Regeringens proposition 1999/2000:117

Lag om kvalificerade elektroniska signaturer, m.m.

Prop. 1999/2000:117

Regeringen överlämnar denna proposition till riksdagen.

Malmö den 18 maj 2000

Göran Persson

Mona Sahlin
(Näringsdepartementet)

Propositionens huvudsakliga innehåll

För genomförande av ett EG-direktiv om ett gemenskapsramverk för elektroniska signaturer (1999/93/EG) föreslås i propositionen en ny lag om s.k. kvalificerade elektroniska signaturer. Vidare föreslås en mindre ändring i sekretesslagen (1980:100) för att tillgodose behovet av sekretesskydd för koder o.d. som möjliggör säkerhetskontroll.

En elektronisk signatur kan användas för att säkerställa att elektroniskt överförd information inte har förändrats, att informationens avsändare är den som uppges samt att avsändaren inte senare förnekar att han eller hon sänt informationen.

För att kunna använda en elektronisk signatur i ett öppet system där parterna inte känner varandra i förväg, såsom Internet, behöver parterna kunna inhämta information om kopplingen mellan en elektronisk signatur och en bestämd person. Därför har det utvecklats ett system för elektroniska signaturer som kan benämnas det öppna nyckelsystemet (Public Key Infrastructure, PKI). I detta system utfärdas ett elektroniskt intyg (certifikat) av en betrodd tredje part. Ett certifikat innehåller uppgifter om vem som är innehavare av en elektronisk signatur.

Direktivets reglering bygger på elektroniska signaturer enligt det öppna nyckelsystemet. Det innehåller främst näringsrättsliga regler om dem som utfärdar vissa certifikat, men även regler om skadeståndsansvar och om rättsverkan av elektroniska signaturer.

Den föreslagna lagen innehåller regler om krav på, tillsyn över och skadeståndsansvar för den som utfärdar certifikat för elektroniska signaturer till allmänheten, om certifikaten anges ha en viss säkerhetsnivå. Sådana certifikat kallas i lagen för kvalificerade certifikat. En särställning ges vidare åt elektroniska signaturer med en viss säkerhetsnivå, s.k.

kvalificerade elektroniska signaturer. Lagens regler omfattar inte certifikat som utfärdas inom s.k. slutna system. Lagen reglerar inte heller frågor om ingående eller giltighet av avtal.

Enligt direktivet kan medlemsstaterna införa frivilliga ackrediteringssystem som syftar till att höja nivån på tillhandahållandet av certifikattjänster. Lagen (1992:1119) om teknisk kontroll ger möjlighet till frivillig ackreditering av certifieringsorgan med det syfte som anges i direktivet.

En tillsynsmyndighet förutses utöva tillsyn över efterlevnaden av bestämmelserna i lagen och föreskrifter som meddelas med stöd av lagen. Regeringen bemyndigas att införa ett avgiftssystem för att bekosta myndighetens verksamhet.

Den nya lagen föreslås träda i kraft den 1 januari 2001.

Innehållsförteckning

1 Förslag till riksdagsbeslut

Regeringen föreslår att riksdagen antar regeringens förslag till

1. lag om kvalificerade elektroniska signaturer,
2. lag om ändring i sekretesslagen (1980:100).

2 Lagtext

Regeringen har följande förslag till lagtext.

2.1 Förslag till lag om kvalificerade elektroniska signaturer

Härigenom föreskrivs[1] följande.

Allmän bestämmelse

1 § Syftet med denna lag är att underlätta användningen av elektroniska signaturer, genom bestämmelser om säkra anordningar för signaturframställning, om kvalificerade certifikat för elektroniska signaturer och om utfärdande av sådana certifikat.

Lagen gäller sådana certifikatutfärdare som är etablerade i Sverige och som utfärdar kvalificerade certifikat till allmänheten.

Definitioner

2 § I lagen avses med

elektronisk signatur: data i elektronisk form som är fogade till eller logiskt knutna till andra elektroniska data och som används för att kontrollera att innehållet härrör från den som framstår som utställare och att det inte har förvanskats,

avancerad elektronisk signatur: elektronisk signatur som

a) är knuten uteslutande till en undertecknare,

b) gör det möjligt att identifiera undertecknaren,

c) är skapad med hjälpmedel som endast undertecknaren kontrollerar, och

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

kvalificerad elektronisk signatur: avancerad elektronisk signatur som är baserad på ett kvalificerat certifikat och som är skapad av en säker anordning för signaturframställning,

undertecknare: fysisk person som behörigen innehar en anordning för signaturframställning,

signaturframställningsdata: unika data, såsom koder eller hemliga krypteringsnycklar, som används för att skapa en elektronisk signatur,

anordning för signaturframställning: maskin- eller programvara för användning av signaturframställningsdata,

säker anordning för signaturframställning: anordning för signaturframställning som uppfyller kraven i 3 §,

signaturverifieringsdata: data, såsom koder eller öppna krypteringsnycklar, som används för att verifiera en elektronisk signatur,

[1] Jfr Europaparlamentets och rådets direktiv 1999/93/EG av den 13 december 1999 om ett gemenskapsramverk för elektroniska signaturer (EGT L 13, 19.1.2000, s. 12, Celex 399L0093).

certifikat: intyg i elektronisk form som kopplar ihop signaturverifieringsdata med en undertecknare och bekräftar dennes identitet,

kvalificerat certifikat: certifikat som uppfyller kraven i 6 eller 7 §,

certifikatutfärdare: den som utfärdar certifikat eller som garanterar att någon annans certifikat uppfyller vissa krav.

Säkra anordningar för signaturframställning

3 § En anordning för signaturframställning som anges vara säker skall säkerställa att signaturen är tillfredsställande skyddad mot förfalskning. Anordningen skall även säkerställa att signaturframställningsdata

1. i praktiken kan förekomma endast en gång,
2. med rimlig säkerhet inte kan härledas, och
3. på ett tillfredsställande sätt kan skyddas av den behörige undertecknaren, så att andra inte kan komma åt eller använda dem.

Anordningen får inte förändra de uppgifter som skall signeras elektroniskt eller hindra att de presenteras för undertecknaren före den elektroniska signeringen.

4 § Kraven i 3 § på en säker anordning för signaturframställning skall anses uppfyllda för sådan maskin- eller programvara som överensstämmer med sådana standarder för produkter för elektroniska signaturer som Europeiska gemenskapernas kommission fastställt och offentliggjort referensnummer till i Europeiska gemenskapernas officiella tidning.

5 § En anordning som anges vara en säker anordning för signaturframställning får släppas ut på marknaden eller användas för att skapa en kvalificerad elektronisk signatur endast om den uppfyller kraven i 3 §. En prövning av om kraven är uppfyllda skall göras av ett organ som anmälts för detta ändamål enligt lagen (1992:1119) om teknisk kontroll.

Med en prövning enligt första stycket likställs en prövning av ett organ som anmälts för samma ändamål av en annan stat inom Europeiska ekonomiska samarbetsområdet.

Kvalificerade certifikat

6 § För att ett certifikat skall få kallas kvalificerat skall det vara utfärdat för viss tid av en certifikatutfärdare, som uppfyller kraven i 9–12 §§ och föreskrifter meddelade med stöd av 13 §, samt innehålla

1. uppgift om att det utfärdats som ett kvalificerat certifikat,
2. certifikatutfärdarens namn och adress samt uppgift om etableringsland,
3. undertecknarens namn eller pseudonym med uppgift om att det är en pseudonym,
4. särskilda uppgifter om undertecknaren, om de är relevanta för ändamålet med certifikatet,
5. signaturverifieringsdata som motsvarar de signaturframställningsdata som undertecknaren vid tidpunkten för utfärdandet har kontroll över,
6. uppgift om certifikatets giltighetstid,

7. certifikatets identifieringskod,

8. certifikatutfärdarens avancerade elektroniska signatur eller en elektronisk signatur med motsvarande säkerhetsnivå, och

9. uppgift om eventuella begränsningar av certifikatets användningsområde eller av värdet på de transaktioner för vilka certifikatet kan användas (transaktionsbelopp).

Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela närmare föreskrifter om krav enligt första stycket.

7 § Om ett certifikat som uppfyller kraven i 6 § första stycket 1–9 utfärdats av en certifikatutfärdare som inte är etablerad i Sverige skall certifikatet anses kvalificerat om

1. certifikatutfärdaren är etablerad i en annan stat inom Europeiska ekonomiska samarbetsområdet och där får utfärda kvalificerade certifikat,

2. certifikatutfärdaren uppfyller krav som motsvarar dem som anges i 9–12 §§ och föreskrifter meddelade med stöd av 13 § och är ackrediterad i en annan stat inom Europeiska ekonomiska samarbetsområdet, eller

3. certifikatet garanteras vara kvalificerat av en certifikatutfärdare som avses i 1 eller i 6 § första stycket.

Utfärdande av kvalificerade certifikat

8 § En certifikatutfärdare som avser att utfärda kvalificerade certifikat till allmänheten är skyldig att anmäla detta hos den myndighet som regeringen bestämmer (tillsynsmyndigheten) innan verksamheten påbörjas.

9 § En certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten skall bedriva verksamheten tillförlitligt och

1. ha personal med tillräcklig kompetens och erfarenhet för verksamheten, särskilt vad avser ledning, teknik och säkerhetsrutiner,

2. använda sådana rutiner för administration och ledning som uppfyller erkända standarder,

3. använda pålitliga system och produkter som är skyddade mot ändringar och se till att teknisk och kryptografisk säkerhet upprätthålls,

4. förfoga över tillräckliga ekonomiska medel för att kunna bedriva verksamheten enligt denna lag och bära risken för skadeståndsskyldighet,

5. ha säkra rutiner för identitetskontroll av de undertecknare som kvalificerade certifikat utfärdas till,

6. förfoga över ett snabbt och säkert system för registrering och omedelbar återkallelse av kvalificerade certifikat, och

7. vidta åtgärder mot förfalskning av kvalificerade certifikat och i förekommande fall se till att framställandet av signaturframställningsdata sker konfidentiellt.

Kraven i första stycket 3 skall anses uppfyllda för sådan maskin- eller programvara som överensstämmer med sådana standarder för produkter för elektroniska signaturer som Europeiska gemenskapernas kommission fastställt och offentliggjort referensnummer till i Europeiska gemenskapernas officiella tidning.

10 § En certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten skall

1. omedelbart återkalla ett certifikat när undertecknaren begär det eller när det annars finns anledning till det,
2. säkerställa att exakt tidpunkt kan anges för utfärdande och återkallelse av certifikat, och
3. säkerställa att av utfärdaren framställda signaturframställningsdata och signaturverifieringsdata kan användas som komplement till varandra.

11 § En certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten skall bevara all relevant information om certifikaten under den tid som är motiverad med hänsyn till typen av certifikat och övriga omständigheter. Certifikatutfärdaren skall även använda tillförlitliga system för lagring av kvalificerade certifikat i verifierbar form, så att

1. endast behöriga personer kan göra tillägg och ändringar,
2. uppgifternas äkthet kan kontrolleras,
3. certifikaten är offentligt tillgängliga endast när innehavarna av certifikaten har lämnat sitt samtycke, och
4. tekniska förändringar som äventyrar säkerhetskraven framgår för den som handhar systemet.

Certifikatutfärdaren får inte lagra eller kopiera signaturframställningsdata.

12 § Innan en certifikatutfärdare ingår avtal om att utfärda ett kvalificerat certifikat skall certifikatutfärdaren skriftligen och på ett lättbegripligt språk informera motparten om

1. begränsningar och andra villkor för användning av certifikatet,
2. frivillig ackreditering eller certifiering som avses i lagen (1992:1119) om teknisk kontroll, och
3. förfaranden för klagomål och avgörande av tvister.

Informationen enligt första stycket får överföras elektroniskt.

Informationen skall göras tillgänglig också för annan som är beroende av certifikatet och som begär att få den.

13 § Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får utfärda närmare bestämmelser om krav enligt 9–12 §§.

Skadestånd

14 § En certifikatutfärdare som till allmänheten utfärdar certifikat som anges vara kvalificerade skall ersätta den skada som åsamkats den som förlitat sig på certifikatet, om skadan uppkommit genom att

1. certifikatutfärdaren inte har uppfyllt kraven i 10 §,
2. certifikatet inte uppfyller kraven i 6 § första stycket, eller
3. certifikatet vid utfärdandet innehöll felaktiga uppgifter.

Certifikatutfärdaren är dock inte skyldig att betala ersättning om utfärdaren kan visa att skadan inte har orsakats av vårdslöshet hos utfärdaren själv. Certifikatutfärdaren är inte heller ersättningsskyldig för en skada som härrör från att ett kvalificerat certifikat använts i strid med

begränsningar som gäller användningsområde eller transaktionsbelopp och som tydligt angetts i certifikatet.

Vad som sägs i första stycket 2 och 3 samt i andra stycket gäller även en certifikatutfärdare som garanterar att en annan certifikatutfärdares certifikat är kvalificerade.

15 § Avtalsvillkor som i jämförelse med 14 § är till nackdel för den som förlitar sig på certifikatet är utan verkan mot denne.

Behandling av personuppgifter

16 § En certifikatutfärdare som utfärdar certifikat till allmänheten får inhämta personuppgifter endast direkt från den som uppgifterna avser eller med dennes uttryckliga samtycke och endast i den utsträckning som är nödvändig för att utfärda eller upprätthålla ett certifikat. Uppgifterna får inte samlas in eller behandlas för andra ändamål utan uttryckligt samtycke från den som uppgifterna avser.

Kvalificerade elektroniska signaturer

17 § Om det i lag eller annan författning ställs krav på egenhändig underskrift eller motsvarande och om det är tillåtet att uppfylla kravet med elektroniska medel, skall en kvalificerad elektronisk signatur anses uppfylla kravet. Vid kommunikation med eller mellan myndigheter kan dock användningen av elektroniska signaturer vara förenad med ytterligare krav.

Tillsyn

18 § Tillsynsmyndigheten skall ha tillsyn över efterlevnaden av denna lag och föreskrifter som har utfärdats med stöd av lagen.

Tillsynsmyndigheten skall föra och ge offentlighet åt en förteckning över certifikatutfärdare som anmält sig enligt 8 § och som enligt denna lag får utfärda kvalificerade certifikat.

19 § Tillsynsmyndigheten har rätt att på begäran få de upplysningar och ta del av de handlingar som behövs för tillsynen.

Tillsynsmyndigheten har också rätt att få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, där verksamhet som står under tillsyn bedrivs.

Tillsynsmyndigheten har rätt att få biträde av kronofogdemyndigheten för tillsyn enligt första och andra styckena.

20 § Tillsynsmyndigheten får meddela de förelägganden och förbud som behövs för efterlevnaden av denna lag eller av föreskrifter som meddelats med stöd av lagen.

Tillsynsmyndigheten får förelägga en certifikatutfärdare, som till allmänheten utfärdar certifikat som anges vara kvalificerade, att helt eller delvis upphöra med denna verksamhet, endast om mindre ingripande

åtgärder visat sig vara verkningslösa. Myndigheten får besluta hur verksamheten skall avvecklas.

21 § Förelägganden och förbud enligt denna lag får förenas med vite.

Avgifter

22 § Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela föreskrifter om skyldighet för certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten att betala avgift för tillsynsmyndighetens verksamhet enligt denna lag.

Överklagande

23 § Tillsynsmyndighetens beslut enligt denna lag eller enligt föreskrifter som meddelats med stöd av lagen får överklagas hos allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Tillsynsmyndigheten får bestämma att beslut enligt denna lag skall gälla omedelbart.

---

1. Denna lag träder i kraft den 1 januari 2001.

2. Certifikatutfärdare som redan före ikraftträdandet utfärdar sådana certifikat som medför anmälningsplikt enligt 8 § behöver inte göra anmälan före den 1 februari 2001.

3. 15 § tillämpas inte i fråga om avtal som träffats före ikraftträdandet.

2.2 Förslag till lag om ändring i sekretesslagen (1980:100)

Härigenom föreskrivs att 5 kap. 3 § sekretesslagen (1980:100)[1] skall ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
5 kap.	
3 §[2]	
Sekretess gäller för uppgift som lämnar eller kan bidra till upplysning om chiffer, kod eller liknande metod som har till syfte att underlätta befordran eller användning i allmän verksamhet av uppgifter utan att föreskriven sekretess åsidosätts, om det kan antas att syftet med metoden motverkas om uppgiften röjs.	Sekretess gäller för uppgift som lämnar eller kan bidra till upplysning om chiffer, kod eller liknande metod som har till syfte att *1.* underlätta befordran eller användning i allmän verksamhet av uppgifter utan att föreskriven sekretess åsidosätts, *eller* *2. göra det möjligt att kontrollera om data i elektronisk form har förvanskats,* om det kan antas att syftet med metoden motverkas om uppgiften röjs.

Sekretess gäller i verksamhet som avser förande av eller uttag ur körkortsregistret för uppgift om körkorts referensnummer, om det inte står klart att uppgiften kan röjas utan fara för att kontrollen av körkorts äkthet motverkas om uppgiften röjs.

Denna lag träder i kraft den 1 januari 2001.

[1] Lagen omtryckt 1992:1474.
[2] Senaste lydelse 1994:595.

3 Ärendet och dess beredning

Den 30 november 1999 antogs Europaparlamentets och rådets direktiv 1999/93/EG av den 13 december 1999 om ett gemenskapsramverk för elektroniska signaturer. Direktivet innehåller bestämmelser om elektroniska signaturers rättsliga verkan och en reglering av de organ som avser att erbjuda elektroniska intyg om signaturers äkthet. Direktivet trädde i kraft den 19 januari 2000 och skall vara genomfört i medlemsstaterna senast den 19 juli 2001. Direktivet bifogas som *bilaga 1*.

Under förhandlingarna om direktivet skedde samråd med en av Näringsdepartementet tillkallad referensgrupp bestående av företrädare för Kommerskollegium, Statskontoret, Riksarkivet, SWEDAC, Post- och telestyrelsen, Konsumentverket, Riksskatteverket, Göteborgs universitet, IT-kommissionen, Svenska kommunförbundet, Stockholms Handelskammare, SEIS, Sveriges advokatsamfund, Svenska Bankföreningen, Sveriges Industriförbund, Svenska IT-företagen, Advokatfirman Lagerlöf & Leman, Telia Promotor AB, Tele2 AB, Posten AB, Ericsson AB, iD2 Technologies AB och IBM Svenska AB.

Inför antagandet av direktivet var detta föremål för behandling i riksdagens EU-nämnd inför teleråden den 1 december 1997, den 19 maj och 27 november 1998 samt den 22 april och 30 november 1999.

Under hösten 1999 utarbetades inom Näringsdepartementet, i nära samarbete med Justitiedepartementet, departementspromemorian Elektroniska signaturer (Ds 1999:73). Promemorian föregicks av samråd med berörda departement i övriga nordiska länder, då tolkningen och genomförandet av direktivet diskuterades. Promemorians lagförslag bifogas som *bilaga 2*.

