1990.

En certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat bekräftar genom sin avancerade elektroniska signatur, som tas in i det kvalificerade certifikatet, att de uppgifter som ingår i det kvalificerade certifikatet hör till en viss person. Efter att certifikatet överlåtits kontrolleras undertecknarens identitet i allmänhet inte. I och med utfärdandet av certifikatet överlåts också de unika signaturframställningsdata till undertecknaren. Den som verifierar signaturen känner inte nödvändigtvis alls 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 särdeles 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 16 § 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 då certifikatet utfärdas anses enligt detaljmotivering av 16 § vara den tidpunkt då det överlåts till sökanden.

Innan avtal ingås skall certifikatutfärdaren enligt 2 mom. informera sökanden om villkoren för användning av certifikatet, inbegripet eventuella begränsningar av användningen, och om frivilliga ackrediteringssystem, myndighetstillsynen över verksamheten samt förfaranden för klagomål och avgörande av tvister. Uppgifter som skall 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 certifikatet på spärrlistan. Villkoren för användningen skall också omfatta uppgifter om certifikatutfärdarens skadeståndsansvar och andra skyldigheter.

Den som ansöker om ett certifikat skall också informeras om den tillsyn Kommunikationsverket och dataskyddsombudsmannen utövar i fråga om certifikatutfärdaren samt om sökandens rätt att få saken prövad av Kommunikationsverket när det gäller sådan verksamhet som en i denna lag avsedd certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat bedriver.

Uppgifterna skall ges den som ansöker om ett kvalificerat certifikat skriftligen i sådan form att sökanden utan svårighet förstår dem. Information i elektronisk form som är allmänt läsbar och kan lagras anses ha blivit given skriftligen. Vid verksamhet i Finland bör man eftersträva att dessa uppgifter ges den som ansöker om ett kvalificerat certifikat åtminstone på något av de officiella språk som används i Finland.

Genom bestämmelsen genomförs punkterna d och k i bilaga II till direktivet.

13 §. *Återkallande av kvalificerat certifikat.* Med tanke på certifieringsverksamhetens säkerhet 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. skall tas in en uttrycklig skyldighet för undertecknaren att av certifikatutfärdaren begära återkallande av sitt kvalificerade certifikat, om han har grundad anledning att anta att signaturframställningsdata kan användas på obehörigt sätt. Certifikatutfärdaren skall enligt 2 mom. omedelbart återkalla ett kvalificerat certifikat om undertecknaren begär det. Certifikatutfärdaren skall återkalla ett kvalificerat certifikat genom att införa uppgifter därom på en spärrlista enligt 14 § 3 mom. Undertecknaren behöver inte motivera sin begäran.

Den tidpunkt då begäran om återkallande har varit tillgänglig för certifikatutfärdaren i sådan form att den har kunnat behandlas skall betraktas som den tidpunkt då begäran inkommit. 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 3 mom. också återkalla ett certifikat om det finns särskild anledning till det. En särskild anledning kan vara t.ex. undertecknarens bortgång eller annat tvingande skäl. En sådan särskild anledning kunde också vara att certifikatutfärdarens verksamhet upphör. Dessutom kan certifikatutfärdaren återkalla ett certifikat om undertecknaren bryter mot det avtal han eller hon ingått med certifikatutfärdaren eller använder certifikatet i strid mot dess syfte. Enligt 3 mom. skall undertecknaren alltid underrättas om att ett kvalificerat certifikat har återkallats och om tidpunkten för återkallandet. Detta är nödvändigt för att undertecknaren skall kunna försäkra sig om att hans begäran om återkallande har lyckats eller om ett eventuellt återkallande som gjorts på certifikatutfärdarens initiativ.

Bestämmelser om skadeståndsansvaret för certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat och om obehörig användning av signaturframställningsdata ingår i lagförslagets 16 och 17 §.

14 §. *Register som skall föras av certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat.* En certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat har i punkt b i bilaga II till direktivet om elektroniska signaturer ålagts skyldigheten 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 till allmänheten skall 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 certifikat.

Genom bestämmelsen om register som upprätthålls av certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat strävar man efter att garantera att de tjänster som centralt anknyter till användningen av kvalificerade certifikat skall vara tillgängliga på ett så effektivt och tillförlitligt sätt som möjligt. Det är uttryckligen med hjälp av dessa tjänster som certifikatutfärdaren agerar som en tillförlitlig tredje part, som för den som mottar meddelandet med ett kvalificerat certifikat verifierar giltigheten hos de signaturframställningsdata som gäller den som skickat meddelandet och den som undertecknat det. I lagens 14 och 15 § föreskrivs också om de uppgifter som skall lagras och hur de skall förvaras.

En certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat skall enligt 1 mom. föra register över utfärdade certifikat (certifikatregister). I registret skall inte bara införas det datainnehåll i ett kvalificerat certifikat som anges i 7 § 2 mom. utan också de i 12 § 1 mom. avsedda uppgifterna som hänför sig till sökandens person, inbegripet uppgifter om den metod som använts för att identifiera sökanden när det kvalificerade certifikatet utfärdades, samt de i 21 § avsedda uppgifterna om en sådan kontroll av ett certifikats giltighetstid som gjorts på spärrlistan, om en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat utnyttjar rätten att lagra dessa uppgifter enligt 21 §.

En certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat kunde således lagra t.ex. uppgifter om vilken handling som använts vid identifieringen och även lagra de relevanta uppgifterna ur denna handling. En sådan relevant uppgift kunde t.ex. utgöras av passets nummer eller personbeteckningen. En certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat kunde även ta t.ex. fotokopior av de handlingar som använts vid identifieringen. Det väsentliga när det gäller lagringen av uppgifter är det krav på verifiering av en omsorgsfull och tillförlitlig identifiering som ställs på en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat. Eftersom certifikatutfärdaren har ett i 16 § definierat strängt skadeståndsansvar i fråga om huruvida uppgifterna i det kvalificerade certifikat som han utfärdat är korrekta, skall certifikatutfärdaren också ha möjlighet att vid behov bevisa att han har agerat på ett omsorgsfullt sätt. Det vore nödvändigt att lagra uppgifterna om kontrollen av det kvalificerade certifikatet t.ex. med tanke på faktureringen av användningen av certifikaten och utredningen av eventuella tvister. Närmare bestämmelser om användningen av uppgifterna om kontroll ingår i 21 §.

En certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat skall enligt 2 mom. säkerställa att den som förlitar sig på en avancerad elektronisk signatur som är baserad på ett kvalificerat certifikat har tillgång till det kvalificerade certifikatets i 7 § 2 mom. definierade datainnehåll. Avsikten är inte att paragrafen skall omfatta närmare bestämmelser om på vilket sätt uppgifterna skall vara tillgängliga för de parter som förlitar sig på signaturen. Certifikatutfärdaren kunde beroende på vilka tekniska tillämpningar han använder uppfylla kravet på det ändamålsenligaste sättet. Om man i ett avtal mellan undertecknaren och certifikatutfärdaren kommer överens om att undertecknaren själv tillsammans med meddelandet även delar ut ett kvalificerat certifikat, kommer certifikatets innehåll till den parts kännedom som förlitat sig på det utan att certifikatutfärdaren behöver vidta några särskilda åtgärder. I dessa fall behövs inte någon särskild tjänst som certifikatutfärdaren tillhandahåller. Certifikatutfärdaren och undertecknaren kan också komma överens om att certifikatutfärdaren ur certifikatregistret överlåter uppgifterna i datainnehållet enligt 7 § 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.

Enligt 3 mom. skall en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat också se till att återkallade certifikat och den exakta tidpunkten för återkallandet på ett lämpligt sätt och utan dröjsmål införs på spärrlistan. Certifikatutfärdaren skall så snart som möjligt göra en anteckning om återkallelse i spärrlistan. Undertecknarens ansvar för obehörig användning av signaturframställningsdata upphör i regel när han eller hon hos certifikatutfärdaren har begärt att det kvalificerade certifikatet skall återkallas i enlighet med 13 §. Ansvaret för användningen av signaturframställningsdata under den tid som förflyter från det att undertecknaren begär att certifikatet skall återkallas fram till det att certifikatet införs på spärrlistan vilar på certifikatutfärdaren, och därför torde det ligga i certifikatutfärdarens eget intresse att snabbt införa uppgifterna på spärrlistan. Närmare bestämmelser om obehörig användning av signaturframställningsdata ingår i 17 §.

Spärrlistan bör genomföras som ett offentligt register, eftersom spärrlistan är det enda som den part som förlitat sig på undertecknaren kan gå till för att konstatera att ett certifikat eventuellt har återkallats. Spärrlistan kan genomföras t.ex. så att i den endast införs det kvalificerade certifikatets identifieringskod. I detta 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 införs på spärrlistan skall undertecknarens uttryckliga samtycke fås för införandet av uppgifterna. 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 kva-

lificerade certifikatet i fråga har återkallats.