Promemorian har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 3*. Remissyttrandena och en sammanställning av dessa finns tillgängliga i Näringsdepartementet (dnr N1999/12677/ITFoU). Av sammanställningen framgår att flertalet remissinstanser i huvudsak tillstyrker den i promemorian föreslagna lagen.

De nordiska överläggningarna har fortsatt även efter remissbehandlingen.

Den s.k. IT-utredningen överlämnade i mars 1996 betänkandet Elektronisk dokumenthantering (SOU 1996:40). Där föreslogs bl.a. en ändring i sekretesslagen med anledning av användningen av elektroniska signaturer (se avsnitt 9). Betänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 4*. Remissyttrandena och en sammanställning av dessa finns tillgängliga i Justitiedepartementet (dnr Ju1996/1260/L6). Av sammanställningen framgår att remissinstanserna i denna del tillstyrker förslaget eller i allt väsentligt lämnar det utan erinran.

Lagrådet

Regeringen beslutade den 30 mars 2000 att inhämta Lagrådets yttrande över de förslag som finns i *bilaga 5*.

Lagrådet har i huvudsak godtagit förslagen, men föreslagit vissa justeringar. Regeringen har i allt väsentligt följt Lagrådets förslag, vilket bl.a. har medfört en omnumrering av 3–20 §§. Dessutom har vissa redaktionella ändringar gjorts i lagtexten. Lagrådets synpunkter behandlas i avsnitt 6.1, 6.11–6.12, 9 och 10 samt i författningskommentarerna under respektive lagrum. Lagrådets yttrande finns i *bilaga 6*.

4 Bakgrund och utgångspunkter

4.1 Varför behövs elektroniska signaturer?

En elektronisk signatur kan användas för att säkerställa att elektroniskt överförd information inte har förändrats, för att identifiera informationens avsändare och för att förhindra avsändaren att förneka att han eller hon sänt informationen.

Långt innan informationstekniken (IT) började förändra vårt sätt att hantera och kommunicera information har den personliga namnteckningen varit en väsentlig del av den ekonomiska och juridiska verkligheten. Namnteckningar eller signaturer tillgodoser flera olika behov vid skriftlig informationshantering.

En signatur kan ge uttryck för en vilja att handla på ett visst sätt. Närmast avser undertecknaren att acceptera innehållet i den text som är placerad före namnteckningen. Nära knuten till denna viljefunktion är den varningsfunktion som är förbunden med namnteckningen. Ett krav på underskrift klargör på ett tydligt sätt att en bindande förpliktelse kan vara för handen.

Genom att skriva en namnteckning på en handling som innehåller en text, knyts texten på visst sätt till namnteckningen och därmed till den person som utpekas av namnteckningen. Namnteckningen kan sålunda användas för att identifiera den person som skall knytas till texten. Det faktum att både texten och namnteckningen fästs på papperet medför ett visst skydd mot manipulation och talar för att handlingen är äkta.

Identifieringsfunktionen och äkthetsfunktionen kan användas i situationer där behov av bevisning uppkommer, t.ex. för att i efterhand styrka rättshandlingar. Att förse en pappershandling med en namnteckning kan sägas vara ett sätt att säkra eventuellt framtida behov av att kunna bevisa såväl identiteten på som avsikten hos den som undertecknat en handling. Uttryckt på ett annat sätt kan namnteckningen sägas ha en funktion som hinder för undertecknaren att med framgång hävda att han eller hon inte står bakom en handling (s.k. oavvislighet). Den omständigheten att en person är ”närvarande” i ett IT-system innebär oftast bara att denne via någon form av förbindelse är i direkt kontakt med det tekniska systemet. Det finns därför ofta ett behov av att kunna verifiera användarens identitet. Det behövs för att man skall kunna styra behörighet att ta del av information som inte skall vara allmän. I vissa fall behövs det för att styra någon mer materiell funktion, som t.ex. att få tillgång till sedlar i en uttagsautomat. Identitetsverifieringen används också för att i efterhand kunna spåra vad någon gjort i ett elektroniskt system. Den metod som

helt dominerat för att kontrollera identiteten av användare i datorsystem är att använda ett lösenord, ibland reducerat till en fyrsiffrig säkerhetskod. En elektronisk signatur kan utgöra en säkrare metod som kan användas över Internet och andra osäkra förbindelser. Den mest intressanta frågan är emellertid om elektroniska signaturer också kan ges de funktioner vid elektronisk kommunikation som traditionella underskrifter har vid pappersbaserad kommunikation.

4.2 Rätts- och bevisverkan av signaturer

Allmänt

En nyckelfråga är om en elektronisk signatur kan ges samma rättsverkan som en egenhändig namnunderskrift. Det är dock inte alltid klart vad som avses med denna frågeställning. Frågan har vidare olika innebörd beroende på vilken rättsordning man syftar på. Det finns rättsordningar där den traditionella namnteckningen har en rättslig betydelse i större utsträckning och på ett annat sätt än i svensk rätt. I Sverige finns det i varje fall inom civilrätten förhållandevis få regler som innebär att underskriften är en förutsättning för att vissa rättsverkningar skall inträda. Däremot kan underskriften ofta ha betydelse som bevis för ett visst påstått förhållande, dvs. bevisverkan.

Rättsverkan

När det gäller affärssituationer som avtal om köp av varor och tjänster samt om hyra m.m. finns endast ett mycket begränsat antal situationer där svensk lagstiftning kräver avtal i skriftlig form med underskrifter av parterna. Som exempel kan nämnas fastighetsköp och krediter till konsumenter. Ett avtal om köp av fast egendom skall enligt 4 kap. 1 § jordabalken alltid upprättas skriftligen och undertecknas av köparen och säljaren. Ett avtal som gäller kredit till konsument skall enligt 9 § konsumentkreditlagen (1992:830) ingås skriftligen och undertecknas av konsumenten. Frånvaron av underskrifter kan ha olika konsekvenser i olika fall. I fallet med fastighetsförvärv är avtalet ogiltigt om underskrift saknas. I fallet med konsumentkrediter är avtalet ändå giltigt, utom i fråga om villkor som är till nackdel för konsumenten. På familjerättens område finns det också ett antal situationer där det krävs underskrifter. Det gäller exempelvis testamente och äktenskapsförord, som inte är giltiga utan underskrifter. På förvaltningsrättens område finns det ett tämligen stort antal regler om att ansökningar m.m. till myndigheter skall göras skriftligen och undertecknas av exempelvis den sökande.

I det vardagliga privat- och affärslivet finns det dock väldigt få lagregler om att underskrifter måste användas. Användningen av underskrifter eller namnteckningar har i stället under lång tid utvecklats som ett slags vardagens praxis. Undertecknandet har blivit en etablerad metod för bekräftelse, kontroll och bevisning kring våra göranden och låtanden i allmänhet. Detta är alltså något som i princip utvecklats utan lagstiftning. Av någon betydelse i sammanhanget kan kanske vara existensen av

brottet ”förnekande av underskrift”. Enligt 15 kap. 13 § brottsbalken kan nämligen den som förnekar sin underskrift på en urkund dömas till böter eller fängelse i högst sex månader, förutsatt att åtgärden innebär fara i bevishänseende. Om brottet är grovt är straffet fängelse i högst två år.

Oavsett hur de lagregler som finns rörande underskrifter skall uppfattas i samband med elektronisk kommunikation, är det knappast främst lagstiftning som står i vägen för att elektroniska signaturer skall få samma betydelse som egenhändiga namnunderskrifter. Det viktigaste torde i stället vara att det utvecklas säkra och lättanvända tekniska lösningar för elektroniska signaturer så att människor känner tillit till dem och tycker att de är praktiska att använda.

När det gäller de formkrav som ändå finns på underskrift i olika författningar är den avgörande frågan om syftena bakom dessa krav lika väl kan uppfyllas med elektroniska signaturer. I detta sammanhang kan det vara intressant att erinra om det betraktelsesätt som kan uttolkas ur UNCITRAL:s[1] modellag om elektronisk handel[2], kallat ”funktionell ekvivalens”. Detta betraktelsesätt innebär att man, när man ställs inför frågan om ett nytt kommunikationssätt bör omfattas av det gamla regelverket, skall ta fasta på de bakomliggande syftena med regeln. Sedan får man analysera om dessa syften kan tillgodoses också i den elektroniska miljön. Det elektroniska kommunikationssättet skall inte förnekas rättslig betydelse enbart på den grunden att det sker i elektronisk form.

De formkrav på underskrifter som finns i svenska författningar kan ha många syften. Ett syfte kan vara att säkra bevisning om att en åtgärd vidtagits, om vem som vidtagit den och om dess innehåll. Därvid kan ett viktigt syfte vara att det på ett smidigt sätt skall gå att arkivera och bevara informationen under mycket lång tid. Ett annat syfte kan vara att det för statsmakterna kan underlätta vissa förfaranden, exempelvis beskattning. Ett betydelsefullt syfte är vidare ofta att formkrav kan ha en varnings-funktion, dvs. mana till och ge tid för eftertanke innan man vidtar en betydelsefull rättshandling eller annan åtgärd. Dessa formkrav infördes innan det var aktuellt med elektroniska rutiner och signaturer eller kan antas ha tillkommit utan att informationstekniken har beaktats.

Frågan är då hur krav på underskrift eller liknande uttrycksätt bör förstås vid elektronisk hantering. Denna fråga har behandlats bl.a. i betänkandet Elektronisk dokumenthantering (SOU 1996:40, s. 93 ff). I betänkandet anförs att ordet ”skriftlig”, i anknytning till förfaranderegler, huvudsakligen synes användas för att utesluta muntliga rutiner och utesluter därmed inte användning av elektroniska rutiner. I betänkandet konstateras emellertid att när det krävs att en handling skall vara ”undertecknad” innefattas inte elektroniska rutiner. Här hänvisar utredaren bl.a. till att telefaxmeddelanden i praxis inte ansetts uppfylla rättegångsbalkens krav på att handlingen skall vara egenhändigt undertecknad genom att det i kravet på egenhändigt undertecknande också har ansetts ligga ett krav på att det just är det undertecknade exemplaret som skall ges in till domstolen.

[1] United Nations Commission on International Trade Law.
[2] ”Model Law on Electronic Commerce”, antagen 1996.

Ett åtminstone delvis annorlunda synsätt förefaller finnas hos Christina Hultmark (se exempelvis Elektronisk handel och avtal, 1998, s. 65 ff). Med utgångspunkt från en analys av syftena bakom olika formkravsregler menar hon att ett krav på underskrift i en författning i allmänhet inte behöver betyda att det krävs en egenhändigt skriven namnunderskrift, utan att det skulle gå lika bra med en elektronisk signatur. Resonemanget bygger på principen om funktionell ekvivalens som kan härledas från UNCITRAL:s modellag om elektronisk handel (se ovan).

Även om man anlägger ett sådant betraktelsesätt som kan uttolkas ur UNCITRAL:s modellag är det i dag inte realistiskt att tänka sig att svenska domstolar och myndigheter skulle tolka alla formkrav på underskrift eller liknande i författningar så att de även skulle kunna uppfyllas genom elektroniska signaturer. I sammanhanget är det dock intressant att påpeka att när det gäller formkrav som kräver skriftlighet har myndigheter och domstolar på vissa områden godtagit att dessa krav kan uppfyllas med elektroniska rutiner, exempelvis telefax.

Elektroniska signaturers likställighet med traditionella egenhändiga namnunderskrifter är en komplicerad fråga. Det är viktigt att komma ihåg att de är olika till sin natur och utförs på olika sätt. Den elektroniska signaturen bygger ofta på ett komplicerat tekniskt krypteringsförfarande, och en och samma signatur kan oftast användas av alla personer som har tillgång till de nödvändiga koderna och signeringsutrustningen. Det är alltså i och för sig möjligt för den som är innehavare av de nödvändiga koderna eller nycklarna, att lämna dem till andra personer och låta dessa göra signaturer med hjälp av nycklarna. Eftersom en elektronisk signatur är resultatet av en beräkning som görs dels med stöd av de nödvändiga nycklarna, dels med stöd av innehållet i den handling som skall signeras, har dock en elektronisk signatur inget värde fristående från den handling till vilken den är knuten. En elektronisk signatur är följaktligen direkt kopplad till den informationsmängd som signerats och inte fristående på samma sätt som en namnteckning. Vidare präglas tekniken med elektroniska signaturer av en hög grad av säkerhet. Förfalskningar avseende härkomst och innehåll är betydligt svårare att åstadkomma än när det gäller pappershandlingar med namnunderskrifter. En namnunderskrift är visserligen knuten till en viss persons sätt att skriva och kan inte överlämnas till andra, men vissa personer kan vara mycket skickliga på att efterbilda andras underskrifter. Elektroniska signaturer av tillräckligt hög kvalitet torde därför ha en minst lika god säkerhet som traditionella underskrifter.

Bevisverkan

Även i de fall en underskrift inte utgör ett formellt krav tillmäts den ibland mycket stor betydelse i bevishänseende. En namnunderskrift på en handling kan användas som bevis för att en viss person skrivit under den och att denna person godtagit de villkor som står i exempelvis ett skriftligt kontrakt.

Svensk rättsskipning bygger på principen om fri bevisprövning. Det betyder egentligen två saker. Det ena är att det inte finns någon begränsning när det gäller vilka kunskapskällor man får använda som

bevis i en rättegång. Principen innebär dessutom att när en domare skall bedöma och värdera bevisningen är denne obunden av lagregler. Det finns alltså ingen begränsning i svensk rätt om att åberopa eller beakta elektroniska signaturer eller andra IT-tillämpningar som bevisning.

Vad som däremot ibland finns i både lagstiftning och praxis är bevisbörderegler. I det här sammanhanget är det särskilt intressant att se om det finns några bevisbörderegler när någon förnekar en namnunderskrift och påstår att den är förfalskad. Det har inte ansetts nödvändigt att lagstifta om detta, men det finns avgöranden där Högsta domstolen har uttalat sig i frågan. Rättsfallet NJA 1976 s. 667 gällde ett fall där en person förnekade att det var han som undertecknat en skuldförbindelse. Högsta domstolen uttalade att om någon gör en sådan invändning får den påstådde fordringsägaren visa att handlingen är äkta. Om en gäldenär däremot gör gällande att handlingen visserligen är äkta men att texten ändrats, s.k. innehållsförfalskning, anses dock allmänt att gäldenären i princip har bevisbördan. Högsta domstolen har även prövat frågan vad som skall gälla när det gäller påstådda förfalskningar av inköpsnotor i samband med användande av kontokort (NJA 1992 s. 263). I detta rättsfall ansåg Högsta domstolen det ligga på kontohavaren att åtminstone göra antagligt att det förelåg en förfalskning. Om detta krav uppfylls krävs enligt Högsta domstolen att kontokortsföretaget visar att inköpsnotan är äkta.

Frågan om bevisverkan av elektroniska signaturer behandlades i departementspromemorian Digitala signaturer – en teknisk och juridisk översikt (Ds 1998:14). Där gjordes bedömningen att det aldrig kan komma i fråga att rubba den fria bevisprövningen. Man ansåg vidare att det inte heller skulle vara ändamålsenligt att uppställa vissa generella bevisbörderegler för elektroniska signaturer. Så gott som samtliga remissinstanser delade denna bedömning.

Det vore onekligen en farlig väg att ge generella bevisbörderegler när det gäller elektroniska signaturer. Bevisbördan bör inte placeras uteslutande med ledning av vilket medium som kommit till användning. Det avgörande måste naturligtvis vara bl.a. vad det är för typ av uppgifter som bekräftats genom den elektroniska signaturen, vad det rör för typ av rättshandling och vad det är för förhållande som skall bevisas. Parternas inbördes förhållande kan också ha betydelse.

4.3 Tekniska grunder

Tekniken kring elektronisk dokumenthantering och signering är relativt ny och den juridiska diskussionen kring denna har därför inte pågått i särskilt många år. Det är därför inte förvånande att terminologin fortfarande utvecklas och kan framstå som något förvirrande. Det beror också på att samma eller snarare liknande begrepp används på flera olika sätt. Tekniker har ofta andra utgångspunkter än jurister. Marknadsförare kan också ha ett annat språkbruk som kanske inte alltid är så lämpligt i juridiska sammanhang. Till detta kommer att utvecklingen i hög grad är internationell och det är svårt att hitta bra svenska termer på begrepp som länge endast haft engelska namn och förkortningar.

Termen ”digital signatur” har bl.a. i EG-direktivet fått ge vika för termen ”elektronisk signatur”. Vad gäller relevansen av ordet ”elektronisk” kan följande sägas. En signatur är som regel inte intressant isolerad, utan bara när den används för att säkra andra uppgifter av något slag. Det blir i hög grad karaktären av dessa som också avgör vilka egenskaper en signatur har. Idag lagras och behandlas uppgifter eller data i hög grad i elektroniska system, varför sådana data ofta kallas för ”elektroniska data”. Motsvarigheten till den handskrivna underskriften kan kallas en ”elektronisk signatur”, också för att markera att ett elektroniskt system har använts för att skapa en sådan signatur.

Det är dock viktigt att i ett rättsligt begreppssystem kunna skilja på metoder som används i framställningen av uppgifter inklusive signaturer och de uppgifter man faktiskt har att ta ställning till. Det faktum att en elektronisk ordbehandling idag nästan alltid föregått framställningen av en traditionell pappershandling saknar betydelse för bedömningen av handlingen i fråga. Det kan däremot vara väsentligt att man måste använda sig av ett tekniskt elektroniskt hjälpmedel för att uppfatta och bedöma uppgifterna eller signaturerna.

De ”elektroniska” signaturer som finns i dag är uteslutande ”digitala” signaturer. Dagens informationsteknik är inriktad på digital representation av information där det centrala skyddsobjektet är ett informationsinnehåll som representeras av ettor och nollor. Under hanteringens gång och när information kommuniceras byter denna representation många gånger fysisk form. Den digitala datamängden kan finnas som högst tillfälliga elektriska strömmar, som mer permanenta magnetfält på en hårddisk eller som små fördjupningar på en CD.

En väsentlig egenskap som skiljer den digitala handlingen från andra data är att den är helt entydig med sin digitala informationsrepresentation. Endast vissa bestämda värden tillåts, som representeras av siffror, eller i praktiken ettor och nollor. Det finns inga gråskalor. Det är denna egenskap som gör att man i digitala system exakt kan kopiera en datamängd så att kopian är identisk med ursprungsmängden. Analog kopiering blir aldrig på samma sätt identisk. Det går inte att på traditionellt sätt skilja ett originalexemplar från en kopia när data förs över från en databärare till en annan eftersom informationen endast förekommer som ett originalinnehåll. Denna egenskap gäller givetvis signaturer lika väl som andra elektroniska data.

Vid den följande kortfattade genomgången av de tekniska grunderna redogörs för signering av information i digital form. Genomgående används emellertid termen ”elektronisk signatur”, som numera får anses vara den vedertagna beteckningen. För en mer utförlig beskrivning hänvisas till departementspromemorian Digitala signaturer – en teknisk och juridisk översikt (Ds 1998:14).

4.3.1 Kryptografisk teknik med hemliga och öppna nycklar

Den teknik som idag allmänt används för att skapa elektroniska signaturer utnyttjar kryptografiska principer för att med en matematisk funktion generera en signatur från de data i digital form som ingår i den

elektroniska handling som skall signeras och någon form av unik nyckel som hör ihop med den som signerar (undertecknaren).

Elektroniska signaturer säkerställer att förändring av ett meddelande kan upptäckas och verifierar vem som signerat det. Kryptografiska metoder kan även användas för att dölja ett meddelandes informationsinnehåll. Detta användningsområde behandlas emellertid inte här.

Signering

Signering av datamängden, som kan representera text, bild, ljud eller information i någon annan form, börjar med att datamängden förbehandlas med en s.k. hashfunktion. Av datamängden skapas därigenom ett s.k. hashvärde som kan liknas vid ett kondensat eller ”fingeravtryck” av datamängden. Hashvärdet är unikt i den meningen att sannolikheten för att två datamängder som inte är identiska skulle ge identiska hashvärden i praktiken är försumbar. Hashvärdet är också icke omvändbart, vilket betyder att datamängden inte kan beräknas utifrån hashvärdet.

Nästa steg i signeringen sker genom kryptering. Kryptering innebär att en datamängd omvandlas genom en bestämd metod, en algoritm. Vid krypteringen används förutom datamängden vissa andra ingångsvärden som fungerar som nycklar vid krypteringen.

Vid signering används i allmänhet s.k. asymmetrisk kryptering med användande av ett nyckelpar. En nyckel är ett mycket stort tal, idag oftast 1 024 bitar motsvarande cirka 300 siffror. Den ena delen av nyckelparet kallas ”hemlig nyckel” och används av undertecknaren för att skapa signaturer. Den måste skyddas mot obehörig åtkomst, vilket diskuteras närmare nedan (se avsnitt 4.3.5). Den andra delen av nyckelparet kallas ”öppen nyckel” och kan användas för att verifiera signaturer, men inte för att skapa dem. Denna nyckel kan spridas öppet till alla som har anledning att verifiera en persons elektroniska signatur, eftersom den inte kan missbrukas för att skapa signaturen och därmed inte behöver distribueras med sekretesskydd. Krypteringen sker genom att hashvärdet (kondensatet av datamängden) bearbetas med hjälp av en algoritm som tar den hemliga nyckeln som ett ingångsvärde. Resultatet av denna beräkning är den elektroniska signaturen.

Signeringen avslutas med att signaturen, bestående av det krypterade hashvärdet, tillförs den signerade handlingen. Handlingen med signatur kan nu sändas öppet till mottagaren.

Viktiga funktioner hos asymmetrisk kryptering är dels att ett krypterat meddelande inte kan dekrypteras med samma nyckel i nyckelparet, dels att det trots kunskap om den ena nyckeln i nyckelparet är omöjligt att beräkna den andra nyckeln. De två nycklarna är därmed beroende av varandra och bildar ett unikt par. Den asymmetriska krypteringen binder innehavaren av den hemliga nyckeln till hashvärdet och därmed till den signerade handlingen.

En elektronisk signatur verifieras på följande sätt. Mottagaren separerar meddelandet och den medföljande signaturen. Samma hashfunktion som avsändaren använde vid sin signering används för att bearbeta det mottagna meddelandet, varvid man får ett hashvärde. Signaturen, i form av ett krypterat hashvärde, dekrypteras av mottagaren med upphovsmannens öppna nyckel och ett okrypterat hashvärde erhålls. Mottagaren jämför dessa två hashvärden. Om de är identiska vet mottagaren att meddelandet inte är förändrat samt att det verkligen härrör från innehavaren av det unika nyckelpar som innehåller den använda öppna nyckeln. Han kan vara säker på detta eftersom det bara är avsändarens hemliga nyckel som kan ha krypterat hashvärdet och det endast är ett identiskt meddelande som kan skapa ett identiskt hashvärde.

En central fråga med dessa tekniker är hur den som skall verifiera en signatur skall kunna vara säker på att en bestämd öppen nyckel verkligen hör ihop med den person som framstår som utställare av en elektronisk handling. Man kan tänka sig olika metoder för säker teknik och administrativa funktioner, men de som helt kommit att dominera bygger på en användning av s.k. *certifikat* (se vidare nedan under avsnitt 4.3.3).

4.3.2 Utrustning för att signera elektroniskt

När en elektronisk handling skall signeras behöver undertecknaren någon form av elektronisk utrustning som kan

- presentera den information som skall signeras på ett begripligt sätt så att undertecknaren vet vad som signeras,
- lagra och använda den hemliga signeringsnyckel som skall användas,
- skapa en medveten beslutspunkt för undertecknaren att faktiskt signera, och
- utföra den beräkning som krävs av hashfunktionen på de digitala data som skall signeras och den kryptoberäkning som behövs för att skapa den elektroniska signaturen.

4.3.3 Certifikat

Ett certifikat för en öppen nyckel är i sig en elektroniskt signerad handling där en betrodd part intygar att en viss öppen nyckel hör ihop med en viss person. Mottagaren kan vända sig till den som utfärdat certifikatet för att få veta vem som innehar den öppna nyckeln, om certifikatet – och därmed signaturen – är giltigt, om giltighetstiden löpt ut eller om certifikatet är spärrat. Mottagaren kan också få reda på om det finns begränsningar för vad certifikatet kan användas till.

Certifikaten kan spridas på olika sätt, t.ex. genom elektroniska katalogtjänster. Det är också vanligt att den som signerar en elektronisk handling inkluderar ett certifikat med sin öppna nyckel, som skall kunna kontrolleras av mottagaren. Sådana certifikat, eller nyckelcertifikat, brukar följa en internationell standard kallad X.509, som anger vilka uppgifter som måste eller kan förekomma och hur dessa skall vara

anordnade. Själva certifikatet är en signerad mängd data där den som utfärdat certifikatet tar ansvar för innehållet.

4.3.4 Infrastruktur för öppna nycklar

För att man på ett säkert och ekonomiskt rimligt sätt skall kunna använda elektroniska signaturer (och andra tjänster som utnyttjar öppna nycklar) i samhället mellan större grupper, enskilda, företag och myndigheter behövs det en infrastruktur som på engelska ofta kallas public key infrastructure (PKI), men som på svenska kan benämnas ”det öppna nyckelsystemet”. Det finns ingen klar definition av vad begreppet omfattar, men följande kan nämnas.

- Utfärdande av certifikat är centralt.
- Distribution av certifikat kan i och för sig ske med hjälp av en öppen katalogtjänst. Vid kryptering för konfidentialitet och för identifiering av användare kan det ofta vara en nödvändig lösning, men för elektroniska signaturtjänster behövs inte katalogen. I samband med utfärdandet kan nämligen nyckelinnehavaren/undertecknaren få sitt certifikat i någon form (t.ex. på ett elektroniskt ID-kort eller via e-post) och den som signerar kan själv bifoga certifikatet till den signerade handlingen.
- Innehavaren av certifikatet och eventuellt andra parter skall kunna begära hos den som utfärdat certifikatet att det skall spärras, t.ex. beroende på att den hemliga nyckeln som motsvarar certifikatets öppna nyckel befaras ha kommit på avvägar. Det kan t.ex. vara fråga om ett borttappat eller stulet elektroniskt ID-kort.
- Tillhandahållande av information om certifikatens aktuella status via spärrlistor eller statuskontroll ”on-line” av certifikat är en nödvändig funktion för att man skall kunna ha tilltro till en elektronisk signatur.
- En definition av ett certifikatformat som kan förstås av de samverkande parterna måste finnas. Detta kan synas trivialt men möjliggör att man faktiskt kan kommunicera och t.ex. verifiera signaturer.

4.3.5 Vissa säkerhetsfrågor för system med elektroniska signaturer

Förmedlingen av information från dataform till en för avsändaren/mottagaren uppfattbar form

Det är viktigt att klargöra gränserna mellan de digitala data som finns i ett elektroniskt informationssystem som t.ex. en vanlig persondator och den information som en människa slutligen tolkar utifrån dessa data. Vare sig dessa data skapar en text, en figur på en bildskärm, skrivs ut på papper eller kommunicerar talat språk via en högtalare, så tolkas primära data till en annan form, vilken mer eller mindre exakt uppfattas av mottagaren. I allmänhet har man nöjt sig med att försöka skydda den digitala handlingen med hjälp av signaturtekniker utan att ta hänsyn till den process som så småningom skall göra dessa data begripliga för en människa.

Denna skillnad gäller inte bara för den tänkte mottagaren av den elektroniska handlingen utan kan även gälla för den som är upphovsman till informationen. I de moderna informationssystemen är det oftast svårt att vara helt övertygad om att den information som skrivs in och som kan iakttas före elektronisk signering också är korrekt representerad av den datamängd som blir signerad i en komplicerad matematisk process vars närmare detaljer inte kan iakttas eller kontrolleras direkt.

Skyddet för den hemliga nyckeln

Den mest centrala frågan att ta ställning till när det gäller utrustning för elektroniska signaturer, gäller skyddet av den hemliga nyckeln. Man brukar här tala om ”hårda” respektive ”mjuka” lösningar. Med hårda lösningar menar man då en speciell utrustning som tillverkats enligt mycket strikta metoder och som innehåller ett skyddande fysiskt skal mot olika former av attacker. Aktiva (”smarta”) kort är den mest använda formen. För en närmare diskussion om fördelar med att använda aktiva kort för elektroniska signaturer hänvisas till departementspromemorian Digitala signaturer – en teknisk och juridisk översikt (Ds 1998:14), kapitel 3 och 5 samt bilaga 2.

Lösningar där man i stället med vanlig datorutrustning och speciell programvara försöker skydda en hemlig nyckel (med t.ex. kryptering) kallas på motsvarande sätt mjuka och är ofta billigare och enklare att införa, men säkerheten är mer svårbedömbar.

I många elektroniska signatursystem har man någon form av metod för att försöka verifiera att den behöriga innehavaren av signeringsnyckeln verkligen är närvarande. Den idag helt dominerande metoden är att ett lösenord erfordras. Med aktiva kort, mobiltelefoner eller andra mindre, handburna enheter har detta lösenord i allmänhet reducerats till ett antal tecken (t.ex. fyra siffror).

Denna typ av verifiering, som inte ensam duger till att unikt identifiera en person, kan dock i många fall tillsammans med övriga skyddsåtgärder anses vara tillräcklig för detta syfte. Man bör betona att i system med sådana handburna signeringsverktyg som aktiva kort, så är det det fysiska innehavet som är den väsentligaste skyddsfaktorn. En annan metod för att öka säkerheten som diskuterats en hel del som ersättning för en säkerhetskod, men sällan prövats i samband med signeringssystem, är att använda någon form av biometrisk mätutrustning. En sådan utrustning kan t.ex. känna igen den behöriga innehavarens tumavtryck.

Den pragmatiska lösning som i allmänhet tillämpas är att använda olika skyddsåtgärder, inte minst vanliga fysiska lås, som skall säkerställa att den persondator och den programvara som används är rimligt säkra.

Det är också viktigt att uppmärksamma skyddet av övrig signeringsutrustning. I begreppet utrustning måste man här inkludera all den programvara som används för den aktuella tillämpningen.

Standarder och standardiseringsarbete har ökat i betydelse för stora delar av samhället. En stor mängd varor och tjänster är utformade enligt internationell eller nationell standard. Tack vare olika standarder passar t.ex. glödlampan i sockeln, filmen i kameran, skruven i muttern osv.

Ett system med i princip frivilliga överenskommelser mellan olika intressenter om vilka standarder som skall tillämpas har vuxit fram. Ursprungligen togs standarder fram av näringslivet, huvudsakligen för att sänka tillverkningskostnaderna. Så småningom stod det dock klart att standardisering och tillverkarens egenkontroll inte var tillräckligt för att garantera säkerheten och den tekniska kvaliteten hos olika tillverkares produkter. Därför skapades olika, frivilliga certifieringssystem. Med certifiering (av överensstämmelse) menas en handling utförd av en tredje part, som visar att tillräcklig tilltro uppnåtts om att en vederbörligen identifierad produkt, process eller tjänst är i överensstämmelse med en bestämd standard eller med ett annat regelgivande dokument.

Standarder utnyttjas för att harmonisera tekniska regler som har betydelse för skydd av liv, hälsa och miljö och är således en angelägenhet även för myndigheter och andra offentliga organ. Standardisering har numera en mycket stor betydelse för den fria rörligheten för varor och tjänster över nationella gränser.

Internationella standardiseringsorganisationen (ISO) är en världsomfattande sammanslutning av nationella standardiseringsorgan. Tillsammans med International Electrotechnical Commission (IEC), som täcker standardisering inom det elektrotekniska området, utgör ISO världens största icke-statliga system för frivilligt industriellt och tekniskt samarbete på internationell nivå. Resultatet av ISO:s arbete utgörs av ISO-standarder eller riktlinjer. Internet Engineering Task Force (IETF) är dock den internationella organisation som ligger bakom i stort sett alla idag förekommande standarder som rör elektroniska signaturer.

Centralorgan för standardisering i Sverige är Standardiseringen i Sverige (SIS), som har till uppgift bl.a. att främja och fastställa svensk standard. SIS är en fristående ideell förening, vars stadgar är fastställda av staten. All fastställd svensk standard har prefixet SS. Om det rör sig om en svensk standard som överför global standard utan ändringar blir prefixet t.ex. SS-ISO. Överförd europeisk standard betecknas SS-EN.

SIS och dess auktoriserade standardiseringsorgan inom olika fackområden deltar aktivt i utarbetandet av internationella standarder, dels inom ISO och IEC, dels i de europeiska standardiseringsorganen Comité Européen de Normalisation (CEN), Comité Européen de Normalisation Electrotechnique (CENELEC) och European Telecommunications Standards Institute (ETSI).

Det bör dock poängteras att standarder inom IT-området, där utvecklingen är mycket snabb, i praktiken oftare sätts av de dominerande leverantörerna och av andra organisationer än av de ovan beskrivna standardiseringsorganen.

EG-kommissionen presenterade 1985 en vitbok med ett program för förverkligande av den inre marknaden, innefattande bl.a. fri rörlighet för varor. Programmet resulterade senare i den reformering av Romfördraget

som skedde genom Europeiska enhetsakten. En ny metod för harmonisering av medlemsstaternas lagstiftning om produkter (”the New Approach”) anvisades. Enligt denna skall direktiven endast fastställa de väsentliga säkerhetskrav som produkterna skall uppfylla med hänsyn till skydd för liv, hälsa eller miljö m.m. Det överlåts sedan till de europeiska standardiseringsorganen att utarbeta harmoniserade frivilliga standarder med närmare tekniska specifikationer för produkten. En produkt som tillverkas i enlighet med dessa standarder skall förutsättas uppfylla de väsentliga kraven i direktivet. Tillverkarens egenkontroll i kombination med en försäkran från tillverkaren om att tillämpliga standarder har följts skall normalt vara en tillräcklig kontrollåtgärd.

Produkter som kan medföra stor risk för hälsa och säkerhet skall dock i normalfallet kontrolleras av ett tredjepartsorgan. Detsamma gäller när en tillverkare inte har tillämpat harmoniserade standarder eller då sådana saknas. Det skall räcka med att en sådan kontroll sker i ett land för att få tillträde till hela den inre marknaden.

Efter förslag i vitboken antog EG också en resolution om en helhetssyn för provning och certifiering[3]. I denna anges riktlinjer för hur EG:s system för bestyrkande av överensstämmelse skall utformas. Som ett komplement till den nya metoden föreskrivs hur ömsesidiga erkännanden av provningar och certifieringar mellan medlemsstaterna skall komma till stånd samt gemensamma villkor och regler för laboratorier och för certifierings- och kontrollorgan.

De tredjepartsorgan som får utföra en sådan bedömning som omtalats ovan skall anmälas till Europeiska gemenskapernas kommission. Organen kallas därför anmälda organ. Dessa kan vara både offentliga och privaträttsliga organ som av medlemsstaten bedömts ha tillräcklig kompetens för uppgiften. Det anmälda organet utför bedömningen på uppdragsbasis och får normalt självt bestämma avgiften för detta.

För att skapa förtroende för provningar och bevis om överensstämmelse, oavsett i vilket land de utförts, har de europeiska standardiseringsorganen, på EG:s vägnar, utarbetat enhetliga standarder för kompetensen hos provnings-, certifierings- och kontrollorgan. Dessa återges i den europeiska standardserien EN 45 000.

Att kraven är uppfyllda kan visas genom s.k. ackreditering. Med ackreditering menas ett formellt erkännande av att ett organ (t.ex. ett laboratorium, ett certifieringsorgan eller ett besiktningsorgan) är kompetent att utföra specificerade uppgifter, såsom provningar, kalibreringar, mätningar eller certifieringar. I Sverige har Styrelsen för teknisk kontroll (SWEDAC) i uppgift att svara för bedömning av kompetensen hos laboratorier, certifieringsorgan och kontrollorgan.

Liksom SIS deltar i det internationella standardiseringsarbetet är SWEDAC engagerat i uppbyggnaden av de europeiska systemen för ömsesidigt godtagande av provning och kontroll samt i utformandet av enhetliga regler för bedömning av kompetens hos de organ som utför teknisk kontroll. Detta sker främst inom ramen för organisationen

[3] Resolutionen den 21 december 1989 om en helhetssyn på bedömning av överensstämmelse (EGT C 10, 16.1.1990, s. 1). Se även beslutet den 13 december 1990 om moduler för olika stadier i förfaranden vid bedömning av överensstämmelse, avsedda att användas i tekniska harmoniseringsdirektiv (EGT L 380, 31.12.1990, s. 13).

European Accreditation (EA). Inom EA finns multilaterala avtal om ömsesidigt erkännande av ackrediteringssystem och om erkännande av kompetens och därigenom av certifikat och system.

I Sverige har det beskrivna öppna systemet med anmälda organ genomförts genom lagen (1992:1119) och förordningen (1993:1065) om teknisk kontroll. Enligt dessa får både offentliga och enskilda organ som uppfyller kraven på kompetens utföra certifierings-, provnings- och besiktningsuppgifter och konkurrera om uppdragen. SWEDAC har till uppgift att i samråd med berörda sektorsmyndigheter bedöma om de organ som önskar bli anmälda uppfyller kraven. Som huvudregel gäller att organen skall kunna visa att de uppfyller kraven i EN 45 000-serien. Enligt lagen och förordningen om teknisk kontroll gäller dessutom som huvudprincip att kraven även för ackreditering av organ som utför annan kontroll, besiktning och certifiering än de som föreskrivs i EG-direktiven skall baseras på EN 45 000-serien.