Uppgifterna enligt 7 § 2 mom. i det kvalificerade certifikatet samt spärrlistan skall enligt 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 7 § 2 mom., skall tjänsten vara tillgänglig dygnet runt. Om undertecknaren själv ger ut det kvalificerade certifikatet finns det inget behov av en särskild tjänst som genomförs av certifikatutfärdaren, utan i detta fall kunde man anse att innehållet i det kvalificerade certifikatet enligt 7 § 2 mom. är tillgängligt dygnet runt när det delas ut av undertecknaren. Den spärrlista som upprätthålls av en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat skall dock alltid vara tillgänglig dygnet runt.

Genom bestämmelsen genomförs punkterna b och c i bilaga II till direktivet.

15 §. *Förvaring av uppgifter i certifikatregistret*. Certifikatutfärdaren är skyldig att på ett tillförlitligt och ändamålsenligt sätt förvara de uppgifter som enligt 14 § skall införas i certifikatregistret i 10 år från det att det kvalificerade certifikatet upphörde att gälla. Uppgifterna kan också förvaras i elektronisk form.

Då tillhandahållandet och användningen av certifikat fortfarande är så outvecklade, kan man inte exakt fastställa de situationer där certifikaten kommer att användas i framtiden. Således är det också omöjligt att exakt uppskatta eventuella problem som kan uppstå i anslutning till bevisningsfrågorna och tillgången till bevisning, t.ex. när det gäller skada till följd av missbruk. Med anledning av detta är det motiverat att föreskriva att certifikatregistrets uppgifter skall förvaras under en lång tidsperiod på tio år.

Vid förvaringen skall tillförlitliga system för lagring av data användas. Uppgifterna lagras och ändras endast av pålitliga personer som certifikatutfärdaren har bemyndigat. Dessutom skall de tekniska förändringar som kan äventyra säkerheten hos de uppgifter som lagras noteras av den instans som förvarar uppgifterna. Behandlingen av personuppgifter skall ske i enlighet med bestämmelserna i personuppgiftslagen. I 19 § ingår en informativ hänvisning till tillämpningen av personuppgiftslagen på alla certifikatutfärdares verksamhet.

Genom bestämmelsen genomförs punkterna i och l i bilaga II till direktivet.

16 §. *Skadeståndsansvar för certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat.* Användningen av elektroniska signaturer grundar sig till stor del på att användaren har förtroende för certifikatutfärdarens verksamhet. I fråga om eventuella problem som uppstår i samband med användningen av elektroniska signaturer och orsaken till dessa problem kan andra än certifikatutfärdaren i praktiken ha svårt att bevisa. Det kan vara svårt eller nästan omöjligt för den som lidit skada att bevisa vårdslöshet eller försummelse i certifikatutfärdarens verksamhet. Därför förutsätter direktivet om elektroniska signaturer att ansvaret för en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat regleras 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 hans verksamhet och att ordna sin verksamhet därefter.

Bestämmelserna i paragrafen 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. En bestämmelse om fördelningen av risken i fråga om obehörig användning av signaturframställningsdata mellan certifikatutfärdaren och undertecknaren ingår separat i 17 §.

I paragrafens 1 mom. ingår en bestämmelse om de omständigheter som berörs av det skadeståndsansvar som är strängare än det normala ansvaret för vårdslöshet för en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat. Certifikatutfärdaren är skyldig att ersätta skador som beror på de i 1-5 punkten uppräknade omständigheterna, om inte certifikatutfärdaren kan påvisa

att skadan inte har orsakats av vårdslöshet hos utfärdaren själv eller någon som denna 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 paragrafens 1 mom. 1 och 2 punkt är en certifikatutfärdare som tillhandahåller allmänheten 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 om det kvalificerade certifikatet inte innehåller de uppgifter som nämns i 7 § 2 mom. Med tidpunkt 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 uppstått i de uppgifter som uppgivits vid tidpunkten för utfärdandet, för att utfärdaren skulle kunna utfärda ett nytt kvalificerat certifikat som motsvarar de förändrade uppgifterna.

Enligt paragrafens 1 mom. 3 punkt svarar en utfärdare av ett kvalificerat certifikat för den skada som uppkommer om den person som anges i det kvalificerade certifikatet inte 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 finns i det kvalificerade certifikatet. I problemsituationer skall en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat för undvikande av skadeståndsansvar kunna visa att han enligt 12 § 1 mom. omsorgsfullt och på ett tillförlitligt sätt kontrollerat sökandens identitet och överlåtit signaturframställningsdata till den person som är berättigad att besitta dem. Om den som ansöker om ett kvalificerat certifikat eller någon annan än certifikatutfärdaren skapar signaturframställningsdata för vilka signaturverifieringsdata antecknas i det kvalificerade certifikatet, skall certifikatutfärdaren före överlåtelsen av det kvalificerade certifikatet försäkra sig om att sökanden förfogar över signaturframställningsdata.

Enligt 1 mom. 4 punkten svarar certifikatutfärdaren för en skada som orsakats av att signaturframställningsdata och signaturverifieringsdata inte kan användas som komplement till varandra. Kravet på att signaturframställningsdata och signaturverifieringsdata skall komplettera varandra är en nödvändig förutsättning för användningen av elektroniska signaturer. I punkten föreskrivs endast om sådana fall i vilka en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat eller en person som han eller hon anlitar har framställt både signaturframställningsdata och signaturverifieringsdata. Om den som anhåller om ett kvalificerat certifikat själv har skapat eller på annat sätt skaffat signaturframställningsdata och signaturverifieringsdata och enbart skaffar övriga tjänster hos certifikatutfärdaren, är certifikatutfärdaren inte ansvarig för att data kompletterar varandra.

Enligt 1 mom. 5 punkten svarar certifikatutfärdaren för skada som åsamkas den som med grundad anledning förlitat sig på ett kvalificerat certifikat, om certifikatet inte har återkallats på det sätt som anges i 13 §. Den tredje parten, dvs. den som verifierar den elektroniska signaturen, skall kunna lita på att certifikatet är giltigt och att det är i den persons besittning som är berättigad därtill, om inte certifikatet har återkallats och införts på spärrlistan, som certifikatutfärdaren upprätthåller över återkallade kvalificerade certifikat. Om signaturframställningsdata förkommer eller förstörs förhindrar ett omedelbart återkallande av det kvalificerade certifikatet effektivt att skador uppkommer. Det skadeståndsansvar som regleras i punkten gäller tiden efter det att undertecknarens begäran om återkallande av certifikatet har inkommit. Innan begäran om återkallande har inkommit till certifikatutfärdaren ansvarar undertecknaren med de begränsningar som följer av 17 § för de skador som uppkommit.

Så som redan tidigare har konstaterats är spärrlistans tillförlitlighet en viktig faktor i användningen av elektroniska signaturer och certifikat. Av denna anledning kan man anse

att det ligger i sådan omsorgsfull parts intresse som förlitar sig på ett kvalificerat certifikat att försäkra sig om att spärrlistan kontrolleras. Då en certifikatutfärdare, som tillhandahåller allmänheten kvalificerade certifikat, inför den som förlitar sig på certifikatet enbart ansvarar för återkallandet, dvs. att uppgifter om det kvalificerade certifikatet införs på en spärrlista, är utgångspunkten att den som förlitar sig på det kvalificerade certifikatet skall vara omsorgsfull och kontrollera spärrlistan. Kontrollen av spärrlistan kan dock göras automatiskt mellan de system som används av certifikatutfärdaren och den som förlitar sig på kvalificerade certifikatet, vilket innebär att den som förlitar sig på certifikatet inte personligen kontrollerar spärrlistan. Den som förlitar sig på kvalificerade certifikatet skall även i detta fall hos upprätthållaren av det system som han eller hon använder försäkra sig om att kontrollen av spärrlistan alltid sker automatiskt. Beroende på de tekniska tillämpningar som används kan sålunda olika förfaranden användas för att kontrollera spärrlistan, men utgångspunkten är att den som förlitar sig på det kvalificerade certifikatet skall se till att spärrlistan kontrolleras för att han eller hon skall kunna försäkra sig om det kvalificerade certifikatets giltighetstid.

Enligt 2 mom. är en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat befriad från ansvaret enligt 1 mom., om utfärdaren kan visa att skadan inte har orsakats av vårdslöshet hos utfärdaren själv eller någon som han eller hon har anlitat. Detta s.k. presumtiva vållandeansvar innebär ett undantag från den skadeståndsrättsliga huvudbestämmelse som säger att 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 framlägga bevis för ett orsakssamband mellan certifikatutfärdarens verksamhet och den skada han eller hon lidit.