Av särskilt intresse i detta sammanhang är den provning och certifiering av produkter som sker frivilligt, utan att det krävs i EG-direktiv eller i nationella föreskrifter – det s.k. frivilliga området. Detta är vanligt och krav på produkter finns ofta formulerade i standarder mot vilka frivillig certifiering kan ske. Det är viktigt att påpeka att certifiering inte bara sker av produkter, utan också av t.ex. kvalitetssystem, ledningssystem, personal, eller av verksamheten i allmänhet.

Det är utan tvivel en fördel om det även inom det frivilliga området tillämpas likartade former för provning och certifiering. I EG:s system för bedömning av överensstämmelse har man också tagit fasta på att tekniken för att bedöma om en produkt överensstämmer med vissa uppställda krav är densamma oavsett om bedömningen sker utifrån tvingande regler eller frivilliga former. I sitt meddelande av den 24 juni 1989 ”En helhetssyn på certifiering och provning” markerade EG-kommissionen att ömsesidiga erkännanden inte bara är av intresse för den reglerade sektorn utan i lika hög grad har betydelse inom det frivilliga området. Även frivillig provning och certifiering kan, om den skiljer sig åt i olika länder, medföra betydande handelshinder. Problemen med att skapa ömsesidiga godtaganden är desamma inom de reglerade och de frivilliga områdena, nämligen att skapa förtroende för att de berörda organen är kompetenta och oberoende.

5 Direktivet om ett gemenskapsramverk för elektroniska signaturer

5.1 Allmänt

Anledningen till att kommissionen lade fram ett förslag till direktiv var bl.a. att den befarade att skilda juridiska och tekniska strategier i medlemsstaterna beträffande elektroniska signaturer skulle utgöra ett allvarligt hinder för den inre marknaden och hindra utvecklingen av nya ekonomiska verksamheter som är kopplade till elektronisk handel. Olika bestämmelser i medlemsstaterna om rättsligt erkännande av elektroniska

signaturer och om auktorisering av dem som tillhandahåller certifikat för elektroniska signaturer skulle skapa betydande sådana hinder.

Syftet med direktivet är att underlätta användningen av elektroniska signaturer och bidra till deras rättsliga erkännande. Avsikten är att fastställa ett rättsligt ramverk för elektroniska signaturer och vissa certifikattjänster för att säkerställa en väl fungerande inre marknad. Direktivet omfattar inte frågor om ingående eller giltighet av avtal om formkrav föreskrivs och påverkar inte heller bestämmelser som reglerar användningen av dokument (*artikel 1*). Regelverket för elektroniska signaturer är avsett att stärka förtroendet för och ge ett allmänt godtagande av den nya tekniken.

I direktivet definieras signaturer som uppfyller vissa specificerade krav som ”avancerade elektroniska signaturer”. Ett intyg i elektronisk form som kopplar ihop en person med uppgifter, såsom koder eller öppna kryptografiska nycklar, som verifierar en signatur samt bekräftar personens identitet kallas som redan nämnts ”certifikat” (se avsnitt 4.3.3). Den tredje part som utfärdar certifikatet och som således går i god för att den uppgivne undertecknaren verkligen är den som påstås kallas ”tillhandahållare av certifikattjänster”. Ett certifikat som innehåller i en bilaga uppräknade uppgifter och som utfärdats av en tillhandahållare av certifikattjänster som uppfyller kraven i en annan bilaga benämns ”kvalificerat certifikat”. Dessa och flera andra definitioner ges i *artikel 2*.

Den metod som används i direktivet är att ge avancerade elektroniska signaturer, som baseras på ett kvalificerat certifikat och som dessutom skapas av en ”säker anordning för skapande av signaturer” (se nedan), en viss rättsverkan. Dessa signaturer skall anses uppfylla kraven på en signatur i förhållande till uppgifter i elektronisk form på samma sätt som en handskriven signatur uppfyller samma krav i förhållande till uppgifter på papper och skall godtas som bevis vid rättsliga förfaranden. Vidare stadgas att andra elektroniska signaturer under vissa förutsättningar inte får förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden (*artikel 5).*

Villkoren för marknadstillträde för tillhandahållare av certifikattjänster och den tillsyn som skall ske regleras i *artikel 3*. Fri rörlighet för certifikattjänster behandlas i *artikel 4* och skadestånd i *artikel 6*. I *artikel 7* regleras behandlingen av certifikat utfärdade i länder utanför gemenskapen, medan *artikel 8* behandlar frågor om dataskydd. I övrigt ges regler om den kommitté för elektroniska signaturer som skall biträda kommissionen (*artikel 9* och *10*), om uppgifter som skall anmälas till kommissionen (*artikel 11*), om en översyn av direktivet tre och ett halvt år efter dess ikraftträdande (*artikel 12*) samt om genomförande och ikraftträdande (*artikel 13–15*).

Vid direktivets utformning var målsättningen att regleringen skulle vara teknikneutral, att certifikattjänster skulle kunna tillhandahållas utan krav på förhandstillstånd samt att elektroniska signaturer skulle få rättslig verkan.

5.2 Tillämpningsområde

Av ingressen till direktivet (punkt 16) framgår att elektroniska signaturer som används endast inom system som grundar sig på frivilliga civilrättsliga avtal mellan ett bestämt antal deltagare (s.k. slutna system) inte faller under direktivets tillämpningsområde. Direktivreglerna avser därför bara tillhandahållare av certifikattjänster som riktar sig ”till allmänheten”. Avtalsparters frihet att sinsemellan komma överens om i vilken mån och på vilka villkor de godkänner elektroniskt signerade uppgifter påverkas alltså inte av direktivet.

Av ingressen till direktivet (punkt 9) och av definitionen av tillhandahållare av certifikattjänster framgår vidare att dessa tillhandahållare inte bör vara begränsade till att endast utfärda och hantera certifikat. Även andra tjänster som har anknytning till elektroniska signaturer bör kunna erbjudas, såsom registrerings-, tidsstämplings-, katalog-, databehandlings- och konsulttjänster. För tillhandahållare av certifikattjänster och för produkter med anknytning till elektroniska signaturer föreskriver direktivet en fri inre marknad, vilket gäller för alla sorters elektroniska signaturer, certifikattjänster och ”signaturprodukter”.

Direktivet omfattar inte frågor som avser ingående eller giltighet av avtal eller andra rättsliga förpliktelser om den nationella lagstiftningen eller gemenskapslagstiftningen föreskriver vissa formkrav. Det påverkar heller inte bestämmelser och begränsningar i nationell lagstiftning eller gemenskapslagstiftning som reglerar användningen av dokument.

5.3 Definitioner

En elektronisk signatur definieras som uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra elektroniska uppgifter och som används som metod för autenticering.

För att en signatur skall få kallas avancerad elektronisk signatur krävs att den är knuten uteslutande till undertecknaren, vilken kan identifieras genom signaturen, att den är skapad med medel som undertecknaren kan behålla uteslutande under sin egen kontroll samt att den är kopplad till de uppgifter den avser på ett sådant sätt att alla efterföljande ändringar av uppgifterna kan upptäckas.

Genom direktivet införs vidare en rad tekniska termer såsom ”uppgifter för skapande av signaturer” och ”uppgifter för signaturverifiering”, som avser unika uppgifter såsom koder eller krypteringsnycklar som används för att skapa respektive verifiera en elektronisk signatur. Program- eller hårdvara för att använda uppgifterna för att skapa en signatur respektive uppgifterna för signaturverifiering benämns ”anordning för skapande av signaturer” respektive ”anordning för signaturverifiering”.

För att få kallas *säker* anordning för skapande av signaturer skall anordningen uppfylla de krav som anges i bilaga III till direktivet. Anordningarna skall enligt denna säkerställa att uppgifterna för att skapa signaturen i praktiken enbart kan förekomma en gång och att sekretessen för uppgifterna är säkerställd inom rimliga gränser. Vidare skall uppgifterna för att skapa signaturen ”med rimlig garanti” inte kunna

härledas och signaturen vara skyddad mot förfalskning ”med den teknik som för närvarande finns tillgänglig”. Ett ytterligare krav är att uppgifterna för att skapa signaturen kan skyddas på ett tillförlitligt sätt, så att andra inte kan komma åt dem. Slutligen stadgas att anordningen inte får förändra de uppgifter som skall signeras eller hindra att dessa uppgifter presenteras för undertecknaren före undertecknandet.

Beträffande signaturverifiering finns en bilaga IV till direktivet, som innehåller rekommendationer för säker signaturverifiering.

Som ”tillhandahållare av certifikattjänster” definieras som nämnts inte endast den som utfärdar certifikat, utan även den som tillhandahåller andra tjänster som har anknytning till elektroniska signaturer.

Kvalificerade certifikat

Kvalificerade certifikat är sådana certifikat som uppfyller kraven i direktivets bilaga I och som utfärdas av en tillhandahållare av certifikattjänster som uppfyller kraven i direktivets bilaga II. Certifikatet skall bl.a. innehålla uppgift om att det har utfärdats som ett kvalificerat certifikat, uppgifterna för signaturverifiering som motsvarar de uppgifter för skapande av signaturer som undertecknaren har kontroll över samt uppgift om certifikatets giltighetstid (se vidare i bilaga I).

Bilaga II innehåller krav på pålitlighet, ett säkert och snabbt system för omedelbart återkallande, identitetskontroll av den till vilken ett certifikat utfärdas, kompetent personal, användandet av pålitliga system och produkter som garanterar teknisk säkerhet, konfidentialitet beträffande uppgifter för skapande av signaturer, m.m. (se vidare i bilaga II).

Certifikatutfärdaren skall dessutom förfoga över tillräckliga ekonomiska medel för att bedriva verksamheten i enlighet med direktivets krav, i synnerhet för att kunna uppfylla eventuell skadeståndsskyldighet. De certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten skall nämligen vara ansvariga för skada, åtminstone i den utsträckning som anges i artikel 6.

Nämnas kan också att utfärdaren enligt bilaga II måste informera den som ansöker om ett certifikat om villkoren, inklusive eventuella begränsningar för certifikatet, förekomsten av ett frivilligt ackrediteringssystem samt förfarande för klagomål och avgörande av tvister. Vidare är utfärdaren förbjuden att lagra eller kopiera uppgifter för skapande av signaturer.

5.4 Marknadstillträde

Medlemsstaterna får inte göra tillhandahållandet av certifikattjänster beroende av förhandstillstånd. Med förhandstillstånd menas enligt ingressen till direktivet inte endast alla tillstånd som kräver ett beslut från de nationella myndigheterna innan tillhandahållaren av certifikattjänster får tillhandahålla dessa tjänster, utan också alla andra åtgärder med samma verkan.

Det står dock medlemsstaterna fritt att införa eller behålla frivilliga ackrediteringssystem som syftar till att höja nivån på tillhandahållandet

av certifikattjänster. ”Frivillig ackreditering” definieras i direktivet som sådana tillstånd i vilka de rättigheter och skyldigheter fastställs som är specifika för tillhandahållandet av certifikattjänster och som på begäran av den berörda tillhandahållaren av certifikattjänster skall utfärdas av de offentliga eller privata institutioner som ansvarar för utarbetandet och övervakningen av dessa rättigheter och skyldigheter. Tillhandahållaren av certifikattjänster får inte utöva rättigheterna enligt tillståndet förrän denne har erhållit beslutet från institutionen.

Medlemsstaterna är skyldiga att införa ett system som gör det möjligt att övervaka de tillhandahållare av certifikattjänster som är etablerade på deras territorium och som utfärdar kvalificerade certifikat till allmänheten. I direktivet ges inga närmare regler för hur denna övervakning skall vara organiserad eller hur sträng den skall vara. I ingressen påpekas att övervakningssystem upprättade inom den privata sektorn inte utesluts.

Vad gäller säkra anordningar för skapande av signaturer föreskriver direktivet att medlemsstaterna skall utse särskilda organ som skall avgöra om anordningarna överensstämmer med bilaga III.

I direktivet ges en möjlighet för medlemsstaterna att förena användningen av elektroniska signaturer inom den offentliga sektorn med högre krav än vad som följer av direktivet.

5.5 Fri rörlighet

Medlemsstaterna får inte begränsa tillhandahållandet av certifikattjänster med ursprung i andra medlemsstater. De skall också säkerställa att det råder fri rörlighet på den inre marknaden för produkter för elektroniska signaturer som överensstämmer med direktivet.

Ett beslut av ett organ i en medlemsstat att en anordning för skapande av signaturer överensstämmer med kraven i bilaga III skall erkännas av samtliga medlemsstater. Kommissionen får fastställa och offentliggöra referensnummer till allmänt erkända standarder för produkter för elektroniska signaturer. Medlemsstaterna skall då utgå från att dessa produkter överensstämmer med kraven i direktivet.

5.6 Rättslig verkan

Det finns två nivåer av rättsligt erkännande av elektroniska signaturer beroende på den tekniska säkerhet som signaturen anses ha. Den rättsliga verkan för avancerade elektroniska signaturer som baseras på ett kvalificerat certifikat och som skapas av en säker anordning för skapande av signaturer har beskrivits i avsnitt 5.1.

För övriga elektroniska signaturer gäller att dessa inte får förvägras rättslig verkan eller giltighet som bevis enbart på grund av att signaturen är i elektronisk form, inte är baserad på ett kvalificerat certifikat eller ett certifikat som utfärdats av en ackrediterad tillhandahållare av certifikattjänster, eller inte är skapad av en säker anordning.

I ingressen anges att direktivet inte påverkar nationella domstolars behörighet att fastslå om det föreligger överensstämmelse med kraven i

direktivet. Det anges även att direktivet inte inverkar på nationella bestämmelser om fri bevisprövning. Frågan om vilken betydelse detta har för tolkningen av direktivets bestämmelser om elektroniska signaturers rättsliga verkan diskuteras vidare i avsnitt 6.11.

5.7 Skadestånd

Direktivet fastställer en undre gräns för skadeståndsskyldighet för tillhandahållare av certifikattjänster som utfärdar kvalificerade certifikat eller som garanterar att andras certifikat är kvalificerade. Medlemsstaterna skall se till att tillhandahållaren är ansvarig för skada som orsakas den som har rimlig anledning att förlita sig på ett certifikat. Tillhandahållaren skall ansvara för skada som uppkommit på grund av att det förelegat felaktigheter eller brister i den information som lämnats i ett kvalificerat certifikat, att den undertecknare som anges i certifikatet vid utfärdandet inte var i besittning av de uppgifter för att skapa en signatur som påstås, att uppgifter för signaturskapande respektive signaturverifiering inte stämmer överens samt att återkallandet av ett certifikat inte registrerats. Tillhandahållaren kan dock undgå skadeståndsskyldighet om han kan visa att han inte har handlat försumligt.

Tillhandahållare av certifikattjänster skall kunna ange begränsningar i ett certifikats tillämpningsområde eller för värdet av de transaktioner som certifikatet får användas för. Tillhandahållaren är då inte ansvarig för skador som härrör från att ett certifikat använts i strid med dessa begränsningar, under förutsättning att begränsningarna varit identifierbara för tredje man.

5.8 Internationella aspekter

Kvalificerade certifikat som utfärdats av en tillhandahållare av certifikattjänster som är etablerad i tredje land (utanför Europeiska ekonomiska samarbetsområdet) skall enligt direktivet i tre situationer betraktas som rättsligt likvärdiga med kvalificerade certifikat utfärdade inom unionen, nämligen

- då tillhandahållaren i tredje land uppfyller kraven i direktivet och är ackrediterad i en medlemsstat,
- då en tillhandahållare inom gemenskapen som utfärdar kvalificerade certifikat och uppfyller kraven i direktivet garanterar certifikatet, eller
- då certifikatet eller tillhandahållaren är erkänd genom ett bilateralt eller multilateralt avtal mellan gemenskapen och tredje land eller en internationell organisation.

Direktivet föreskriver också som uppgift för kommissionen att lägga förslag till standarder och internationella avtal som underlättar gränsöverskridande certifikattjänster och rättsligt erkännande av signaturer med ursprung i tredje land.

5.9 Dataskydd

Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter är tillämpligt på tillhandahållare av certifikattjänster och på nationella organ med ansvar för ackreditering och övervakning.

Tillhandahållare av certifikattjänster som utfärdar certifikat till allmänheten får endast samla in uppgifter direkt från den berörda personen eller med dennes uttryckliga medgivande och endast för att utfärda och bibehålla certifikatet. Uppgifterna får inte samlas in eller behandlas för andra ändamål utan ett uttryckligt medgivande från den berörda personen. Vidare får medlemsstaterna inte hindra tillhandahållare av certifikattjänster från att ange en pseudonym i stället för undertecknarens namn i certifikatet. För kvalificerade certifikat ställs dock krav på att det anges när det rör sig om en pseudonym.

5.10 Kommitté

En förvaltande kommitté, bestående av företrädare för medlemsstaterna och under ordförandeskap av en representant för kommissionen, skall konsulteras för att klargöra kraven i direktivets bilagor, kriterierna för utseende av de organ som skall avgöra om säkra anordningar för skapande av signaturer överensstämmer med kraven i bilaga III samt innehållet i de allmänt erkända standarder för produkter för elektroniska signaturer som kommissionen skall fastställa och offentliggöra.

Beslutsproceduren för förvaltande kommittéer framgår av artikel 4 i rådets beslut 1999/468/EG av den 28 juni 1999 om de förfaranden som skall tillämpas vid utövandet av kommissionens genomförande-befogenheter.

5.11 Anmälan, genomförande och översyn

Medlemsstaterna skall informera varandra och kommissionen om dels de ackrediteringssystem som tillämpas, dels namn på de organ som svarar för ackreditering och övervakning och som avgör om anordningar för signaturskapande överensstämmer med direktivets krav samt dels namn på samtliga ackrediterade tillhandahållare av certifikattjänster.

De nationella bestämmelser som behövs för att genomföra direktivet skall vara i kraft senast ett och ett halvt år efter det att direktivet trätt i kraft, dvs. den 19 juli 2001. Kommissionen skall göra en översyn av direktivet och överlämna en rapport om denna senast den 19 juli 2003.

6 Genomförande av direktivet

Den stora fördelen med direktivet är att det innebär en gemensam reglering för medlemsstaterna i Europeiska unionen (EU) och övriga

länder inom Europeiska ekonomiska samarbetsområdet (EES). Den utveckling med olikartad reglering av elektronisk kommunikation i varje land som hade påbörjats, har därigenom avstyrts.

Den marknad som regleras i direktivet har ännu inte vuxit fram i nämnvärd omfattning och det har ännu inte riktigt identifierats vilka problem som kan kräva lagstiftning. Vid det svenska genomförandet av direktivet finns det därför anledning att vara försiktig med att reglera ett bredare område än vad direktivet kräver. Det skulle kunna anföras skäl för att på vissa områden, t.ex. avseende skadestånd, även reglera sådant som inte krävs enligt direktivet. Regeringen föreslår dock inte någon sådan reglering, utan påpekar endast att utvecklingen kan göra det nödvändigt att i framtiden komplettera lagstiftningen.

6.1 En ny lag

Regeringens förslag: EG-direktivet (1999/93/EG) skall genomföras genom en särskild lag om kvalificerade elektroniska signaturer.

Promemorians förslag: Överensstämmer med regeringens förslag. I promemorian föreslogs dock att lagen skulle benämnas lagen om vissa elektroniska signaturer m.m.

Remissinstanserna: Flertalet remissinstanser är positiva till att direktivet genomförs genom en ny lag. Några remissinstanser påpekar dock att lagens egentliga innehåll inte överensstämmer med lagens namn. *GEA, Statskontoret, Kommerskollegium, IT-kommissionen, LO, Lagerlöf & Leman, Posten och Telia* förordar att de krav som anges i bilagorna till direktivet i stället genomförs genom en förordning.

Skälen för regeringens förslag: Enligt artikel 249 i EG-fördraget är ett direktiv bindande för medlemsstaterna vad avser det resultat som skall uppnås. Det överlåts dock åt de nationella myndigheterna att bestämma form och tillvägagångssätt för genomförandet.

Ett genomförande av direktivet innebär införande av ett tämligen stort antal nya, främst näringsrättsliga, regler. Telelagen (1993:957) innehåller visserligen närliggande regler om förmedling av telemeddelanden via telenät. Elektroniska signaturer utgör dock en ny företeelse och berör en helt ny marknad som inte rör televerksamhet i telelagens mening. På samma sätt finns kopplingar till regleringen av den finansiella sektorn, men direktivet rör ett mycket vidare område än den sektorn.

I andra sammanhang har det ansetts naturligt att föreslå ett införande i förvaltningslagen (1986:323) av definitioner och allmänna regler för elektroniska signaturer. Detta kan visserligen mycket väl vara lämpligt, men förvaltningslagen är inte rätt plats för att införa det främst näringsrättsliga regelverk det här är fråga om.

Det lämpligaste sättet att genomföra direktivets regler synes därför vara genom en ny särskild lag. I promemorian föreslogs att lagen skulle heta ”lag om vissa elektroniska signaturer m.m.”. Flera remissinstanser påpekar att lagen kommer att handla mer om kvalificerade certifikat för elektroniska signaturer och krav på dem som utfärdar sådana certifikat,

än om elektroniska signaturer i sig. Även *Lagrådet* har menat att ”lag om kvalificerade certifikat för elektroniska signaturer” vore en mer adekvat benämning. Lagens bestämmelser om certifikat, certifikatutfärdare och anordningar för signaturframställning syftar dock sammantaget till att skapa ett regelverk för kvalificerade elektroniska signaturer, för att skapa förtroende för och därigenom underlätta användningen av elektroniska signaturer. Lagens syfte anges, på förslag från Lagrådet, i den inledande bestämmelsen (se kommentaren till 1 §). Regeringen föreslår därför att lagen skall heta ”lag om kvalificerade elektroniska signaturer”.

Med hänsyn till direktivets karaktär blir det ofrånkomligt att delar av direktivet mer eller mindre ordagrant måste tas in i lagen. Flera remissinstanser ifrågasätter om det inte vore lämpligare att bilagorna till direktivet – som rör de krav som skall ställas på kvalificerade certifikat, utfärdare av certifikattjänster och säkra anordningar för signaturframställning – i stället borde genomföras genom en förordning. Som skäl för denna uppfattning anför de i huvudsak att lagen därmed skulle framstå som mer teknikneutral och att kraven lättare skulle kunna anpassas efter den tekniska utvecklingen. Regeringen har noga övervägt frågan, men kommit fram till att argumenten för en sådan uppdelning inte väger tyngre än argumenten emot. En hänvisning i lagen till en förordning där kraven regleras skulle inte innebära att regleringen som helhet blev mer teknikneutral. Det finns inte heller någon särskild procedur som gör det lättare att ändra i direktivets bilagor än i själva direktivtexten. Den kommitté som skall tillsättas (se avsnitt 5.10) skall inte föreslå ändringar i bilagorna, utan endast klargöra innebörden av dem. Det finns därför inga skäl att tro att de krav som ställs i bilagorna kommer att ändras särskilt snabbt eller ofta. Till största delen är kraven också ganska allmänt hållna, vilket innebär att den närmare innebörden av dem ändå måste klargöras genom föreskrifter av regeringen eller tillsynsmyndigheten och genom rättstillämpningen. Vidare blir regleringen mer lättläst om de krav som ställs finns samlade direkt i lagen. Även i övriga nordiska länder föreslås att kraven skall anges i själva lagen, och det är enligt regeringens mening en fördel om de nordiska lagarna blir så lika varandra som möjligt.

6.2 Lagens syfte och tillämpningsområde

Regeringens förslag: Lagen skall innehålla regler om krav på, tillsyn över och skadeståndsansvar för den som utfärdar certifikat för elektroniska signaturer, om certifikaten anges ha en viss säkerhetsnivå och om de utfärdas till allmänheten. Lagen skall vidare ge en särställning åt elektroniska signaturer med en viss säkerhetsnivå (s.k. kvalificerade elektroniska signaturer). Lagen skall inte reglera frågor om ingående eller giltighet av avtal.

Promemorians förslag: Överensstämmer med regeringens förslag.

Remissinstanserna: Remissinstanserna tillstyrker i huvudsak promemorians förslag. Några är dock kritiska till den gränsdragning som gjorts

av begreppet ”till allmänheten”. *Konsumentverket* och *IT-kommissionen* menar att lagen bör utvidgas till att avse alla som utfärdar någon form av certifikat för elektroniska signaturer. Flertalet remissinstanser tillstyrker dock promemorians förslag om vilka certifikatutfärdare som skall omfattas av lagen.

Skälen för regeringens förslag: Handel och annan kommunikation mellan enskilda, myndigheter och företag kan förväntas ske elektroniskt i ökad utsträckning, om det finns ett allmänt förtroende för att den information som skickas via Internet och andra öppna nät är tillförlitlig. Avsikten är att lagen skall bidra till detta genom att den främjar användandet av elektroniska signaturer som har en sådan säkerhetsnivå att de får ett allmänt erkännande och därmed kan användas för säker kommunikation, även mellan parter som inte har ett tidigare avtal om hur deras inbördes kommunikation skall gå till.

I direktivet läggs stor vikt vid resonemanget om elektroniska signaturers rättsliga verkan. För Sveriges del, där principerna om den fria bevisprövningen och den fria bevisvärderingen är etablerade sedan länge, intar denna fråga inte en central roll vad gäller lagstiftningen. Vad som kommer i fokus är i stället vilka regler som skall gälla för dem som vill tillhandahålla certifikattjänster, såsom på vilka villkor deras verksamhet får bedrivas, hur de ska övervakas, vilket ansvar de har etc. Målsättningen bör vara att bygga upp ett system som inte i onödan hämmar marknadens utveckling, t.ex. genom att låsa fast användning av en viss teknik eller skapa etableringshinder. Samtidigt skall systemet vara uppbyggt på ett sådant sätt att det långsiktigt skapas en tilltro till det hos konsumenter, näringsidkare och andra användare. Därigenom underlättas utvecklingen mot en allt större användning av elektroniska signaturer, vilket sannolikt kommer att stimulera den elektroniska handeln och medföra en rationalisering av förvaltningsväsendet baserad på elektroniska rutiner.

Av ingressen till direktivet (punkt 16) framgår att syftet med direktivet inte är att skapa något rättsligt ramverk för elektroniska signaturer som endast används inom system som grundar sig på frivilliga civilrättsliga avtal mellan ett bestämt antal deltagare (slutna system). Det anges vidare att parternas frihet att sinsemellan komma överens om på vilka villkor de godkänner elektroniskt signerade uppgifter bör respekteras, i den utsträckning det är förenligt med den nationella lagstiftningen. Det skall med andra ord stå var och en fritt att komma överens om vilken säkerhetsnivå som accepteras inbördes för att sluta avtal etc. I överensstämmelse med direktivets syfte skall lagen därför inte omfatta andra certifikat än sådana som utfärdas inom öppna system, eller ”till allmänheten”, vilket är det begrepp som används i direktivtexten och i lagen. I förhållande till promemorians lagförslag har detta förtydligats genom att tillämpningsområdet redan i inledningsbestämmelsen avgränsas till certifikat som utfärdas till allmänheten.

Svårigheten ligger i att definiera vad som utgör slutna respektive öppna system, för att kunna avgöra när ett certifikat skall anses utfärdat ”till allmänheten”. Vissa klara fall kan dock identifieras. När det är helt klart att certifikatutfärdaren är den ende som skall förlita sig på certifikatet och signaturen, är det utan tvekan frågan om ett slutet system. Ett exempel på

en sådan situation är bankernas Internettjänster, där det föreligger ett på förhand träffat avtal mellan banken och kunden och banken själv är den ende som skall förlita sig på certifikatet. Ett annat exempel på ett system som normalt torde vara slutet är när ett certifikat utfärdats för att enbart användas inom ett visst företag eller en viss organisation. Ett system måste däremot anses vara öppet i de fall de mottagare som skall förlita sig på certifikatet saknar varje form av avtal med undertecknaren eller certifikatutfärdaren. Ett exempel på ett sådant system är det finska initiativet med elektroniska ID-kort. På kortet finns ett certifikat utfärdat av Befolkningsregistercentralen och tanken är att kortet skall kunna användas för många olika ändamål, som vid utfärdandet inte är kända för vare sig utfärdaren eller kortinnehavaren. I ett sådant fall är det tydligt att certifikatet är utfärdat ”till allmänheten”. Däremellan kan det dock finnas många olika varianter där avgränsningen kan vara svår att göra.

Direktivet saknar närmare vägledning om hur begreppet ”till allmänheten” skall tolkas. I promemorian angavs att storleken på den grupp till vilken certifikatet erbjuds skulle ha betydelse för bedömningen. Flera remissinstanser, bl.a. *GEA* och *Posten*, har dock riktat stark kritik mot den inställningen. De har bl.a. anfört att syftet med att reglera certifikat som utfärdas till allmänheten är att tillvarata tredje mans skyddsintresse och att detta är lika stort oavsett om denne agerar ensam eller tillhör en större grupp. Enligt dessa remissinstanser bör därför det avgörande för bedömningen vara om certifikatet är avsett att användas gentemot tredje man, med vilken utfärdaren inte har någon tidigare relation. Regeringen delar remissinstansernas synpunkter att storleken på den grupp till vilken ett certifikat erbjudits inte bör vara avgörande för bedömningen av om det är utfärdat till allmänheten eller inte. I stället kan det vara rimligt att som huvudregel utgå från att det rör sig om utfärdande till allmänheten när en certifikatutfärdare erbjuder ett certifikat som är avsett att användas vid kommunikation med andra än certifikatutfärdaren, alltså en tredje part, och det inte föreligger något kontraktsförhållande mellan utfärdaren och denne tredje part. När en certifikatutfärdare anger att certifikaten är kvalificerade utan att i certifikaten begränsa kretsen av möjliga mottagare på ett mer precist sätt, kan det finnas anledning att anse att certifikatutfärdaren omfattas av lagens tillämpningsområde. Den närmare tolkningen av begreppet ”till allmänheten” får dock överlämnas till rättstillämpningen.

Det är viktigt att framhålla att det inte är alla certifikat utfärdade till allmänheten som regleras, utan endast sådana som anges vara ”kvalificerade”. I lagen anges en säkerhetsnivå för sådana kvalificerade certifikat för elektroniska signaturer. och ställs krav på dem som vill utfärda sådana till allmänheten. De som utfärdar kvalificerade certifikat till allmänheten ställs under viss tillsyn och deras skadeståndsansvar fastställs. Reglerna gäller endast certifikatutfärdare som är etablerade i Sverige. Se dock 3 § andra stycket och avsnitt 6.4.

Avsikten är inte att i lagen reglera alla tjänster rörande elektroniska signaturer. Det kommer även efter lagens ikraftträdande att vara möjligt att utfärda certifikat för elektroniska signaturer utan att underkasta sig tillsyn eller vara tvungen att använda sig av viss bestämd teknik. Till exempel regleras inte certifikat som avser juridiska personer eller andra

sammanslutningar. Sådana certifikat kan med fördel användas i många situationer där det inte anses viktigt att få reda på exakt vilken person som har vidtagit en viss åtgärd. De som utfärdar certifikat till allmänheten och som väljer att beteckna certifikaten som kvalificerade certifikat, väljer dock också att omfattas av den ordning som föreskrivs i lagen. Lagen syftar till att möjliggöra att det på marknaden finns produkter och tjänster som uppfyller vissa minimikrav, som är gemensamma för länderna inom EES-området.

Vad gäller uppfyllandet av formkrav på egenhändig underskrift och liknande ges i lagen en särställning åt elektroniska signaturer som har en viss säkerhetsnivå (”kvalificerade elektroniska signaturer”).

Lagen reglerar inte frågor om ingående eller giltighet av avtal.

6.3 Definitioner

Regeringens förslag: EG-direktivets (1999/93/EG) definitioner skall i allt väsentligt anges också i lagen.

Promemorians förslag: Överensstämmer med regeringens förslag. I promemorian föreslogs dock en definition av begreppet ”elektronisk handling”. Däremot föreslogs inga definitioner av begreppen ”kvalificerat certifikat” och ”säker anordning för signaturframställning”.

Remissinstanserna: Flertalet remissinstanser lämnar promemorians förslag i huvudsak utan invändning, men har många synpunkter på den närmare utformningen av definitionerna. Flera remissinstanser har bl.a. haft invändningar mot införandet av begreppet ”elektronisk handling”.

Skälen för regeringens förslag: Den tekniska utvecklingen och ersättandet av traditionella pappershandlingar med elektroniska data reser en mängd frågor om, och i så fall på vilket sätt, denna företeelse kräver en annan rättslig reglering än den existerande. Dessa frågor har behandlats i flera utredningar och i vissa fall lett till lagstiftning. Användningen av s.k. elektroniska dokument regleras i ett trettiotal svenska författningar. Som exempel kan nämnas 12 § tullagen (1994:1550), enligt vilken Tullverket kan ge tillstånd till att bl.a. tulldeklarationer får lämnas genom ett elektroniskt dokument. Ett elektroniskt dokument definieras där som en upptagning vars innehåll och utställare kan verifieras genom ett visst tekniskt förfarande. Sådana elektroniska dokument kan också, efter särskilt medgivande, i viss omfattning användas inom skatteområdet och exekutionsväsendet samt för vissa ansökningar gällande registrering av datapantbrev[4].

Definitionerna i direktivet har som nämnts utformats i avsikt att vara teknikneutrala. Den teknik som f.n. är förhärskande, där man använder digitala signaturer med ett certifikat som intygar kopplingen mellan en öppen nyckel och en bestämd person (det öppna nyckelsystemet), har dock legat till grund för den struktur som valts i direktivet.

[4] Se t.ex. 2 kap. 2 § lagen (1990:325) om självdeklaration och kontrolluppgifter, 2 a § indrivningsförordningen (1993:1229) och 17 § lagen (1994:448) om pantbrevsregister.

Till skillnad från direktivet används i den föreslagna lagtexten ordet ”data” i stället för ”uppgifter”, då det mindre är fråga om uppgifter i betydelsen information som skall förstås av så många som möjligt, än om konstellationer av ettor och nollor som ofta inte i sig ger ett mänskligt öga särskilt mycket upplysning. Det är dessutom ofta önskvärt att hemlighålla dessa data. Jfr Datastraffrättsutredningens definition av ”data” som en representation av fakta och av ”information” som innebörden av data i SOU 1992:110.

I betänkandet Elektronisk dokumenthantering (SOU 1996:40) föreslogs att det i förvaltningslagen (1986:223) skulle införas vissa grundläggande begrepp. ”Elektronisk handling” föreslogs där definieras som en bestämd mängd data som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel. Vidare föreslogs att begreppet ”digitalt dokument” skulle införas (till skillnad från det i befintlig lagstiftning använda begreppet ”elektroniskt dokument”) ”Digitalt dokument” definierades i betänkandet som en elektronisk handling med digital signatur eller digital stämpel. ”Digital signatur” definierades i sin tur som resultatet av en omvandling av en elektronisk handling, som gör det möjligt att kontrollera om innehållet härrör från den fysiska person som framstår som utställare. ”Digital stämpel” skulle på samma sätt härröra från en juridisk person eller myndighet. Remissutfallet var blandat och betänkandet har inte lett till någon lagstiftning i denna del.

Sverige är visserligen inte bundet av den terminologi och systematik som angivits i direktivet, om det avsedda resultatet kan uppnås med annan terminologi och systematik. Direktivet är emellertid utformat så att utrymmet att avvika från terminologin är mycket begränsat.

En strävan är givetvis att lagtexten skall vara så enkel och begriplig som möjligt. Den tämligen komplicerade verklighet som direktivet beskriver kräver dock en begreppsapparat som, för att kunna fungera, inte kan förenklas alltför mycket.

En annan strävan är att i möjligaste mån anknyta till den begreppsbildning som redan existerar i Sverige. En tredje är att åtminstone de nordiska länderna skall få en så enhetlig reglering som möjligt.

I promemorian föreslogs ett införande av begreppet ”elektronisk handling”. Bland andra *Kammarrätten i Stockholm, Länsrätten i Stockholms län* och *Tekniska nomenklaturcentralen* menar att begreppet inte är tillräckligt analyserat och att det inte tillför lagen något. Länsrätten påpekar även att begreppet lätt kan leda till förvirring i förhållande till närliggande begrepp som används i andra lagar. De remissinstanser som är positiva till införandet, främst *GEA* och *Försvarets forskningsanstalt*, pekar främst på att en definition av elektronisk handling kan vara av värde i andra sammanhang.

Såsom anfördes i promemorian (s. 60) behövs inte begreppet ”elektronisk handling” för att förklara något i lagen. Begreppet ”elektronisk signatur” kan lika gärna definieras på samma sätt som i direktivet. Vidare framgår av inledningen till 2 § att definitionerna bara förklarar vad som avses med begreppen i just denna lag. En definition i den här lagen har därför inte automatiskt någon betydelse i andra sammanhang. *Statskontoret* menar av det skälet att definitionen passar bättre i förvaltningslagen. Eftersom begreppet inte behövs för att förklara

något i den här lagen och eftersom det riskerar att skapa förvirring i förhållande till närliggande begrepp som används i andra lagar, såsom elektroniska dokument, avstår regeringen från att föreslå att begreppet införs i lagen. Regeringen tar dock inte i detta läge ställning till om det av någon anledning som saknar samband med genomförandet av direktivet finns behov av en definition av elektronisk handling i förvaltningslagen eller någon annanstans. Borttagandet av definitionen medför följdändringar i definitionerna av elektronisk signatur och avancerad elektronisk signatur.