Enligt paragrafens 3 mom. ansvarar en certifikatutfärdare som tillhandahåller allmänheten 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 rättshandlingar som understiger ett visst penningbelopp. En arbetsgivare kan t.ex. begränsa användningen av ett kvalificerat certifikat som utfärdats till en arbetstagare så att det gäller enbart arbetsuppgifter.

Med tanke på certifikatutfärdarens riskhantering är det viktigt att han eller hon inte blir ansvarig för sådan användning som står i strid med de begränsningar av användningen som ingår i certifikatet. För att begränsningarna av användningen skall vara effektiva i förhållande till tredje parter förutsätts att begränsningen kommer till de tredje parternas kännedom. Begränsningarna av användningen skall enligt lagens 7 § 2 mom. 8 punkt synas i det kvalificerade certifikatet så att de alltid förmedlar information även till den som verifierar signaturen.

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

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

Till övriga delar fastställs skadeståndsansvaret för certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat i förhållande till en sådan instans som förlitat sig på det kvalificerade certifikatet och till vilken certifikatutfärdaren inte står i avtalsförhållande i sin helhet i enlighet med skadeståndslagen och de allmänna skadeståndsrättsliga principerna. Skadeståndsansvaret för andra än för dem som tillhandahåller kvalificerade certifikat fastställs i sin helhet i enlighet med skadeståndslagen och de allmänna skadeståndsrättsliga principerna, eftersom

den föreslagna ansvarsregleringen inte skall tillämpas på dem.

I paragrafens 4 mom. skall också ingå en bestämmelse om att den i 16 § föreslagna skadeståndsregleringen skall gälla den certifikatutfärdare som för allmänheten garanterar att ett certifikat är ett kvalificerat certifikat. Direktivet om elektroniska signaturer förutsätter att medlemsstaterna åtminstone försäkrar sig om att det skadeståndsansvar som nämns i 16 § 1 mom. 1-4 punkten även utsträcks att gälla certifikatutfärdare som för allmänheten garanterar att ett certifikat är ett kvalificerat certifikat. I lagförslaget föreslås utöver ansvarsgrunderna enligt 16 § 1 mom. 1-4 punkten dessutom att ansvarsgrunden enligt 5 punkten (underlåtenhet att återkalla 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 att ansvaret för den som för allmänheten garanterar certifikatet i sin helhet blir enhetligt med ansvaret för certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat.

Genom den föreslagna 16 § genomförs artikel 6 i direktivet, som gäller skadeståndsansvaret för certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat eller för certifikatutfärdare som för allmänheten garanterar att ett certifikat är ett kvalificerat certifikat. 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 16 § ingår bestämmelser om skadeståndsansvaret för certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat vad beträffar skada som åsamkats den som förlitat sig på det kvalificerade certifikatet. Eftersom det i artikel 6 i direktivet endast uppställs minimikrav på medlemsstaterna, är det möjligt med nationell reglering i 16 §. Med anledning av minimiregleringen i direktivet är det även möjligt att nationellt bestämma om tillämpningen av ansvarsgrunden enligt 1 mom. 5 punkten på certifikatutfärdare som garanterar att ett certifikat är ett kvalificerat certifikat, fastän direktivet nödvändigtvis inte förutsätter detta.

17 §. *Ansvar för obehörig användning av signaturframställningsdata*. I paragrafen skall regleras undertecknarens ansvar för skada som orsakats av obehörig användning av signaturframställningsdata.

Såsom obehörig användning av signaturframställningsdata anses 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 ta in ansvarsbestämmelser som i fråga om principer har 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. PIN-kod). I framtiden kan signaturframställningsdata skyddas med t.ex. fingeravtrycksidentifikation. I detta fall kommer användningen av signaturframställningsdata i jämförelse med användningen av kreditkort att vara tryggare och obehörig användning betydligt svårare.

Enligt huvudbestämmelsen i paragrafens 1 mom. ansvarar undertecknaren för skada som orsakats av obehörig användning av signaturframställningsdata tills en begäran om återkallande av certifikatet har inkommit till certifikatutfärdaren i enlighet med 13 § 2 mom. Det har inte någon betydelse på vilket sätt signaturframställningsdata har hamnat hos en som inte har rätt att använda dem.

Eftersom tillämpning av den stränga huvudregeln i 1 mom. på konsumenterna skulle vara oskälig ingår i 2 mom. en bestämmelse om de begränsningar som tillämpas på konsumenterna.

Enligt paragrafens 2 mom. 1 punkt kan konsumenten bli tvungen att ansvara för sådana rättshandlingar som någon annan person har utfört obehörigt 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 detta sker.

Enligt paragrafens 2 mom. 2 punkt kan konsumenten bli ansvarig i ett sådant fall dådet beror på vårdslöshet från konsumentens sida, som inte är lindrig, att signaturframställningsdata åtkommits av någon som är obehörig at använda dem. Utgångspunkten är den att undertecknaren omsorgsfullt förvarar signaturframställningsdata och det lösenord eller den identifieringskod som anknyter till användningen av signaturframställningsdata. När man bedömer vårdslösheten bör man fästa uppmärksamhet vid sättet att förvara signaturframställningsdata och lösenordet eller identifieringskoden samt på vilket sätt besittningen av dem har förlorats. Vid bedömningen av vårdslösheten bör man även beakta användningsändamålet med den elektroniska signaturen samt eventuella begränsningar av användningen som framgår av det kvalificerade certifikatet.

Eftersom man med en avancerad elektronisk signatur som baserar sig på ett kvalificerat certifikat och som skapats med en säker anordning för signaturframställning i framtiden kunde utföra vilken rättshandling som helst, kan även ett eventuellt missbruk ha omfattande följder. Å andra sidan kan de begränsningar av användningen som antecknats i det kvalificerade certifikatet ha betydelse när konsumentens vårdslöshet bedöms. Ju färre begräsningar som har antecknats i det kvalificerade certifikatet desto noggrannare kunde man vänta sig att konsumentens signaturframställningsdata förvaras. När vårdslösheten bedöms bör man även beakta att användningen av signaturen hänför sig till många dagliga åtgärder, och därför borde det vara möjligt för undertecknaren att bära signaturframställningsdata med sig. Det bör vara möjligt att t.ex. i plånboken kunna bära ett aktivkort, på vilket signaturframställningsdata finns. När det gäller signaturframställningsdata som i framtiden eventuellt lagras på mobiltelefonernas SIM-kort bör undertecknaren naturligtvis kunna bära mobiltelefonen med sig.

Dessutom bör man vid bedömningen av undertecknarens vårdslöshet i synnerhet beakta hans eller hennes agerande när det gäller att förvara det lösenord eller den identifieringskod som anknyter till skyddet av användningen av signaturframställningsdata omsorgsfullt och på ett sådant sätt att lösenordet och identifieringskoden inte förvaras i samband med signaturframställningsdata. När det gäller att förhindra obehörig användning av signaturframställningsdata kommer det att vara ytterst viktigt att undertecknaren agerar omsorgsfullt vid förvaringen av lösenordet och identifieringskoden.

I paragrafens 2 mom. 3 punkt ingår bestämmelser om situationer där undertecknaren har förlorat kontrollen över signaturframställningsdata på ett sådant sätt att undertecknaren inte alls kan anses ha gjort sig skyldig till vårdslöshet eller att hans eller hennes vårdslöshet har varit lindrig. Enligt momentets 3 punkt kunde undertecknaren bli tvungen att ansvara 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 skall återkallas så som bestäms i 13 § 1 mom. Genom bestämmelsen i den föreslagna 3 punkten strävar man efter att skydda konsumenten, som kunde 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. Undertecknaren ansvarar i fall som avses i 3 punkten för skador som orsakats av obehörig användning av signaturframställningsdata från den tidpunkt då undertecknaren kan anses ha försummat den begäran om återkallande av ett kvalificerat certifikat som avses i 13 § 1 mom. Utgångspunkten är att undertecknaren begär återkallande av det kvalificerade certifikatet omedelbart när han eller hon upptäcker att signaturframställningsdata har försvunnit.

I paragrafens 3 mom. ingår en bestämmelse om att ett avtalsvillkor som till konsumentens nackdel avviker från bestämmelserna i 2 mom. är utan verkan. Ett avtalsvillkor som

förbättrar konsumentens ställning är naturligtvis möjligt. Certifikatutfärdaren kunde alltså i avtalet förbinda sig vid ett mera omfattande ansvar än vad som föreskrivs.

Någon bestämmelse som motsvarar den föreslagna paragrafen ingår inte i direktivet om elektroniska signaturer. Genom bestämmelserna i paragrafen är det nödvändigt att på nationell nivå precisera riskfördelningen i fråga om obehörig användning av signaturframställningsdata.

3 kap. Elektroniska signaturers rättsverkan och behandlingen av personuppgifter

18 §. *Elektroniska signaturers rättsverkan.* I paragrafen skall ingå en bestämmelse om elektroniska signaturers rättsverkan. Om det beträffande en rättshandling i lag ställs krav på underskrift, uppfylls detta krav åtminstone en sådan avancerad elektronisk signatur som baserar sig på ett kvalificerat certifikat och som har skapats med en säker anordning för signaturframställning kravet.

Det har i allmänhet inte uppställts några särskilda formkrav på rättshandlingar. I lag eller andra normer kan man likväl separat bestämma om olika formkrav. När det gäller privaträttsliga avtal är de vanligaste i lagstiftningen förekommande formkraven närmast kraven på att avtal skall ingås skriftligen och att de skall undertecknas. Uttrycken "skriftligen" och "underteckna" har inte definierats närmare i lagstiftningen.

Genom denna bestämmelse vill man försäkra sig om att åtminstone en avancerad elektronisk signatur som baserar sig på ett kvalificerat certifikat och som har skapats med en säker anordning för signaturframställning jämställs med en traditionell, handskriven namnteckning. Bestämmelsen inverkar inte på övriga elektroniska signaturers giltighet. Vilken elektronisk signatur som helst kan naturligtvis bestridas på samma sätt som en traditionell handskriven namnteckning.

Användningen av elektroniska signaturer förutsätter naturligtvis att det är tillåtet och möjligt att utföra en rättshandling elektroniskt. Det att vissa elektroniska signaturers och traditionella namnteckningars rättsverkan fullständigt jämställs med varandra enligt detta lagförslag har inte någon betydelse för när en rättshandling skall göras på papper.

Genom paragrafen genomförs artikel 5 i direktivet. I artikel 5.2 i direktivet bestäms att en elektronisk signatur inte kan förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att signaturen

1) är i elektronisk form,
2) inte är baserad på ett kvalificerat certifikat,
3) inte är skapad av en säker anordning för skapande av signaturer.

Det är klart att en elektronisk signatur inte kan förvägras dess rättsverkan vid en finsk domstol, eller att den inte skulle godkännas som bevis enbart på grundval av de omständigheter som nämns i artikel 5.2 i direktivet. Till följd av den fria bevisprövning som tillämpas vid finska domstolar uppnås målsättningen i bestämmelsen i direktivet utan nationell reglering i Finland.

19 §. *Behandling av personuppgifter*. Genomförandet av artikel 8.2 i direktivet förutsätter en specialbestämmelse om de personuppgifter som inhämtas vid tillhandahållandet av certifikat. Enligt paragrafens 1 mom. får en certifikatutfärdare inhämta de personuppgifter som är nödvändiga för att utfärda och upprätthålla ett certifikat endast från undertecknaren själv. De uppgifter som samlas in måste vara nödvändiga för utfärdandet och upprätthållandet av certifikatet. Inhämtandet av personuppgifter är därmed begränsat utgående från uppgifternas användningsändamål. Det inhämtande av personuppgifter som nämns i momentet ansluter sig till bl.a. identifieringen av en person vid utfärdande av ett certifikat och ett säkert återkallande av ett certifikat, och till dessa kan även ansluta sig olika förfaranden för kontroll av undertecknarens personuppgifter. Vad beträffar en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat hänvisas det dessutom till bestämmelserna i 2 kap. om utfärdande av kvalificerade certifikat, register som skall upprätthållas och förvaring av uppgifter.

Användningen av personbeteckning i samband med utfärdandet av ett certifikat tas upp

i paragrafens 2 mom. Certifikatutfärdaren får kräva att den som ansöker om ett certifikat uppger sin personbeteckning för att styrka sin identitet. Personbeteckningen får dock inte tas in i själva certifikatet.

Enligt 3 mom. krävs undertecknarens uttryckliga samtycke för inhämtande av uppgifter från någon annan källa än undertecknaren själv samt för behandling av uppgifterna för andra ändamål än det som anges i 1 mom. Undertecknarens uttryckliga samtycke skall i allmänhet ges skriftligen och därav skall framgå hurudan behandling av personuppgifterna tillståndet har utfärdats för.

Bestämmelsen skall även tillämpas på sådana certifikatutfärdare som tillhandahåller andra certifikat i anslutning till elektroniska signaturer till allmänheten än de kvalificerade certifikat som avses i denna lag. Eftersom certifikatmarknaden fortfarande är under utveckling och användningsområdet för certifikaten inte har definierats närmare är det inte nödvändigt att närmare reglera innehållet i och behandlingen av de personuppgifter som används vid utfärdandet och upprätthållandet av certifikat, när det gäller andra certifikatutfärdare än dem som tillhandahåller kvalificerade certifikat.

I fråga om behandlingen av personuppgifter gäller dessutom vad som bestäms i personuppgiftslagen (523/1999), som är en allmän lag om behandlingen av personuppgifter. Lagen tillämpas också på certifikatutfärdarens verksamhet. I den föreslagna paragrafens 4 mom. finns för tydlighetens skull en uttrycklig hänvisning till personuppgiftslagen.

Genom lagens 19 och 20 § genomförs artikel 8.1 och 8.2 i direktivet.

20 §. *Användning av befolkningsdatasystemet*. Enligt den föreslagna bestämmelsen har certifikatutfärdaren rätt att skaffa och kontrollera personuppgifter om den som ansöker om ett certifikat med hjälp av befolkningsdatasystemet. Uppgifterna skall dock endast kunna skaffas med sökandens uttryckliga samtycke.

För tydlighetens skull föreslås att det i 2 mom. föreskrivs att de uppgifter som certifikatutfärdaren behöver ur befolkningsdatasystemet för identifiering av en person skall lämnas ut som en offentligrättslig prestation enligt lagen om grunderna för avgifter till staten. I praktiken innebär detta att de utlämnas till självkostnadspris. Eftersom Befolkningsregistercentralen, som upprätthåller befolkningsdatasystemet, själv är verksam som kommersiell certifikatutfärdare är syftet med bestämmelsen att garantera en rättvis konkurrenssituation för certifikatutfärdarna.

Bestämmelsen skall även tillämpas på sådana certifikatutfärdare som tillhandahåller allmänheten andra certifikat i anslutning till elektroniska signaturer än de kvalificerade certifikat som avses i denna lag.

21 §. *Kontroll av certifikats giltighetstid*. Certifikatutfärdaren skall ha rätt att lagra uppgifter om kontroll av certifikatets giltighet. Uppgifterna skall kunna användas endast för fakturering av användningen av certifikat eller för verifiering av rättshandlingar som utförts med hjälp av en elektronisk signatur som baserar sig på ett certifikat.

Lagring av uppgifterna om kontroll är nödvändig speciellt med anledning av eventuella skadeståndskrav som riktas till certifikatutfärdarna. En certifikatutfärdare skall kunna lagra uppgifterna om kontroll av certifikatets giltighet för att han eller hon i synnerhet vid tvister om rättshandlingar skall kunna visa huruvida spärrlistan har kontrollerats och om det vid denna tidpunkt har funnits uppgifter på spärrlistan om återkallande av ett certifikat. Uppgiften om kontroll kunde överlåtas åtminstone till undertecknaren och den som kontrollerat spärrlistan. De som vid eventuella tvister drar nytta av att uppgifterna lagras 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 nödvändigt att den som tillhandahåller certifikat har uppgifter om att faktureringen har skötts ändamålsenligt.

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

Någon bestämmelse som motsvarar den föreslagna paragrafen ingår inte i direktivet om elektroniska signaturer. Genom bestämmelserna i paragrafen är det nödvändigt att på nationell nivå precisera behandlingen av uppgifterna om kontroll av ett certifikats giltighet.

4 kap. **Allmän styrning och tillsyn**

22 §. *Allmän styrning och tillsyn*. Den allmänna styrningen samt utvecklandet av tillhandahållandet av certifikat ankommer på kommunikationsministeriet. Detta innebär i första hand beredning av sådana nödvändiga författningar som eventuellt blir aktuella i och med att certifikatmarknaden utvecklas samt deltagande i sådan verksamhet vid Europeiska gemenskapernas organ som ansluter sig till certifieringsverksamhet.