Det saknas behov av att införa begreppet ”digital stämpel” eller liknande, som diskuterats ovan. Direktivet förutsätter att en fysisk person är knuten till signaturen. Det hindrar visserligen inte ett system med elektroniska stämplar för juridiska personer eller certifikat som anger att signaturen innehas av en identifierad person som är behörig firmatecknare för en juridisk person (s.k. rollcertifikat). Något särskilt behov av att reglera detta synes emellertid inte finnas. I stället kan redan gällande regler om rättshandlingsförmåga, fullmakt och behörighet att företräda juridiska personer tillämpas.

En elektronisk signatur bör i lagen definieras på samma sätt som i direktivet. Ett flertal remissinstanser menar att det bör förtydligas att en elektronisk signatur, till skillnad från en avancerad eller kvalificerad elektronisk signatur (se nedan) bara är en teknisk metod och inte behöver vara knuten till en fysisk person. Regeringen delar den uppfattningen och föreslår att ordet ”undertecknare”, som enligt definitionen är en fysisk person, byts ut mot ”utställare”, som kan vara såväl en fysisk som en juridisk person. *Patent- och registreringsverket* påpekar att förslagets definition av elektronisk signatur avviker något från hur begreppet definierats i direktivet. I direktivet anges att en elektronisk signatur används som en metod för ”autentisering”. Med autentisering torde avses inte bara identitetskontroll av undertecknaren, utan även kontroll av att innehållet inte förvanskats. Regeringen föreslår därför ett tillägg i definitionen i förhållande till promemorians förslag.

Definitionerna av ”avancerad elektronisk signatur”, och ”certifikat” kan lämpligen hämtas direkt från direktivet. Såsom några remissinstanser påpekar kan dock användningen av orden ”alla efterföljande ändringar” i punkten d) misstolkas så att det skall kunna upptäckas *vilka* olika ändringar som eventuellt har gjorts. Det som skall kunna upptäckas är dock bara *att* en ändring av den elektroniska handlingen har gjorts. I förhållande till promemorians förslag har därför orden ”alla efterföljande” strukits. Genom kravet att en avancerad, och därmed också en kvalificerad, signaturer skall vara knuten till en undertecknare och genom definitionen av undertecknare framgår att en sådan signatur – till skillnad från en ”enkel” elektronisk signatur – alltid måste vara knuten till en fysisk person. Rent tekniskt är det dock, vilket *IT-kommissionen* påpekar, inte signaturen i sig som är knuten till undertecknaren utan dennes hemliga nycklar (signaturframställningsdata) i kombination med dennes certifikat.

En ”undertecknare” är den fysiska person som innehar en anordning för signaturframställning. I promemorian föreslogs att en undertecknare skulle definieras som ”den som har kontroll över” en anordning för

signaturframställning. Många remissinstanser påpekar dock att det bör förtydligas att undertecknaren måste vara en fysisk person. Några remissinstanser menar även att definitionen kan tolkas så att det räcker med att någon just för tillfället råkar ha kontroll över anordningen för att denne skall anses som undertecknare. De menar därför att direktivets definition – den som ”innehar” – är att föredra framför den som föreslogs i promemorian. Regeringen delar uppfattningen att det bör förtydligas att undertecknaren måste vara en fysisk person och att det är lämpligare att använda ordet ”innehar” än ”har kontroll över”. Naturligtvis kan undertecknaren med stöd av vanliga regler om rättshandlingsförmåga, fullmakt och behörighet representera en annan fysisk eller juridisk person. Det behöver därför inte, som i direktivet, anges särskilt.

”Uppgifter för skapande av signaturer” (”den hemliga nyckeln” i det öppna nyckelsystemet) och ”uppgifter för signaturverifiering” (den öppna nyckeln) föreslås ersättas med ”signaturframställningsdata”, respektive ”signaturverifieringsdata”. Dessa begrepp är visserligen varken korta eller särskilt lättbegripliga vid första anblicken. De är dock i överensstämmelse med vad som föreslås i andra nordiska länder och ger en god bild av vad som avses. Användandet av ordet ”data” i stället för ”uppgifter” torde, som tidigare nämnts, bidra till en bättre beskrivning av företeelserna. I promemorian användes begreppet ”privata” krypteringsnycklar. *Tekniska nomenklaturcentralen* förordar dock att begreppet ”hemliga” krypteringsnycklar i stället används, vilket regeringen finner lämpligt.

Begreppen ”anordning för skapande av signaturer” och ”säker” sådan anordning kan i princip definieras såsom det angetts i direktivet, med de ändringar som följer av det föregående. Regeringen har dock, liksom i promemorian, valt att använda begreppet ”anordning för signaturframställning”. Såsom *Tekniska nomenklaturcentralen* påpekar fyller dock ordet ”konfigurerad” inte någon funktion. Det måste förutsättas att all maskin- och programvara som är avsedd att användas för ett visst ändamål också är konfigurerad för detta ändamål. ”Anordning för signaturverifiering” kommer inte att regleras i lagen, varför det saknas skäl att införa begreppet.

Direktivet använder sig av begreppet ”tillhandahållare av certifikattjänster” och inbegriper där inte bara de som utfärdar certifikat utan också de som tillhandahåller andra tjänster som har anknytning till elektroniska signaturer. Det som regleras i direktivet är dock begränsat till utfärdande av kvalificerade certifikat och i viss mån garanterande av annans certifikat som kvalificerade. Exempelvis rör kraven i direktivets bilaga II endast tillhandahållare av certifikattjänster vilka utfärdar kvalificerade certifikat. Det finns därför inte behov av att i lagen skapa en definition som omfattar mer än de som utfärdar certifikat eller garanterar annans certifikat, lämpligast genom termen ”certifikatutfärdare”. I den mån man i annat sammanhang önskar reglera även andra tjänster, såsom registrering av återkallande, tidsstämpling, kryptering för konfidentialitet eller diverse konsulttjänster, låter sig detta väl göras utan att här tynga lagtexten med en onödigt vid och diffus definition. Detta kan kanske också bidra till att minska den redan olyckliga förväxlingsrisken mellan de certifikat och den certifiering som här avses och det styrkande av

certifikatutfärdarens kompetens som i sin tur kan ges av (eventuellt ackrediterade) certifieringsorgan.

I promemorian återfanns inte begreppen ”kvalificerat certifikat” och ”säker anordning för signaturframställning” bland definitionerna, vilket ett flertal remissinstanser har kritiserat. Begreppen, vars innebörd behandlas i avsnitt 6.4 och 6.8, har därför definierats med hänvisning till de respektive bestämmelser där kraven anges.

Direktivet vill ge de elektroniska signaturer som inte bara är avancerade utan också baserade på ett kvalificerat certifikat och skapade av en säker anordning för signaturframställning en särskild ställning. Det förefaller därför lämpligt att ge dessa signaturer en särskild benämning. Här har valts ”kvalificerade elektroniska signaturer”.

Det saknas anledning att i svensk lag införa den definition av ”frivillig ackreditering” som ges i direktivet. Dess innebörd är oklar och ett införande skulle inte tjäna till annat än att tynga lagtexten och försvåra förståelsen av densamma (se avsnitt 6.7). Inte heller begreppet ”produkt för elektroniska signaturer” fyller någon funktion i den svenska lagtexten.

6.4 Kvalificerade certifikat

Regeringens förslag: Det skall anges i lagen vad som krävs för att ett certifikat skall anses ha en särskild säkerhetsnivå. Dessa certifikat skall betecknas ”kvalificerade certifikat”.

Promemorians förslag: Överensstämmer med regeringens förslag. I promemorian föreslogs dock inte någon bestämmelse avseende certifikat utfärdade av en certifikatutfärdare etablerad utanför Sverige.

Remissinstanserna: Remissinstanserna tillstyrker förslaget eller lämnar det utan erinran (se dock under avsnitt 6.1).

Skälen för regeringens förslag: I direktivet regleras en särskild, högre nivå på certifikat som benämns ”kvalificerade certifikat”. De krav på vad certifikatet måste innehålla som anges i bilaga I till direktivet bör också anges i den svenska lagtexten. Likaså bör i enlighet med direktivet anges att endast certifikat som utfärdats av en certifikatutfärdare som uppfyller vissa i lagen angivna krav är kvalificerade certifikat.

I kravet på att kvalificerade certifikat måste ha visst innehåll ligger att detta innehåll skall vara tillgängligt för den mottagare som förlitar sig på certifikatet. När denne tar emot ett signerat meddelande måste han således kunna tillgodogöra sig denna information, antingen genom att han ser certifikatet, där all nödvändig information finns, eller genom att informationen på annat sätt presenteras i samband med att han mottar en elektronisk handling. Inte minst viktiga är uppgifter om begränsningar för certifikatet vad gäller användningsområde eller värdet på de transaktioner för vilka certifikatet kan användas.

I direktivet anges i artikel 4.1 att medlemsstaterna inte får begränsa tillhandahållandet av certifikattjänster med ursprung i andra medlemsstater. I artikel 7.1 anges även att medlemsstaterna skall säkerställa att certifikat som utfärdas som kvalificerade certifikat till allmänheten av

certifikatutfärdare som är etablerade i ett tredje land, under vissa förutsättningar, betraktas som rättsligt likvärdiga med certifikat som utfärdats av certifikatutfärdare etablerade inom EES. De särskilda förutsättningar som krävs för detta är att certifikatutfärdaren uppfyller kraven i direktivet och har ackrediterats i en medlemsstat, att en certifikatutfärdare som är etablerad inom EES garanterar certifikatet, eller att certifikatet eller certifikatutfärdaren har erkänts genom ett bilateralt eller multilateralt avtal (se avsnitt 5.5 och 5.8). Genom den inledande bestämmelsen i 1 § har lagens tillämpningsområde begränsats till sådana certifikatutfärdare som är etablerade i Sverige (se avsnitt 6.2). För att inte lagen skall innebära begränsningar för certifikatutfärdare etablerade i andra länder i strid med artikel 4.1 och 7.1 bör det införas en bestämmelse som innebär att även certifikat utfärdade av sådana, under vissa förutsättningar skall anses vara kvalificerade.

6.5 Utfärdande av kvalificerade certifikat

Regeringens förslag: Det skall anges i lagen vad som krävs av en certifikatutfärdare för att denne skall få kalla sina certifikat kvalificerade.

Promemorians förslag: Överensstämmer med regeringens förslag.

Remissinstanserna: Remissinstanserna tillstyrker förslaget eller lämnar det utan erinran (se dock under avsnitt 6.1). Bland andra *iD2 Technologies*, *GEA* och *Posten* menar att det inte bör krävas att det i certifikatet anges en elektronisk signatur som skapats av en fysisk person.

Skälen för regeringens förslag: En certifikatutfärdares uppgift är att som en betrodd part intyga att vissa signaturverifieringsdata hör till en viss undertecknare. Nyckelordet i sammanhanget är ”betrodd”. För att certifikatutfärdarna skall bli betrodda krävs att de bedriver verksamheten med erforderlig garanti för pålitlighet.

Direktivet ställer krav endast på de certifikatutfärdare som utfärdar kvalificerade certifikat. Det saknas anledning att i svensk lagstiftning ställa krav på en vidare krets av certifikatutfärdare än dessa. (Vad gäller skadeståndsskyldigheten kan det däremot finnas anledning att mer ingående diskutera om en reglering bör träffa en vidare krets, se avsnitt 6.9.2.)

I bilaga I h) till direktivet anges att certifikatet måste innehålla certifikatutfärdarens avancerade elektroniska signatur. Den definition av avancerad elektronisk signatur som anges i lagen innebär att en sådan måste vara kopplad till en fysisk person. Bland andra *iD2 Technologies, GEA* och *Posten* påpekar dock att en certifikatutfärdare vanligtvis torde vara en juridisk person och därför inte kan skapa en avancerad elektronisk signatur. De menar att även om en fysisk person med stöd av vanliga fullmaktsregler alltid kan signera å certifikatutfärdarens vägnar, så skulle ett sådant krav innebära stora praktiska problem för certifikatutfärdarna. Regeringen anser att syftet med direktivets krav på denna punkt varit att den elektroniska signatur som certifikatutfärdaren

använder måste ha en tillräckligt hög säkerhetsnivå, men inte att den nödvändigtvis måste vara knuten till en fysisk person. Regeringen föreslår därför att det i certifikatet måste anges antingen en avancerad elektronisk signatur (som är knuten till en fysisk person med behörighet att företräda certifikatutfärdaren), eller en elektronisk signatur med motsvarande säkerhetsnivå (som kan vara knuten till certifikatutfärdaren själv). Med motsvarande säkerhetsnivå avses alltså att det måste vara möjligt att identifiera vilken juridisk person som skapat signaturen (utställaren), att signaturen är skapad med hjälpmedel som endast utställaren kontrollerar och att signaturen är knuten till andra elektroniska data på ett sådant sätt att ändringar av dessa data kan upptäckas.

De krav som direktivet ställer på certifikatutfärdare som utfärdar kvalificerade certifikat (bilaga II), bör ställas också i den svenska lagen. Detta innebär krav på bl.a. pålitlighet, system för säker och snabb spärrning av certifikat, säker identitetskontroll av undertecknaren, kompetent personal samt användande av pålitliga system och produkter som garanterar teknisk säkerhet. Vad gäller kravet på användandet av pålitliga system och produkter bör vidare anges att det skall anses uppfyllt om de överensstämmer med standarder för produkter för elektroniska signaturer som kommissionen offentliggjort referenser till (artikel 3.5 i direktivet).

Certifikatutfärdaren åläggs bl.a. att bevara all relevant information om certifikatet under en rimlig tid. Den information som skall bevaras omfattar dock inte signaturframställningsdata. Eftersom det är väsentligt för tilltron till elektroniska signaturer att det bara är undertecknaren som har tillgång till signaturframställningsdata (hemliga nycklar o.d.) förbjuds certifikatutfärdaren att bevara och lagra sådana data. För att förtydliga detta har, på förslag från *Kammarrätten i Stockholm*, det andra stycke i 8 § som föreslogs i promemorian i regeringens förslag flyttats till 10 §, som behandlar certifikatutfärdarens informationshantering.

Certifikatutfärdaren åläggs även att, innan denne ingår avtal om att utfärda ett kvalificerat certifikat, skriftligen informera motparten om vissa särskilt väsentliga uppgifter. Med uttrycket att informationen skall lämnas skriftligen avses här att den inte får lämnas muntligen, men dock elektroniskt. Innebörden av begreppet skriftligen diskuteras bl.a. i betänkandet Elektronisk dokumenthantering, SOU 1996:40, avsnitt 5.3 och 5.4.

6.6 Standardisering

För att elektroniska signaturer ska få en bred användning är det väsentligt att ha en gemensam syn på vilka tekniska krav som skall gälla i olika avseenden och bygga upp system som kan samverka med varandra. Tekniska standarder har här en viktig roll att fylla och kan underlätta för användare av systemen och göra det möjligt att bedöma signaturernas säkerhet.

Tekniska standarder kan ange precisa krav för produkter för elektroniska signaturer, såsom t.ex. anordningar för signaturframställning och signeringsalgoritmer, och för certifikatutfärdande och andra certifikat-

tjänster. Standardisering underlättar också bedömningen av om ett specifikt system eller en viss produkt uppfyller de krav som man vill ställa för den aktuella tillämpningen.

Tekniska standarder möjliggör vidare interoperabilitet, dvs. att utrustningen hos avsändare och mottagare av elektronisk kommunikation är sådan att de faktiskt kan förstå varandras meddelanden. Det önskvärda är att det utvecklas ett informationssamhälle där man helst globalt eller åtminstone inom en definierad intressesfär kan utbyta och verifiera elektroniskt signerade handlingar. Myndigheternas elektroniska gränsyta mot omvärlden skulle bli ohanterlig om antalet metoder som används för elektroniska signaturer inte begränsas.

Kommissionen gav hösten 1998 i uppdrag åt de europeiska standardiseringsorganen och andra organisationer att analysera de framtida behoven av standardisering enligt direktivet, med avseende på produkter för elektroniska signaturer och tjänster som finns tillgängliga på marknaden. Det ingick i uppdraget att föreslå en plan för att utveckla de standarder som behövs. Detta resulterade i European Electronic Signature Standardization Initiative (EESSI) som presenterat en rapport under 1999.

Analysen i rapporten visar att området är mycket komplext. Ett hundratal existerande relevanta standarder identifierades. Trots detta var slutsatsen att många viktiga specifikationer behöver utvecklas med hög prioritet (se vidare under avsnitt 6.7).

Rapporten följdes under hösten 1999 av ett ”mandat” från kommissionen till de europeiska standardiseringsorganen (CEN, CENELEC och ETSI) att följa upp EESSI-rapporten, i syfte att förse marknaden med standarder till stöd för genomförandet av direktivet. I mandatet ingår också att bilda en särskild rådgivande grupp, kallad Electronic Signature Standardization Industry Advisory Group, för att ge rekommendationer till den rådgivande kommitté som skall inrättas enligt direktivet (se avsnitt 5.10). Kommittén skall konsulteras av kommissionen när denna skall klargöra kraven i direktivets bilagor och kriterierna för utseende av de organ som skall avgöra om säkra anordningar för skapande av signaturer överensstämmer med kraven i bilaga III. Kommittén skall också konsulteras om de allmänt erkända standarder för produkter för elektroniska signaturer som kommissionen skall fastställa och offentliggöra referensnummer till.

6.7 Ackreditering och certifiering

Regeringens bedömning: Lagen (1992:1119) om teknisk kontroll ger redan nu en möjlighet till frivillig ackreditering av certifieringsorgan med det syfte som anges i direktivet.

Promemorians bedömning: Överensstämmer med regeringens bedömning.

Remissinstanserna: Remissinstanserna delar promemorians bedömning eller lämnar den utan erinran.

Skälen för regeringens bedömning: Enligt direktivet kan medlemsstaterna införa frivilliga ackrediteringssystem som syftar till att höja nivån på tillhandahållandet av certifikattjänster. Inom direktivets svårgenomträngliga definition av ”frivillig ackreditering” torde rymmas det system för ackreditering och, inte minst, certifiering under ackreditering, som tillhandahålls genom lagen (1992:1119) om teknisk kontroll. Mot bakgrund av att direktivet uttryckligen förbjuder varje form av förhandstillstånd torde de ”rättigheter och skyldigheter” som nämns i definitionen vara rättigheten att kalla sig ackrediterad/certifierad och skyldigheten att leva upp till den nivå som krävs för ackreditering/certifiering.