Kommunikationsverkets uppgift är enligt 2 mom. att övervaka att den föreslagna lagen iakttas. Kommunikationsverket meddelar vid behov tekniska föreskrifter och rekommendationer om kraven på tillförlitlighet och datasäkerhet när det gäller certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat. Till föreskrifterna och rekommendationerna hänförs endast ringa användning av prövningsrätten och genom dem preciseras vid behov innehållet i kraven enligt 7 § och 10-15 § på kvalificerade certifikat och utfärdare av kvalificerade certifikat. Kommunikationsverkets föreskrifter och rekommendationer innehåller endast tekniska och mindre viktiga detaljer. Möjligheten att meddela närmare föreskrifter och rekommendationer är nödvändig till följd av att den nuvarande certifieringsverksamheten är outvecklad och standardiseringsverksamheten inte är slutförd.

Enligt paragrafens 3 mom. övervakar dataombudsmannen att bestämmelserna om behandling av personuppgifter i den föreslagna lagen iakttas. När dataombudsmannen fullgör sina uppgifter har han rätt att få information och utöva tillsyn i enlighet med personuppgiftslagen. Också bestämmelser om sökande av ändring när det gäller dataombudsmannens verksamhet finns i personuppgiftslagen. Enligt 39 § 1 mom. 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. Enligt 39 § 2 mom. personuppgiftslagen har dataombudsmannen rätt att inspektera personregister. Dataombudsmannen och de sakkunniga har för inspektionen rätt att få tillträde till lokaliteter som den registeransvarige och den som handlar på hans uppdrag har i sin besittning och i vilka personuppgifter behandlas eller personregister förs. De skall även få tillgång till sådana upplysningar och anordningar som behövs för inspektionen. I lokaler som omfattas av hemfriden får inspektionen utföras endast om det i det föreliggande fallet finns specificerade skäl att misstänka att brott skett eller kommer att ske mot bestämmelserna om behandling av personuppgifter. En inspektion skall utföras så att den inte i onödan vållar den registeransvarige olägenhet eller kostnader.

Genom 22-28 § genomförs artikel 3.3 i direktivet.

23 §. *Rätt till upplysningar*. Utan hinder av sekretessbestämmelserna har Kommunikationsverket rätt att få upplysningar av certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat och av dem som dessa certifikatutfärdare anlitar. Dem som certifikatutfärdare anlitar kan vara både fysiska och juridiska personer. Rätten att få upplysningar gäller de upplysningar som krävs för fullgörande av tillsynsuppgifterna enligt 22 §.

24 §. *Inspektionsrätt*. En inspektör som Kommunikationsverket har förordnat för uppgiften har rätt att utföra inspektioner om det är nödvändigt för tillsynen över att denna lag och föreskrifter som meddelas med stöd av lagen följs. Med föreskrifter avses föreskrifter som Kommunikationsverket meddelar med stöd av denna lag. Den inspektör som utför inspektionen har rätt att hos en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat som hänför sig till elektroniska signaturer eller hos dem som denna anlitar undersöka sådan maskin- och programvara som kan vara av betydelse vid tillsynen över att denna lag och föreskrifter som meddelas med stöd av lagen följs.

En certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat som hänför sig till elektroniska signaturer och de personer som denna anlitat skall för inspektionen ge Kommunikationsverkets inspektör tillträde till produktions- och affärslokaler samt lagerutrymmen. Denna skyldighet gäller inte lokaler som omfattas av hemfriden.

Kommunikationsverket kan få handräckning av polisen för utförande av inspektionen. Med personer som certifikatutfärdare anlitar avses i denna paragraf både fysiska och juridiska personer.

25 §. *Tystnadsplikt*. Riksdagen har i sitt svar på regeringens proposition med förslag till lag om offentlighet i myndigheternas verksamhet samt till lagar som har samband med den (RSv 303/1998 rd, RP 30/1998 rd) bl.a. förutsatt att man i framtiden förhåller sig återhållsamt till att ta in bestämmelser om hemlighållande av myndigheternas uppgifter i speciallagstiftningen. Eftersom de bestämmelser om tystnadsplikt som införs i speciallagar innebär undantag från denna målsättning, skall i lagen inte tas in en egen bestämmelse om tystnadsplikt, utan till denna del hänvisar man till lagen om offentlighet i myndigheternas verksamhet. Enligt 23 § i lagen får inte den som är anställd hos en myndighet eller innehar ett förtroendeuppdrag röja en uppgift som är sekretessbelagd eller någon annan uppgift för vilken tystnadsplikt föreskrivs genom lag. Tystnadsplikten gäller även efter det att det uppdrag som utförts har avslutats. Dessa uppgifter får inte användas för att skaffa sig själv eller någon annan fördel eller för att skada någon annan.

5 kap. **Särskilda bestämmelser**

26 §. *Straffbestämmelse*. Med tanke på certifieringsverksamhetens trovärdighet är det väsentligt på vilket sätt certifikatutfärdaren behandlar personuppgifter vid tillhandahållandet av tjänster. Av certifikatutfärdarna förutsätts en tillförlitlig behandling av personuppgifter. I lagförslagets 12 § skall ingå bestämmelser om verifiering av relevanta personuppgifter när kvalificerade certifikat utfärdas. I lagförslagets 14 § skall ingå en bestämmelse om skyldigheterna för certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat att upprätthålla certifikatregister och spärrlista samt förvara lagrade uppgifter enligt 15 §. En bestämmelse om behandlingen av personuppgifter som gäller alla certifikatutfärdare skall ingå i 19 §. Det står klart att ett straffrättsligt ansvar ansluter sig till certifikatutfärdarens verksamhet.

I den föreslagna 26 § hänvisas till vad som föreskrivs om personregisterbrott och personregisterförseelser. Eftersom certifikatregistret är ett personregister, är bestämmelsen enbart en informativ hänvisning.

27 §. *Förvaltningstvångsmedel*. Enligt paragrafens 1 mom. kan Kommunikationsverket i egenskap av tillsynsmyndighet 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 beslutet med vite, hot om avbrytande av verksamheten eller hot om tvångsutförande. Rättelseåläggandet och beslutet om vite eller hot kan meddelas samtidigt eller separat.

Kommunikationsverkets tillsynsbehörighet omfattar tillhandahållande av kvalificerade certifikat samt den verksamhet som bedrivs av det kontrollorgan som eventuellt senare utses. Ett hot om avbrytande av verksamheten kan gälla en del av eller hela den verksamhet som omfattas av lagen. Hot som förstärker åläggandena skall alltid stå i proportion till det fel eller den försummelse den försumlige har gjort sig skyldig till. Vite eller tvångsutförande skall alltid vara den åtgärd som först förenas med åläggandet. Hot om avbrytande av verksamheten skall i regel endast utnyttjas i sådana situationer där den försumlige inte har rättat felet eller försummelsen trots vitesföreläggande eller hot om tvångsutförande.

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

28 §. *Ändringssökande*. I beslut som Kommunikationsverket har fattat med stöd av lagen får ändring sökas enligt förvaltningsprocesslagen (586/1996). Enligt 8 § 2 mom. förvaltningsprocesslagen kan besvär anföras hos förvaltningsdomstolen.

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

29 §. *Ikraftträdande*. Lagförslagets 29 § innehåller en ordinär ikraftträdandebestämmelse.

30 §. *Övergångsbestämmelse*. Det är nödvändigt att ta in en övergångsbestämmelse i den föreslagna lagen. Enligt bestämmelsen skall en certifikatutfärdare som har börjat tillhandahålla allmänheten kvalificerade certifikat innan denna lag har trätt i kraft inom tre månader från ikraftträdandet göra en anmälan enligt 9 §.

1.2. Lag om kommunikationsförvaltningen

2 §. I lagen om kommunikationsförvaltningen (625/2001) föreskrivs om Kommunikationsverkets uppgifter. Lagens 2 § innehåller en förteckning över de uppgifter som åligger Kommunikationsverket enligt olika lagar. Det föreslås att lagen om elektroniska signaturer tas in i förteckningen i paragrafens 1 punkt.

2. Närmare stadganden och bestämmelser

Det kan uppstå ett behov av att utfärda närmare föreskrifter på grund av den snabba utvecklingen då det gäller certifieringsverksamheten och tekniken i anslutning till den. Det är nödvändigt att kunna utfärda närmare föreskrifter i synnerhet till följd av att certifieringsverksamheten är outvecklad och standardiseringsverksamheten inte är slutförd. Eftersom det är svårt att bedöma hur användningen av elektroniska signaturer och tillhandahållandet av certifikat i anslutning till dem utvecklas har det inte varit möjligt att i lagen beakta alla eventuella problem som kan uppkomma. Därför är det nödvändigt att det även genom Kommunikationsverkets föreskrifter och rekommendationer skall vara möjligt att styra sådana funktioner som ansluter sig till elektroniska signaturer och tillhandahållandet av certifikat.

Kommunikationsverket kunde meddela nödvändiga föreskrifter och rekommendationer om lämnande av de uppgifter som med stöd av 9 § skall uppges och om närmare innehåll i dem. Genom Kommunikationsverkets föreskrifter kunde man senare precisera de uppgifter som är relevanta för konstaterande av i lag definierade villkor och för utförande av tillsynsuppgiften.