Syftet med ackreditering (jfr avsnitt 4.4) är att skapa tilltro till de tjänster som de ackrediterade organen presterar. Härigenom skapas också tilltro till provningsintyg, certifikat m.m., som bl.a. gör det möjligt att godta sådan dokumentation från ett annat land utan förnyad kontroll. Därmed har ackreditering fått en viktig roll för att främja fri rörlighet av varor och tjänster på den inre marknaden. I detta arbete gäller som en viktig princip att statliga förhandsgodkännanden skall undvikas. Det hindrar inte att krav ställs på provning och kontroll. Bedömning av överensstämmelse ses dock som en teknisk uppgift utanför den offentligrättsliga sfären.

En ackreditering är alltid frivillig. Aktörer på marknaden vill ofta ha bevis på att varor och tjänster uppfyller ställda krav. Provning eller kontroll utförda av organ med särskild påvisad kompetens kan vara ett sätt att åstadkomma detta. Att ackreditering i sig är frivillig hindrar inte att ett ackrediteringssystem kan utnyttjas för att åstadkomma legalt tvingande regler om provning och kontroll, vilket ibland har skett i Sverige. Tvånget har då bestått i ett åliggande att anskaffa ett provningsintyg eller certifikat från ett ackrediterat organ. Ett sådant intyg eller certifikat får därmed rättsverkningar utan att förhållandet mellan utfärdaren och beställaren får någon offentligrättslig prägel. Staten tar själv inget ansvar för dokumentet på annat sätt än genom att ålägga beställaren att anskaffa dokumentet från ett organ som uppfyller av staten uppställda kvalitetskrav. I Sverige knyts dessa kvalitetskrav normalt till ett krav på ackreditering.

Så behöver dock inte alltid vara fallet. Inom EU har man hittills undvikit att ställa formella krav på ackreditering och i stället formulerat kvalitetskrav som ibland knyts till standarder. För certifieringsorgan kan således krävas att organet skall uppfylla kraven i t.ex. standarden EN 45 011. Detta behöver dock inte visas med ackreditering, även om ackreditering är det normala sättet att styrka att kravet är uppfyllt. Inom ramen för EG:s produktdirektiv skall medlemsländerna utse s.k. anmälda organ för uppgifter som innefattar provning och certifiering. Inte heller här uppställs krav på ackreditering, men det anges att ett organ som är ackrediterat skall antas uppfylla kraven.

I Sverige finns det nationella ackrediteringssystemet reglerat i lagen om teknisk kontroll. Där finns också regler om utseende av anmälda organ enligt EG-regler. Grundläggande för både ackreditering och utseende av anmälda organ är att systemen är öppna för alla organ som begär

det och kan visa sin kompetens enligt ställda krav. Anmälda organ skall granskas av SWEDAC på samma sätt som vid ackreditering.

Som har framgått ovan har certifikaten en stor betydelse i den ordning som regleras i direktivet. Tilltron till certifikaten får därmed central betydelse och medlemsländerna förutsätts på olika sätt främja kvaliteten på erbjudna certifikat. I enlighet med vanliga EG-rättsliga principer förbjuds krav på förhandstillstånd. Medlemsländerna får dock enligt en uttrycklig bestämmelse utnyttja frivilliga ackrediteringssystem, som då skall vara objektiva, öppna och icke-diskriminerande.

En ordning med ackreditering av organ för certifiering av certifikatutfärdare ligger helt inom ramen för SWEDAC:s verksamhet enligt lagen om teknisk kontroll. Någon ordning för ackreditering av den här typen av certifieringsorgan finns ännu inte helt färdig men kan relativt lätt inrättas. Den befintliga standarden EN 45 012 kan med små justeringar användas för ackreditering av certifieringsorgan för att certifiera certifikatutfärdare. Dessutom är standarder för att ackreditera certifieringsorgan för produktcertifiering under utarbetande.

Vidare finns det redan i viss mån standarder som kan användas vid certifiering av certifikatutfärdare vad gäller lednings- och säkerhetssystem, såsom den brittiska BS 7799, del 1 (Code of practise for Information Security management) och ISO TR 13335 (Guidelines for the Management of Information Technology Security-GMITS). Numera finns även en svensk standard, baserad på den brittiska SS 62 77 99. Det finns även standarder som i princip kan användas för certifiering av framställning av kvalificerade certifikat (t.ex. X.509).

Lagen om teknisk kontroll ger redan nu en möjlighet till frivillig ackreditering av certifieringsorgan med det syfte som anges i direktivet. Det finns därmed ingen anledning att i lagen om certifikat för elektroniska signaturer införa regler om ackreditering eller certifiering. Skyldigheten enligt direktivet att informera kommissionen och andra medlemsstater om ackrediterade nationella tillhandahållare av certifikattjänster följer av grunderna för förordningen (1994:2035) om vissa skyldigheter för myndigheter vid ett medlemskap i Europeiska unionen.

Eftersom ackreditering är frivillig, finns det inte något hinder att utan ackreditering bedriva certifiering av certifikatutfärdare.

6.8 Anordningar för signaturframställning

Regeringens förslag: Det skall anges i lagen vad som krävs för att en anordning för signaturframställning skall vara säker. Det skall också föreskrivas att en anordning som anges vara en säker anordning får släppas ut på marknaden eller användas för att skapa en kvalificerad signatur endast om ett för ändamålet anmält organ inom Europeiska ekonomiska samarbetsområdet (EES) avgjort att anordningen uppfyller kraven. Vidare skall det anges att anordningar som överensstämmer med vissa standarder skall presumeras uppfylla kraven.

Promemorians förslag: Överensstämmer med regeringens förslag.

Remissinstanserna: Remissinstanserna tillstyrker förslaget eller lämnar det utan erinran.

Skälen för regeringens förslag: På samma sätt som för de kvalificerade certifikaten bör de krav som anges i direktivets bilaga III anges i den svenska lagtexten beträffande de säkra anordningar för signaturframställning, som krävs för att skapa en kvalificerad signatur. I den svenska versionen av direktivet sägs i 1.a i bilagan att signaturframställningsdata ”praktiskt taget” skall kunna förekomma bara en gång. Uttrycket tycks dock grunda sig på en felöversättning av engelskans ”practically”. Regeringen menar, liksom flera remissinstanser, att orden ”i praktiken” bättre uttrycker vad som avses och föreslår att de orden används i lagtexten i stället.

Artikel 3.4 i direktivet anger att vissa organ *skall* avgöra om säkra anordningar överensstämmer med kraven i bilaga III. Det får förstås som ett krav på att endast anordningar som av ett sådant organ bedömts överensstämma med kraven får användas för att framställa kvalificerade signaturer eller släppas ut på marknaden under beteckningen ”säkra anordningar för signaturframställning”. Samtidigt anges i artikel 3.5 att medlemsstaterna skall utgå från att produkter som uppfyller standarder som kommissionen refererat till i Europeiska gemenskapernas officiella tidning överensstämmer med kraven i bilaga III. Någon möjlighet att tolka direktivet som att det kan räcka med en tillverkardeklaration om att en produkt uppfyller de aktuella standarderna torde inte finnas. Den sistnämnda regeln måste anses vara riktad till de aktuella organen. Denna bedömning görs också i de övriga nordiska länderna. En regel om obligatorisk kontroll av anordningarna kompletterad med presumtionen för produkter som uppfyller de nämnda standarderna bör alltså införas i den svenska lagen.

Den möjligen kostsamma och tidskrävande obligatoriska certifiering som det här är fråga om torde dock inte nödvändigtvis innebära alltför negativa konsekvenser, då det ju räcker med att produkten godkänns i ett av länderna inom EES. Tillverkaren eller marknadsföraren är dessutom inte hänvisad till ett organ i hemlandet. Detta följer också av artikel 3.4 i direktivet där det stadgas att ett beslut som fattats av ett organ i en medlemsstat skall erkännas av samtliga medlemsstater. Även detta bör anges i lagtexten.

Enligt direktivet skall medlemsstaterna, i enlighet med kriterier som kommissionen senare skall fastställa, utse sådana organ som skall avgöra om säkra anordningar för signaturframställning överensstämmer med kraven i direktivets bilaga III. Regeringen föreslår att det görs en hänvisning till lagen om teknisk kontroll, där det i 3 § föreskrivs att regeringen eller den myndighet som regeringen bestämmer utser de organ som skall anmälas till EU för uppgifter i samband med bedömning av överensstämmelse enligt bestämmelser som gäller inom EES (se avsnitt 4.4). Regeringen eller myndigheten (SWEDAC) har därvid att ta hänsyn till de kriterier som kommissionen kommer att fastställa. Regeringen kan vid behov utfärda närmare bestämmelser om detta enligt ett bemyndigande i 5 § lagen om teknisk kontroll.

6.9.1 Allmänt om skadestånd och användning av elektroniska signaturer

Det öppna nyckelsystemet

Direktivet bygger som nämnts på ett tekniskt och organisatoriskt system för elektroniska signaturer som benämns det öppna nyckelsystemet (se avsnitt 4.3.4). Systemet är för dagen det helt förhärskande för elektroniska signaturer. I framtiden kan dock något annat komma att gälla.

Det öppna nyckelsystemet bygger på medverkan av tre aktörer, nämligen undertecknare, certifikatutfärdare och mottagare. Det kan dock förekomma – och det är inte ovanligt – att en och samma person eller företag är mer än en aktör i denna kedja. Det är t.ex. vanligt att en bank är både certifikatutfärdare och mottagare. Så är fallet när en bank utfärdar certifikat för att sedan förlita sig på elektroniska signaturer som används av bankens kunder.

Undertecknaren kan också benämnas ”nyckelinnehavaren”, dvs. den som innehar det unika nyckelpar som utgörs av en hemlig nyckel och en öppen nyckel (se avsnitt 4.3.1). Nyckelinnehavaren/undertecknaren är ”den behörige”, som har kontroll över signaturframställningsdata och anordningen för signaturframställning.

Det öppna nyckelsystemet reser i huvudsak tre olika särskilda skadeståndsrättsliga ansvarsförhållanden, nämligen

a. undertecknarens ansvar vid obehörig användning av den elektroniska signaturen,

b. certifikatutfärdarens ansvar gentemot undertecknaren, och

c. certifikatutfärdarens ansvar gentemot mottagaren.

Undertecknarens ansvar vid obehörig användning

Det kan inträffa att någon annan än den egentlige undertecknaren obehörigen använder den hemliga nyckeln och med hjälp av denna vidtar rättshandlingar i undertecknarens namn. Det betyder alltså att någon falskeligen uppträder som undertecknare. Ett sådant missbruk kan t.ex. ha möjliggjorts genom att undertecknaren handskats vårdslöst med sin säkerhetskod eller sitt smarta kort. Det kan också vara så att den elektroniska signaturen missbrukas utan undertecknarens förskyllan, t.ex. av en s.k. hacker eller av att certifikatutfärdaren lämnat ut den hemliga nyckeln till fel person.

De ansvarsfrågor som aktualiseras här regleras över huvud taget inte i direktivet. Det kan ändå finnas skäl att något behandla problemet.

Enligt svensk rätt torde som utgångspunkt gälla att undertecknaren inte blir bunden av rättshandlingar som inte har företagits av honom eller henne. I rättspraxis har man visserligen i vissa fall låtit den som åberopar ogiltigheten bli skadeståndsskyldig om han eller hon genom vårdslöshet möjliggjort förfalskningen (jfr t.ex. NJA 1935 s. 646). Huruvida en undertecknare skulle kunna bli skadeståndsskyldig enligt dessa principer om denne varit oaktsam och därigenom möjliggjort det obehöriga användandet måste dock betecknas som mycket osäkert.

Det är viktigt att komma ihåg att det alltid råder ett avtalsförhållande mellan undertecknaren och certifikatutfärdaren. Undertecknaren måste ju vända sig till certifikatutfärdaren för att få ett certifikat utfärdat. Det finns således alltid möjligheter att reglera ansvarsfrågor i avtalet mellan parterna.

De här aktuella problemen uppvisar vissa likheter med obehörig användning av kontokort. För dessa fall finns en särskild reglering i 34 § konsumentkreditlagen (1992:830). Bestämmelsen har införts för att komma till rätta med stränga avtalsvillkor rörande konsumenternas betalningsansvar vid obehöriga uttag med kontokort.

Det kan finnas skäl att överväga en särskild reglering på detta område i svensk rätt. Det kan nämnas att i den modellag för elektroniska signaturer som man för närvarande arbetar fram inom UNCITRAL (jfr modellagen för elektronisk handel, avsnitt 4.2) diskuteras just principer för undertecknarens ansvar för obehörig användning. Frågan är dock komplicerad och bör lämpligen övervägas i något annat sammanhang än vid genomförandet av direktivet.

Certifikatutfärdarens ansvar gentemot undertecknaren

Som ovan nämnts är förhållandet mellan certifikatutfärdaren och undertecknaren kontraktsrättsligt. Frågan om certifikatutfärdarens ansvar gentemot undertecknaren kompliceras dock av att det kan vara svårt att ange vad som är avtalets objekt och vilken typ av avtal det är frågan om. Den hemliga nyckeln kan vara lagrad på ett smart kort, på en hårddisk, på en diskett osv. och man kan tänka sig att certifikatutfärdaren genererar ett nyckelpar till undertecknaren.

Certifikatutfärdaren och undertecknaren kan i dag efter gottfinnande reglera relevanta frågor i avtalet såsom ansvarsgrunder, ansvarets omfattning och ansvarsbegränsningar. Avtalsfriheten begränsas ytterst av 36 § lagen (1915:218) om avtal och andra rättshandlingar på förmögenhetens område (avtalslagen). Om certifikatutfärdaren inte uppfyller sina förpliktelser enligt avtalet med undertecknaren kan ett avtalsbrott föreligga.

Förhållandet mellan certifikatutfärdaren och undertecknaren regleras i viss mån genom artikel 6 i direktivet.

Certifikatutfärdarens ansvar gentemot mottagaren

Om uppgifterna i ett certifikat är felaktiga – t.ex. eftersom certifikatutfärdaren inte har kontrollerat identiteten hos undertecknaren på det sätt som påstås i certifikatet – kan mottagaren lida en skada om denne vid en ekonomisk transaktion förlitar sig på den elektroniska signaturen. Relationen mellan certifikatutfärdaren och mottagaren kan vara av olika slag. De kan ha en kontraktsrättslig relation, men vanligen torde det inte finnas något avtal mellan dem.

När det inte finns något avtal mellan certifikatutfärdaren och mottagaren gäller utomkontraktuella regler. I utomkontraktuella förhållanden är huvudregeln att skadeståndsskyldighet för ren förmögenhetsskada (dvs. ekonomisk skada som uppkommit utan att någon lidit person- eller sak-

skada) föreligger endast om skadan orsakats genom brott. Det framgår av 2 kap. 4 § skadeståndslagen (1972:207). För att ren förmögenhetsskada skall vara ersättningsgill i andra fall krävs i princip en specialbestämmelse i lag. Av förarbetena till 2 kap. 4 § skadeståndslagen framgår dock att avsikten inte varit att lägga hinder i vägen för en rättsutveckling i praxis i riktning mot ett vidgat ansvar för ren förmögenhetsskada (jfr prop. 1972:5 s. 568). Sedan länge har också i rättspraxis skadeståndsansvar godtagits beträffande t.ex. felaktiga vederhäftighets- och vittnesintyg samt beträffande soliditetsupplysningar. Särskilt intressant i detta sammanhang är rättsfallet NJA 1987 s. 692 där en värderingsman som av oaktsamhet utfärdat ett oriktigt värderingsintyg ansågs skadeståndsskyldig gentemot en långivare som förlitat sig på intyget.

Det kan diskuteras i vilken utsträckning en mottagare kan göra gällande att en certifikatutfärdare är skadeståndsskyldig i enlighet med principerna i 1987 års fall. När certifikatutfärdaren utfärdar ett certifikat sker det normalt i syfte att tredje man skall kunna förlita sig på uppgifterna i certifikatet. Certifikatet riktar sig ju ofta just till tredje man. I så måtto finns likheter med 1987 års fall. Av betydelse är dock att målgruppen för certifikatet i regel kan vara obegränsad. Det är omöjligt för en certifikatutfärdare att överblicka de transaktioner som signaturen kommer att användas till och vem som kan förväntas förlita sig på certifikatet. I normalfallet saknar certifikatutfärdaren vetskap om för vilka ändamål signaturen kommer att användas. Så behöver dock inte vara fallet om certifikatutfärdaren har begränsat t.ex. certifikatets användningsområde. Rättsläget måste hur som helst betecknas som osäkert.

I de fall det trots allt finns ett avtal mellan certifikatutfärdaren och mottagaren är det i dag fritt för dem att sinsemellan reglera förutsättningarna för ansvar. Avtalsfriheten begränsas också här ytterst av 36 § avtalslagen. Om certifikatutfärdaren inte uppfyller sina förpliktelser enligt avtalet med mottagaren kan ett avtalsbrott föreligga.

Ansvarsförhållandet mellan certifikatutfärdaren och mottagaren regleras i artikel 6 i direktivet.

6.9.2 Genomförandet av direktivets artikel om skadestånd

Regeringens förslag: I lagen skall det föreskrivas ett skadeståndsrättsligt presumtionsansvar för den som utfärdar kvalificerade certifikat till allmänheten gentemot den som förlitar sig på certifikatet. Det skall även föreskrivas att bestämmelsen är tvingande till fördel för den som förlitar sig på certifikatet.

Promemorians förslag: Överensstämmer i huvudsak med regeringens förslag. I promemorian föreslogs dock ingen bestämmelse om att skadeståndsbestämmelsen skulle vara tvingande.

Remissinstanserna: Flertalet remissinstanser tillstyrker i huvudsak förslaget eller lämnar det utan erinran. *Konsumentverket* anser dock att det finns skäl att överväga ett strikt ansvar. *Post- och telestyrelsen* och *Juridiska fakultetsnämnden vid Uppsala universitet* menar att det bör klargöras om skadeståndsbestämmelsen är tvingande eller inte.

Ansvarets omfattning

Artikel 6 i direktivet föreskriver som ett minimikrav att medlemsstaterna skall säkerställa att de certifikatutfärdare som utfärdar certifikat som uppges vara kvalificerade eller som garanterar att någon annans certifikat är kvalificerade har ett s.k. presumtionsansvar. Det innebär att om den som förlitar sig på certifikatet lider en skada till följd av t.ex. en felaktighet i certifikatet skall certifikatutfärdaren ersätta skadan såvida inte certifikatutfärdaren kan visa att felaktigheten beror på något annat än att denne varit vårdslös. Certifikatutfärdaren skall alltså antas – presumeras – ha orsakat skadan genom vårdslöshet, men om utfärdaren lyckas bevisa att skadan inte beror på vårdslöshet på dennes sida skall utfärdaren kunna undgå skadeståndsansvar. Eftersom detta i direktivet formulerats som ett minimikrav är det möjligt för medlemsstaterna att i stället föreskriva ett strikt ansvar för certifikatutfärdaren, dvs. att denne skall vara skadeståndsskyldig oberoende av eget vållande.