Kommunikationsverket har enligt 22 § 2 mom. till uppgift att övervaka att den föreslagna lagen iakttas. Kommunikationsverket meddelar vid behov tekniska föreskrifter och rekommendationer om de krav som ställs på tillförlitligheten och datasäkerheten i verksamheten när det gäller certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat. Med tekniska föreskrifter och rekommendationer som Kommunikationsverket med stöd av 22 § meddelar avses sådana föreskrifter och rekommendationer som specificerar innehållet i de krav som enligt 7 och 10-15 § ställs på ett kvalificerat certifikat och certifikatutfärdarnas verksamhet och som omfattar endast tekniska och mindre viktiga detaljer.

Genom föreskrifterna skapas inte några nya skyldigheter för dem som tillhandahåller kvalificerade certifikat och till meddelandet av dessa föreskrifter skall endast hänföras utövande av prövningsrätten endast i ringa mån. Om certifikatmarknaden eller tekniken i anslutning till certifikaten utvecklas på ett sådant sätt att detta förutsätter bestämmelser om nya krav på certifikaten eller nya skyldigheter för certifikatutfärdaren, sker detta på lagnivå.

3. Ikraftträdande

Lagarna föreslås träda i kraft så snart som möjligt efter det att de har antagits och blivit stadfästa. Åtgärder som verkställigheten av lagarna förutsätter får dock vidtas innan lagarna träder i kraft.

4. Lagstiftningsordning

I regeringens proposition till lag om elektronisk kommunikation i förvaltningsärenden (RP 153/1999 rd) anses att en certifikatutfärdares - privat eller offentlig - verksamhet

skall jämställas med verksamhet inom den indirekta offentliga förvaltningen. Som motivering för detta anfördes att utfärdandet av ett certifikat gäller sökandens intresse på det sätt som avses i 16 § regeringsformen. I förvaltningsutskottets betänkande (FvUB 10/1999 rd) godkändes uppfattningen i regeringens proposition om certifieringsverksamhetens offentligrättsliga karaktär, fastän även motsatta åsikter framfördes när sakkunniga hördes.

I motiveringen till lagförslaget konstateras också att man i samband med genomförandet av direktivet om elektroniska signaturer på nytt kan bedöma arrangemangen med rättsskyddet för de kunder som använder certifikattjänster i förvaltningen. Detta är nödvändigt särskilt när det gäller förfarandet i certifikatutfärdarens verksamhet, om vilket bestäms särskilt i 7 § 1 mom. i nämnda lag. I momentet i fråga konstateras att när det gäller utfärdandet och upprätthållandet av certifikat liksom även användningen av register i anslutning till dem skall lagen om förvaltningsförfarande, språklagen, lagen om användning av samiska hos myndigheter (516/1991), lagen om offentlighet i myndigheternas verksamhet, personuppgiftslagen och arkivlagen iakttas.

Enligt 124 § 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. I den regeringsproposition (RP 1/1998 rd) som resulterade i grundlagen konstateras att kravet på ändamålsenlighet kan "när det är fråga om uppgifter i samband med serviceproduktion uppfyllas lättare än t.ex. i fråga om beslutsfattande som gäller en enskild persons eller sammanslutnings centrala rättigheter". I motiveringen konstateras vidare att bestämmelsen understryker betydelsen av att de som sköter offentliga förvaltningsuppgifter skall vara utbildade för ändamålet och sakkunniga samt att de skall stå under tillräcklig offentlig tillsyn.

Det lagförslag som skall ges kan anses uppfylla kraven enligt 124 § grundlagen på regleringen av verksamhet som gäller privata certifikatutfärdare som tillhandahåller kvalificerade certifikat. Med anledning härav kunde de kvalificerade certifikat som avses i lagförslaget och som ansluter sig till användningen av elektroniska signaturer godkännas även när förvaltningens elektroniska tjänster används. Detta är ytterst viktigt med tanke på de elektroniska tjänsternas utveckling. Att göra det möjligt att använda samma kvalificerade certifikat och den elektroniska signatur som skapats med hjälp därav såväl inom den privata som den offentliga sektorn i enlighet med propositionen är också en central faktor när det gäller att göra de elektroniska tjänsterna lätt tillgängliga.

I den regeringsproposition som nu skall avlåtas till riksdagen definieras ett kvalificerat certifikat av hög kvalitet och regleras ansvaret och skyldigheterna för certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat samt myndigheternas tillsyn över tillhandahållandet av kvalificerade certifikat. Tillhandahållandet av kvalificerade certifikat skall enligt detta lagförslag anses vara främst privaträttslig kommersiell verksamhet. Rättsskyddet för kunder till certifikatutfärdare som tillhandahåller sådana kvalificerade certifikat som används i elektroniska signaturer blir i den mån effektivt ordnat genom bestämmelserna i denna proposition om att bestämmelserna om certifieringsverksamhet och certifikat kunde upphävas i lagen om elektronisk kommunikation.

I vissa utlåtanden om lagförslaget har man anfört att propositionen inte i tillräcklig utsträckning tryggar finska medborgares språkliga rättigheter. Dessutom har det anförts att endast handlingar utfärdade av polisen skulle användas vid identifieringen av den som ansöker om ett kvalificerat certifikat för att en tillförlitlig identifiering skall kunna säkerställas.

I 12 § i lagförslaget ingår en bestämmelse om skyldigheterna för en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat att omsorgsfullt och på ett tillförlitligt sätt kontrollera identiteten hos en person som ansöker om ett kvalificerat certifikat. Certifikatutfärdaren som tillhandahåller allmänheten kvalificerade certifikat skall

identifiera sökanden personligen. Dessutom åläggs en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat i fall som avses i 16 § ett strängt skadeståndsansvar för skador som har åsamkats den som har förlitat sig på det kvalificerade certifikatet. I 12 § i lagförslaget ingår dessutom en bestämmelse om skyldigheten för en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat att innan avtal ingås informera sökanden skriftligen om villkoren för användning av det kvalificerade certifikatet, inbegripet eventuella begränsningar av användningen, och om frivilliga ackrediteringssystem, myndighetstillsynen över verksamheten samt förfarandena för klagomål och avgörande av tvister. Nämnda information skall enligt 12 § ges den som ansöker om ett kvalificerat certifikat skriftligen i sådan form att sökanden kan förstå den utan svårighet. När finska medborgare betjänas kan detta krav i regel anses innebära att tjänsterna tillhandahålls åtminstone på de officiella språk som används i Finland. Såväl de språkliga rättigheterna för som en tillförlitlig identifiering av sökanden blir sålunda ändamålsenligt beaktade i lagförslaget.

Det centrala syftet med certifieringsverksamheten är att garantera en tillförlitlig elektronisk kommunikation när det gäller såväl kommersiella tjänster som förvaltningstjänster. När en certifikatutfärdare utfärdar ett kvalificerat certifikat ger han sökanden metoder att på ett tillförlitligt sätt använda elektroniska tjänster. Utöver de krav som i detta lagförslag har uppställts på certifikatutfärdare som tillhandahåller kvalificerade certifikat bör man sträva efter att undvika att ålägga certifieringsverksamheten onödigt tunga skyldigheter. Det är skäl att inte ålägga certifieringsverksamheten sådana rättsliga skyldigheter som t.o.m. kan anses utgöra ett hinder för handeln, om avsikten är att användningen av certifikat skall främjas och de elektroniska tjänsterna utvecklas. Privat kommunikation och kommunikation med myndigheterna förutsätter tekniskt sett inte några annorlunda krav eller bestämmelser. Ändamålsenligheten i certifieringsverksamheten kontrolleras både av Kommunikationsverket och av dataskyddsombudet, och därför torde särskilda garantier för rättsskyddet i fråga om tillvägagångssättet inte längre inneha en så central ställning som när lagen om elektronisk kommunikation i förvaltningsärenden stiftades.

I artikel 3.7 i direktivet om elektroniska signaturer, vilket genomförs genom denna lag, bestäms att medlemsstaterna får förena användningen av elektroniska signaturer i den offentliga sektorn med eventuella ytterligare krav. Sådana krav skall vara objektiva, tydliga, proportionella och icke-diskriminerande och skall endast gälla de särskilda egenskaperna för den berörda tillämpningen. Dessa krav får inte utgöra ett hinder för gränsöverskridande tjänster för medborgaren. Om det vid tillämpningen av vissa elektroniska tjänster inom förvaltningen framkommer sådana särdrag om vilka bestämmelser som avviker från bestämmelserna i detta lagförslag bör utfärdas, skall bestämmelser av detta slag tas in i speciallagstiftningen för förvaltningsområdet i fråga. Som exempel kan nämnas sådan elektronisk kommunikation som hänför sig till social- och hälsovårdstjänster samt till försvarsförvaltningens tjänster. I samband med utvecklandet av dessa tjänster bör man särskilt dryfta om de elektroniska signaturerna och användningen av certifikat i anslutning till dem är lämpliga samt behovet av eventuella tilläggskrav med beaktande av dessa områdens särdrag och lagstiftning.

Å andra sidan omfattar den elektroniska kommunikationen inom förvaltningen en betydande mängd sådan kommunikation som inte alls behöver certifikat eller elektroniska signaturer som gjorts med hjälp av dem. Man måste även i fortsättningen inom förvaltningen kunna kommunicera med e-post, telefaxmeddelande och telefon och även på andra möjliga sätt när det inte är nödvändigt att i kommunikationsprocessen beakta särskilda krav som har samband med datasäkerheten.

Regeringen anser att lagförslagen kan stiftas i normal lagstiftningsordning. I detta lagförslag ingår bestämmelser om nya metoder med hänsyn till elektronisk kommunikation inom förvaltningen. Till följd av de associeringar till grundlagen som avser certifieringsverksamhetens offentligrättsliga karaktär, individens ställning när certifikat utfärdas samt näringsfriheten anser regeringen det

vara önskvärt att riksdagens grundlagsutskott skall ges möjlighet att ge sitt utlåtande om förslaget.

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

Lagförslagen

1.

Lag

om elektroniska signaturer

I enlighet med riksdagens beslut föreskrivs:

1 kap.

Allmänna bestämmelser

1 §

Lagens syfte

Syftet med denna lag är att underlätta användningen av elektroniska signaturer och tillhandahållandet av produkter för elektroniska signaturer och tjänster i anslutning till dem samt att främja datasekretessen och dataskyddet vid elektronisk handel och elektronisk kommunikation.

2 §

Definitioner

I denna lag avses med

1) *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,

2) *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 undertecknarens kontrollerar, och

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

3) *undertecknare* en fysisk person som lagligen innehar signaturframställningsdata och agerar på sina egna vägnar eller på den fysiska eller juridiska persons vägnar som han eller hon företräder,

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

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

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

7) *certifikat* ett intyg i elektronisk form som kopplar ihop signaturverifieringsdata med en undertecknare och bekräftar undertecknarens identitet,

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

9) *produkt för elektroniska signaturer* maskinvara eller programvara, eller relevant del i sådant system, som är avsedd att användas av dem som tillhandahåller tjänster vid tillhandahållande av tjänster i anslutning till elektroniska signaturer eller som är avsedd att användas för att skapa eller verifiera elektroniska signaturer, samt

10) *tjänst i anslutning till elektroniska signaturer* tillhandahållande av certifikat samt andra produkter för elektroniska signaturer och tjänster i anslutning till dem.

3 §

Tillämpningsområde

Denna lag tillämpas på elektroniska signaturer samt på dem som tillhandahåller allmänheten produkter för elektroniska signaturer och tjänster i anslutning till dem.

Om användningen av elektroniska signaturer inom förvaltningen gäller dessutom vad som bestäms särskilt.

4 §

Fri rörlighet för tjänster och produkter

I denna lag avsedda produkter för elektroniska signaturer och tjänster i anslutning till dem skall ha fri rörlighet på den inre marknaden.

5 §

Säkra anordningar för signaturframställning

En säker anordning för signaturframställning skall 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 skall 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 gemenskapernas 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.

6 §

Kontrollorgan

Kommunikationsverket kan utse kontrollorgan med uppgift att bedöma om anordningar för signaturframställning uppfyller kraven i 5 § 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 verksamheten 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 skall 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 skall 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, skall Kommunikationsverket återkalla beslutet genom vilket det utsett kontrollorganet. Kontrollorganen skall 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.

2 kap.

Tillhandahållande av kvalificerade certifikat

7 §

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 10-15 §.

Ett kvalificerat certifikat skall innehålla

1) uppgift om att certifikatet är ett kvalificerat certifikat,

2) uppgift om certifikatutfärdaren och 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 det kvalificerade certifikatets användningsområde, samt

9) särskilda uppgifter om undertecknaren, om de behövs för ändamålet med det kvalificerade certifikatet.

8 §

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 i 7 §, om

1) certifikatutfärdaren är etablerad i en annan 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 annan 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 annan 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 tredje länder eller internationella organisationer.

9 §

Anmälan om inledande av verksamhet

En certifikatutfärdare som avser att tillhandahålla allmänheten kvalificerade certifikat skall innan sådana certifikat börjar tillhandahållas göra en skriftlig anmälan till Kommunikationsverket. Anmälan skall innehålla certifikatutfärdarens namn och kontaktuppgifter samt de uppgifter som behövs för att säkerställa att kraven i 7 § och 10-15 § uppfylls. Kommunikationsverket kan meddela för tillsynen behövliga föreskrifter och rekommendationer om det närmare innehållet i de uppgifter som skall lämnas och om inlämnandet av dem till Kommunikationsverket.

Kommunikationsverket skall utan dröjsmål efter det att anmälan inkommit förbjuda certifikatutfärdaren att tillhandahålla certifikat som anges vara kvalificerade, om certifikaten inte uppfyller kraven i 7 § 2 mom. eller om certifikatutfärdaren inte uppfyller kraven i 10-15 §.

Certifikatutfärdaren skall utan dröjsmål skriftligen underrätta Kommunikationsverket, om de uppgifter som avses i 1 mom. ändras.

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

10 §

Allmänna skyldigheter för certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat

En certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat skall bedriva verksamheten på ett omsorgsfullt, tillförlitligt och ändamålsenligt sätt. Certifikatutfärdaren skall 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 skall

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.

11 §

Tillförlitliga maskinvaror och programvaror

En certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat skall 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 gemenskapernas officiella tidning.

12 §

Utfärdande av kvalificerade certifikat

En certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat skall omsorgsfullt och på ett tillförlitligt sätt kontrollera sökandens identitet och andra uppgifter som hänför sig till sökandens person och som är relevanta för utfärdandet och upprätthållandet av det kvalificerade certifikatet. Certifikatutfärdaren som tillhandahåller allmänheten kvalificerade certifikat skall identifiera sökanden personligen.

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

13 §

Återkallande av ett kvalificerat certifikat

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

En certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat skall 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 skall alltid underrättas om att det kvalificerade certifikatet har återkallats och om tidpunkten för återkallandet.

14 §

Register som skall föras av certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat

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

1) de uppgifter som det kvalificerade certifikatet skall innehålla enligt 7 § 2 mom.,

2) de uppgifter som hänför sig till sökandens person och som avses i 12 § 1 mom., inbegripet uppgift om det förfarande för identifiering av sökanden som använts då det kvalificerade certifikatet utfärdades, samt

3) de uppgifter som avses i 21 § om kontroll av ett certifikats giltighetstid som gjorts på spärrlistan, om en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat utnyttjar rätten att lagra uppgifter enligt 21 §.

En certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat skall säkerställa att den som förlitar sig på en avancerad elektronisk signatur som är baserad på ett kvalificerat certifikat har tillgång till certifikatets i 7 § 2 mom. definierade innehåll.

Certifikatutfärdaren skall också föra ett offentligt register över återkallade kvalificerade certifikat (spärrlista). På spärrlistan skall på lämpligt sätt och 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. skall vara tillgängliga dygnet runt.

15 §

Förvaring av uppgifterna i certifikatregistret

En certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat skall på ett tillförlitligt och ändamålsenligt sätt förvara uppgifterna i certifikatregistret i 10 år från det certifikatet upphörde att gälla.

16 §

Skadeståndsansvar för certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat

En certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat är ansvarig för en skada som åsamkats 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 7 § 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 denna anlitat inte kan användas som komplement till varandra, eller

5) certifikatutfärdaren eller en person som denna anlitat inte har återkallat det kvalificerade certifikatet på det sätt som anges i 13 §.

Certifikatutfärdaren är befriad från ansvaret enligt 1 mom., om utfärdaren visar att skadan inte har orsakats av vårdslöshet hos utfärdaren själv eller någon som denna har anlitat.

En certifikatutfärdare som avses i 1 mom. ansvarar inte för skada som orsakats av att ett kvalificerat certifikat har använts i strid med de begränsningar av användningen som ingår i det.

Om skadeståndsansvaret för certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat gäller i övrigt vad som bestäms i skadeståndslagen (412/1974). Vad som bestäms i denna paragraf tillämpas också på en certifikatutfärdare som för allmänheten garanterar att ett certifikat är ett kvalificerat certifikat.

17 §

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 13 § 2 mom.

En konsument har emellertid 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 at 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 skall återkallas så som anges i 13 § 1 mom.

Ett avtalsvillkor som till konsumentens nackdel avviker från bestämmelserna i 2 mom. är utan verkan.

3 kap.

Elektroniska signaturers rättsverkan och behandlingen av personuppgifter

18 §

Elektroniska signaturers rättsverkan

Om det beträffande en rättshandling i lag ställs krav på underskrift, uppfylls detta krav åtminstone en sådan avancerad elektronisk signatur som baserar sig på ett kvalificerat certifikat och har skapats med en säker anordning för signaturframställning.

19 §

Behandling av personuppgifter

En certifikatutfärdare som tillhandahåller allmänheten certifikat får inhämta de personuppgifter som är nödvändiga för att utfärda och upprätthålla ett certifikat endast från undertecknaren själv. När det gäller certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat ingår närmare bestämmelser om utfärdandet av kvalificerade certifikat, de register som skall föras och förvaringen av uppgifter i 2 kap.

När sökandens identitet kontrolleras får certifikatutfärdaren kräva att sökanden uppger sin personbeteckning. Undertecknarens personbeteckning får inte tas in i certifikatet.

Endast med undertecknarens uttryckliga samtycke får personuppgifter

1) inhämtas från andra källor än från undertecknaren själv eller

2) behandlas för andra ändamål än det som anges i 1 mom.

I fråga om behandlingen av personuppgifter gäller dessutom vad som bestäms i personuppgiftslagen (523/1999).

20 §

Användning av befolkningsdatasystemet

Certifikatutfärdaren har med sökandens uttryckliga samtycke rätt att ur befolkningsdatasystemet skaffa och i det kontrollera de personuppgifter som lämnats av sökanden.

Uppgifterna i befolkningsdatasystemet lämnas ut som en offentligrättslig prestation enligt lagen om grunderna för avgifter till staten (150/1992).

21 §

Kontroll av certifikats giltighetstid

Certifikatutfärdaren får lagra uppgifter om kontroll av certifikatens giltighetstid som gjorts på spärrlistan. De lagrade uppgifterna får användas endast för fakturering av användningen av certifikat och för verifiering av rättshandlingar som företagits med hjälp av elektroniska signaturer som är baserad på certifikat.

4 kap.

Allmän styrning och tillsyn

22 §

Allmän styrning och tillsyn

Den allmänna styrningen samt utvecklandet av certifikatverksamheten ankommer på kommunikationsministeriet.

Kommunikationsverket skall övervaka att denna lag iakttas. Kommunikationsverket meddelar vid behov tekniska föreskrifter och rekommendationer om kraven på tillförlitlighet och datasäkerhet i verksamheten när det gäller certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat som hänför sig till elektroniska signaturer.

Dataombudsmannen skall övervaka att bestämmelserna om personuppgifter i denna lag iakttas. Vid fullgörandet av uppgiften har dataombudsmannen rätt att få information och utöva tillsyn i enlighet med personuppgiftslagen. Bestämmelser om sökande av ändring när det gäller dataombudsmannens verksamhet finns i personuppgiftslagen.

23 §

Rätt till upplysningar

Utan hinder av bestämmelserna om tystnadsplikt har Kommunikationsverket rätt att av certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat som hänför sig till elektroniska signaturer och av dem som dessa certifikatutfärdare anlitar få de upplysningar som behövs för fullgörande av de uppgifter som anges i 22 §.

24 §

Inspektionsrätt

En inspektör som Kommunikationsverket har förordnat för uppgiften har rätt att utföra inspektioner för tillsynen över att denna lag och föreskrifter som meddelas med stöd av lagen följs. Den som utför inspektionen har rätt att hos en certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat som hänför sig till elektroniska signaturer eller hos dem som denna anlitar undersöka sådana maskin- och programvaror som kan vara av betydelse vid tillsynen över att denna lag och föreskrifter som meddelas med stöd av lagen följs.

En certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat som hänför sig till elektroniska signaturer, och de personer som denna anlitat, skall för inspektion ge en inspektör som avses i 1 mom. tillträde till produktions- och affärslokaler samt lagerutrymmen.

Kommunikationsverket har rätt att få handräckning av polisen för utförande av inspektion enligt 1 och 2 mom.

25 §

Tystnadsplikt

De som fullgör uppgifter enligt denna lag har tystnadsplikt enligt vad som bestäms i lagen om offentlighet i myndigheternas verksamhet (621/1999).

5 kap.

Särskilda bestämmelser

26 §

Straffbestämmelse

Bestämmelser om straff för personregisterbrott finns i 38 kap. 9 § strafflagen (39/1889) och bestämmelser om straff för personregisterförseelse finns i 48 § 2 mom. personuppgiftslagen.

27 §

Förvaltningstvångsmedel

Om någon bryter mot denna lag eller mot föreskrifter som har utfärdats med stöd av den, kan Kommunikationsverket ålägga denne att rätta sitt fel eller sin försummelse. 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. Beträffande vite, hot om avbrytande och hot om tvångsutförande gäller vad som föreskrivs i viteslagen (1113/1990).

Kostnaderna för en åtgärd som vidtagits på den försumliges bekostnad betalas av statens medel och indrivs hos den försumlige i den ordning som bestäms i lagen om indrivning av skatter och avgifter i utsökningsväg (367/1961).

28 §

Ändringssökande

I beslut som Kommunikationsverket har fattat med stöd av denna lag får ändring sökas enligt förvaltningsprocesslagen (586/1996).

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

29 §

Ikraftträdande

Denna lag träder i kraft den 20 .

Åtgärder som verkställigheten av lagen förutsätter får vidtas innan lagen träder i kraft.

30 §

Övergångsbestämmelse

En certifikatutfärdare som har börjat tillhandahålla allmänheten kvalificerade certifikat innan denna lag har trätt i kraft skall inom tre månader från ikraftträdandet göra en anmälan enligt 9 §.

2.

Lag

om ändring av 2 § lagen om kommunikationsförvaltningen

I enlighet med riksdagens beslut

ändras i lagen den 29 juni 2001 om kommunikationsförvaltningen (625/2001) 2 § som följer:

2 §

Kommunikationsverkets uppgifter

Kommunikationsverket har till uppgift att

1) sköta de uppgifter som enligt telemarknadslagen (396/1997), radiolagen (517/1988), postlagen (907/1993), lagen om televisions- och radioverksamhet (744/1998), lagen om statens televisions- och radiofond (745/1998), lagen om integritetsskydd vid telekommunikation och dataskydd inom televerksamhet (565/1999) samt lagen om elektroniska signaturer (/) ankommer på Kommunikationsverket, samt

2) sköta andra uppgifter som ankommer på Kommunikationsverket enligt andra bestämmelser eller kommunikationsministeriets föreskrifter.

———

Denna lag träder i kraft den 20 .

Åtgärder som verkställigheten av lagen förutsätter får vidtas innan lagen träder i kraft.

———

Helsingfors den 26 oktober 2001

Republikens President

TARJA HALONEN

Kommunikationsminister *Olli-Pekka Heinonen*

Bilaga
Parallelltexter

2.

Lag

om ändring av 2 § lagen om kommunikationsförvaltningen

I enlighet med riksdagens beslut
ändras i lagen den 29 juni 2001 om kommunikationsförvaltningen (625/2001) 2 § som följer:

Gällande lydelse	*Föreslagen lydelse*
2 §	2 §
Kommunikationsverkets uppgifter	*Kommunikationsverkets uppgifter*
Kommunikationsverket har till uppgift att 1) sköta de uppgifter som enligt telemarknadslagen (396/1997), radiolagen (517/1988), postlagen (907/1993), lagen om televisions- och radioverksamhet (744/1998), lagen om statens televisions- och radiofond (745/1998) samt lagen om integritetsskydd vid telekommunikation och dataskydd inom televerksamhet (565/1999) ankommer på Kommunikationsverket, samt 2) sköta andra uppgifter som ankommer på Kommunikationsverket enligt andra bestämmelser eller kommunikationsministeriets föreskrifter.	Kommunikationsverket har till uppgift att 1) sköta de uppgifter som enligt telemarknadslagen (396/1997), radiolagen (517/1988), postlagen (907/1993), lagen om televisions- och radioverksamhet (744/1998), lagen om statens televisions- och radiofond (745/1998), lagen om integritetsskydd vid telekommunikation och dataskydd inom televerksamhet (565/1999) *samt lagen om elektroniska signaturer (/)* ankommer på Kommunikationsverket, samt 2) sköta andra uppgifter som ankommer på Kommunikationsverket enligt andra bestämmelser eller kommunikationsministeriets föreskrifter.

———

Denna lag träder i kraft den 20 .

———