Vid bestämmande av vilken omfattning certifikatutfärdarens ansvar skall ha finns flera hänsyn att ta. Det är viktigt att betona att certifikatets funktion är att skapa trygghet. Den som tar del av innehållet skall kunna förlita sig på att det är riktigt. Ett viktigt syfte med regleringen måste vidare vara att gynna förekomsten av elektroniska signaturer och certifikattjänster. Regleringen får inte riskera att i onödan hämma framväxten av certifikattjänster. Det är därvid väsentligt att komma ihåg att certifikat är något som certifikatutfärdarna normalt tar betalt för. Det vore naturligtvis olyckligt med en utveckling där certifikatutfärdarna tog så mycket betalt för certifikaten att elektroniska signaturer endast skulle komma att användas av företag och inte av privatpersoner.

En annan aspekt som inte är oväsentlig i sammanhanget är att man bör försöka uppnå nordisk rättslikhet på området. I övriga nordiska länder har man hittills planerat att genomföra direktivet så att certifikatutfärdarna åläggs ett presumtionsansvar.

Vid ett presumtionsansvar måste certifikatutfärdaren, sedan t.ex. en felaktighet i certifikatet och en därtill knuten skada för den som förlitar sig på certifikatet har konstaterats, bevisa att skadan inte uppkommit på grund av dennes vårdslöshet. Detta är rimligt eftersom certifikatutfärdaren torde ha lättast att föra fram bevisning i detta avseende. Om däremot certifikatutfärdarna skulle sakna möjlighet att visa att man vidtagit alla rimliga åtgärder för att förhindra en felaktighet skulle utvecklingen av sådana tjänster hämmas på ett olyckligt sätt. Från angivna utgångspunkter framstår enligt regeringens mening ett presumtionsansvar som det lämpligaste alternativet. Ett strikt ansvar bör därför inte föreskrivas.

Hovrätten över Skåne och Blekinge samt *Juridiska fakultetsnämnden vid Uppsala universitet* ifrågasätter betydelsen av att den skadelidande skall ha haft ”rimlig anledning” att förlita sig på certifikatet, såsom angavs i promemorians lagförslag. Hovrätten menar att begränsningen borde kunna hanteras inom adekvansbedömningen, inom läran om skyddat intresse eller med hjälp av allmänna regler om jämkning vid medvållande, med i huvudsak samma utfall som om begränsningen

uttryckligen anges i lagtexten. Hovrätten menar vidare att skyddet för den skadelidande i vart fall inte lär hamna under den miniminivå som direktivet kräver. Fakultetsnämnden anser att utgångspunkten vid tolkningen av bestämmelsen rimligen måste vara att den som förlitar sig på ett kvalificerat certifikat har alla skäl att göra det och att situationen måste vara mycket speciell för att bedömningen skall bli annorlunda. Regeringen delar remissinstansernas bedömning och föreslår därför inte att någon sådan begränsning uttryckligen anges.

Certifikatutfärdare som skall omfattas av skadeståndsregeln

Det skadeståndsansvar som föreskrivs i direktivet omfattar endast de certifikatutfärdare som antingen till allmänheten utfärdar certifikat som uppges vara kvalificerade eller som garanterar att en annan certifikatutfärdares certifikat är kvalificerade. En certifikatutfärdare som inte utger sig för att utfärda kvalificerade certifikat och som inte garanterar att någon annans certifikat är kvalificerade träffas över huvud taget inte av direktivets skadeståndsregler. Inte heller träffas sådana certifikatutfärdare som inte utfärdar certifikat till allmänheten. Frågan är om vi i Sverige nu bör införa en regel som går längre än direktivet och ålägga en skadeståndsskyldighet även för andra certifikatutfärdare. Direktivet torde inte hindra en sådan nationell lagstiftning.

Det finns bärkraftiga argument både för att utöka den krets som skall träffas av direktivets skadeståndsregler och för att inte göra det. Som nämnts ovan är det tämligen oklart vad som i dag gäller om certifikatutfärdares ansvar gentemot mottagaren enligt allmänna skadeståndsrättsliga regler, i varje fall när de inte har något avtalsförhållande med varandra, vilket torde vara det vanliga. Denna osäkerhet talar för att kretsen bör utökas i förhållande till direktivet. Det kan förutsättas att många av de certifikat som finns och kommer att finnas på marknaden i framtiden inte är kvalificerade i direktivets mening. Det kan i dessa fall finnas väl så starka skäl att ha en specialreglering för certifikatutfärdarens ansvar. Samtidigt finns det starka betänkligheter mot en utvidgad krets. Regleringen tar såvitt avser förhållandet mellan certifikatutfärdaren och mottagaren huvudsakligen sikte på skadeståndsansvar för ren förmögenhetsskada i utomobligatoriska förhållanden. På detta område präglas svensk rätt av tämligen stor restriktivitet. Om kretsen skulle utvidgas är det viktigt att den är tydligt identifierbar och definierad. Det skulle kunna föra för långt om skadeståndsansvar för rena förmögenhetsskador i utomkontraktuella förhållanden träffade alla certifikatutfärdare eller alla som i en elektronisk miljö identifierar avsändare av elektroniska meddelanden. Det är förenat med betydande svårigheter att finna tydliga avgränsningar på området. Vidare bygger direktivet till stor del på att det skapas en slags standard för elektroniska signaturer i Europa och de som baserar sig på kvalificerade certifikat ges en särställning i direktivet (jfr avsnitt 6.11). Det kan därför ses som mest förenligt med tankarna bakom direktivet att begränsa skadeståndsregleringen till de fall certifikatutfärdaren anger att han utfärdar kvalificerade certifikat eller som garanterar att någon annans certifikat är kvalificerade. De som förlitar sig på certifikaten får därmed också en tydlig signal om de kvalificerade certifi-

katens särskilda kvalitéer. Samtidigt undviker man att förena certifikat som avses att användas på ett sätt som inte kräver så hög säkerhet med avskräckande höga kostnader.

Övervägande skäl talar därför för att inte utvidga den krets som träffas av direktivets skadeståndsregler. I sammanhanget kan nämnas att man hittills planerat att lösa frågan på samma sätt i övriga nordiska länder. En jämförelse med övriga nordiska länder i detta avseende haltar dock eftersom vi har delvis olika regler om ansvar för ren förmögenhetsskada utanför kontraktsförhållanden.

Reglernas utformning

Artikel 6.1 i direktivet föreskriver att certifikatutfärdare som utfärdar påstått kvalificerade certifikat till allmänheten eller som garanterar att någon annans certifikat är kvalificerade har ett skadeståndsrättsligt presumtionsansvar för att uppgifterna i ett certifikatet är korrekta och fullständiga, att undertecknaren vid tidpunkten för utfärdandet var i besittning av de signaturframställningsdata som motsvarar de signaturverifieringsdata som anges i certifikatet samt att signaturframställningsdata och signaturverifieringsdata kan användas som komplement till varandra om certifikatutfärdaren framställer båda. Vidare har certifikatutfärdare som utfärdar sådana certifikat enligt artikel 6.2 ett presumtionsansvar för skada som genom underlåtenhet att registrera ett återkallande av ett certifikat åsamkats den som förlitat sig på certifikatet.

De i lagen ställda kraven på kvalificerade certifikat och den som utfärdar sådana till allmänheten (se avsnitt 6.5) kan utformas bl.a. som handlingsregler för certifikatutfärdaren, som motsvarar vad certifikatutfärdaren enligt direktivet skall ha ett skadeståndsrättsligt presumtionsansvar för. Skadeståndsreglerna i lagen kan då lämpligen utformas så att certifikatutfärdaren bär det särskilda skadeståndsansvaret om uppgifterna i ett certifikat som anges vara kvalificerat är felaktiga eller ofullständiga, eller certifikatutfärdaren inte har uppfyllt vissa handlingsregler.

Artikel 6 stadgar också att medlemsstaterna skall föreskriva att en certifikatutfärdare får ange begränsningar för områden eller transaktionsbelopp som certifikatet får användas för samt att certifikatutfärdaren inte skall vara ansvarig för skador som härrör från ett överskridande av dessa begränsningar. Även detta bör anges i lagtexten.

Några remissinstanser menar att promemorians lagförslag är otydligt i fråga om vilka certifikatutfärdare som omfattas av skadeståndsbestämmelsen. Såsom framgått ovan omfattas bara sådana certifikatutfärdare som utfärdar påstått kvalificerade certifikat till allmänheten. Certifikatutfärdare som garanterar att någon annans certifikat är kvalificerade omfattas av bestämmelsen i den mån certifikaten inte uppfyller kraven i 3 § eller innehåller felaktiga uppgifter (första stycket 2 och 3). Dessa s.k. certifikatgaranter åläggs dock inte något skadeståndsansvar för någon annan certifikatutfärdares underlåtenhet att uppfylla kraven i 9 § (första stycket 1). Detta har förtydligats i regeringens förslag, bl.a. genom att sammanfoga 13 och 14 §§ och genom det tillagda andra stycket i 13 §.

Post- och telestyrelsen och *Juridiska fakultetsnämnden vid Uppsala universitet* menar att det bör klargöras om rätten till skadestånd är tving-

ande eller om certifikatutfärdaren i avtal kan friskriva sig från ansvar i förhållande till sådana personer som är kunder till certifikatutfärdaren. De anför att om regeln är avsedd att vara tvingande, bör detta anges uttryckligen i lagen. Fakultetsnämnden menar att en tvingande regel torde stämma bäst överens med formuleringen av ingressen till artikel 6 i direktivet och att det vore det lämpligaste alternativet. Regeringen delar den uppfattningen och föreslår därför en särskild bestämmelse som klargör detta. Bestämmelsen bör utformas i enlighet med motsvarande bestämmelser i konsumentlagstiftningen.

6.10 Behandling av personuppgifter

Regeringens förslag: I lagen skall det anges begränsningar för hur den som utfärdar certifikat till allmänheten får behandla personuppgifter.

Promemorians förslag: Överensstämmer med regeringens förslag.

Remissinstanserna: Remissinstanserna tillstyrker förslaget eller lämnar det utan erinran.

Skälen för regeringens förslag: Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter har genomförts i svensk rätt genom personuppgiftslagen (1998:204). Lagen innehåller bestämmelser om när behandling av personuppgifter är tillåten.

Enligt lagen gäller bl.a. följande. Personuppgifter får behandlas (inkluderande insamlas) bara om den registrerade har lämnat sitt samtycke till behandlingen, eller om behandlingen är nödvändig av vissa närmare angivna skäl. Personuppgifter som samlats in för ett ändamål får inte behandlas för något annat oförenligt ändamål. Fler personuppgifter än som är nödvändiga med hänsyn till ändamålet får inte behandlas.

Personuppgiftslagen är tillämplig på certifikatutfärdare, SWEDAC och tillsynsmyndigheten, utan att detta särskilt behöver anges. Artikel 8.2 i direktivet innehåller dock regler som innebär strängare krav än de som uppställs i personuppgiftslagen. Det skall därför i den föreslagna lagen införas en regel om att certifikatutfärdare som utfärdar certifikat till allmänheten endast under dessa strängare förutsättningar får behandla personuppgifter. Regeln skall inte vara begränsad till dem som utfärdar kvalificerade certifikat.

Regeringens förslag: Lagen skall innehålla en regel som anger de kvalificerade elektroniska signaturernas särställning. Regeln innebär att om det i lag eller annan författning ställs krav på egenhändig underskrift eller motsvarande och om det är tillåtet att uppfylla kravet med elektroniska medel, skall en kvalificerad elektronisk signatur alltid anses uppfylla kravet. Användningen av elektroniska signaturer inom eller vid kommunikation med myndigheter skall dock kunna vara förenad med ytterligare krav.

Promemorians förslag: Överensstämmer med regeringens förslag. I promemorian föreslogs dock ingen särskild bestämmelse om användningen av elektroniska signaturer inom eller vid kommunikation med myndigheter..

Remissinstanserna: Flertalet remissinstanser tillstyrker eller har ingen invändning mot att bestämmelsen införs, men menar att formuleringen i promemorians förslag är otydlig. *Hovrätten över Skåne och Blekinge*, *Statskontoret*, *Juridiska institutionen vid Göteborgs universitet*, *IT-kommissionen* och *Lagerlöf & Leman* ifrågasätter dock om bestämmelsen fyller någon praktisk funktion och om den inte borde utgå. Flera remissinstanser invänder att bestämmelsens rubrik kan leda till missförstånd om vad bestämmelsen egentligen innebär. *Riksarkivet, Patent- och registreringsverket, Riksskatteverket, Statskontoret* och *Lagerlöf & Leman* menar att det, i vart fall tills vidare, måste finnas vissa möjligheter att ställa ytterligare krav på användningen av elektroniska signaturer inom offentlig sektor.

Skälen för regeringens förslag

Bakgrund

Som tidigare nämnts finns det en mängd författningar som ställer krav på underskrift för att en rättshandling skall anses giltig eller en åtgärd anses vidtagen etc. I svensk rätt finns dock inga regler som anger hur ett författningsenligt krav på underskrift skall uppfyllas. Det sägs ingenstans att underskriften skall vara läslig på det sättet att personens namn kan utläsas av underskriften. Det sägs vidare inget om att personen skall använda sitt fulla namn eller sina initialer eller enbart ett bomärke eller kryss. Kravet på underskrift uttrycks också på olika sätt i skilda författningar. Exempelvis krävs det i vissa författningar ”underskrift” medan det i andra författningar krävs ”namnunderskrift”. Även om det saknas regler om vad som krävs för att uppfylla ett formkrav på underskrift måste det åtminstone i vissa situationer finnas en gräns för vad som kan godtas när det ställs ett sådant krav. Någon form av angivelse om vem som avses med underskriften torde krävas. Är det en skrivkunnig person kan det möjligen krävas att det är ett allvarligt försök att forma namnet i skrift. I vissa situationer torde därför inte vilket avtryck som helst från exempelvis en penna anses konstituera en underskrift eller namn-

underskrift. Frågan har nog tämligen sällan ställts på sin spets eller vållat några problem.

När det gäller elektroniska signaturer förhåller det sig något annorlunda. Den som förlitar sig på en elektronisk signatur ser inte tekniken i systemet och hur kontrollen går till. I princip får de mottagare som förlitar sig på en elektronisk signatur endast ett meddelande på sin dator om att identitet och innehåll stämmer eller inte stämmer. Som tidigare nämnts bygger direktivet på elektroniska signaturer enligt det s.k. öppna nyckelsystemet. Även om detta koncept har en viss given struktur kan tekniken ha olika hög säkerhetsnivå.

I artikel 5.1 beskrivs en typ av elektroniska signaturer med särskilt hög säkerhetsnivå, i den föreslagna lagen benämnda kvalificerade elektroniska signaturer.

Enligt artikel 5.1.a skall medlemsländerna säkerställa att dessa kvalificerade elektroniska signaturer ”uppfyller de rättsliga kraven på en signatur i förhållande till uppgifter i elektronisk form, på samma sätt som en handskriven signatur uppfyller samma krav i förhållande till uppgifter på papper”. Medlemsstaterna är vidare enligt artikel 5.1.b skyldiga att se till att kvalificerade signaturer godtas som bevis vid rättsliga förfaranden. I artikel 5.2 sägs att medlemsstaterna skall se till att inga elektroniska signaturer förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på vissa särskilt angivna grunder. Frågan är vad artikel 5 egentligen innebär och om det krävs några åtgärder för att svensk rätt skall leva upp till direktivet i denna del.

Innebörden av artikel 5 i direktivet

Finansbolagens förening och *Svenska Inkassoföreningen* menar att innebörden av artikel 5 är att verkan av en elektronisk signatur måste jämställas med verkan av en egenhändig namnteckning. De menar därför att direktivet på denna punkt är mer långtgående än promemorians förslag. Enligt regeringens mening kan dock artikeln inte läsas och tolkas isolerat från övriga artiklar i direktivet. Av särskild betydelse för hur artikel 5 skall uppfattas är artikel 1 i direktivet som reglerar direktivets tillämpningsområde.

Av artikel 1 framgår att syftet med direktivet är att underlätta användningen av elektroniska signaturer och bidra till deras rättsliga erkännande. Av artikeln framgår vidare att direktivet inte omfattar frågor som avser ingående eller giltighet av avtal eller andra rättsliga förpliktelser, om den nationella lagstiftningen eller gemenskapslagstiftningen föreskriver vissa formkrav. Direktivet påverkar inte heller bestämmelser och begränsningar i nationell lagstiftning eller gemenskapslagstiftning som reglerar användningen av dokument.

Enligt regeringens uppfattning är det sålunda klart att direktivet inte inom något rättsområde föreskriver att elektronisk kommunikation *måste* accepteras. Vidare innebär artikel 1 enligt regeringens bedömning att direktivet inte på något rättsområde förbjuder medlemsstaterna att ha formkrav på egenhändiga namnunderskrifter som utesluter användning av elektroniska signaturer. Flertalet remissinstanser synes dela den bedömningen.

Innebörden av artikel 5.1.a kan därför inte vara att medlemsstaterna måste godta kvalificerade elektroniska signaturer i alla de fall där det finns ett krav på underskrift i nationell rätt eller gemenskapsrätt. Därför måste artikel 5.1.a uppfattas så att *om* det enligt nationell rätt – antingen på grund av lagstiftning eller andra föreskrifter eller på grund av tolkning av formkravsregler – över huvud taget är tillåtet att uppfylla ett formkrav på traditionell underskrift e.d. med elektroniska rutiner, måste de kvalificerade elektroniska signaturerna alltid godtas. På detta sätt skapas inom hela gemenskapen en standard för elektroniska signaturer, vilket kan vara gynnsamt för den inre marknaden. Därför bör det i den svenska lagen införas en bestämmelse som klargör detta förhållande.

När det gäller artikel 5.1.b – dvs. att kvalificerade elektroniska signaturer skall godtas som bevis vid rättsliga förfaranden – behövs knappast några lagstiftningsåtgärder. Av principen om den fria bevisprövningen som gäller i Sverige följer att det inte finns något hinder mot att använda vissa kunskapskällor eller medier som bevisning. Något hinder mot att använda elektroniska signaturer som bevis finns således inte.

I artikel 5.2 ges regler för alla slags elektroniska signaturer, dvs. inte enbart de som är kvalificerade. Där sägs att medlemsstaterna skall se till att en elektronisk signatur inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på den grunden att signaturen

– är i elektronisk form,

– inte är baserad på ett kvalificerat certifikat,

– inte är baserad på ett kvalificerat certifikat utfärdat av en ackrediterad tillhandahållare av certifikattjänster, eller

– inte är skapad av en säker anordning för skapande av signaturer.

När det gäller kravet att elektroniska signaturer inte får förvägras giltighet som bevis vid rättsliga förfaranden på grund av skäl som anges i artikel 5.2 innebär det med hänvisning till principen om den fria bevisprövningen inga problem för svensk del. Några lagstiftningsåtgärder krävs inte för att genomföra direktivet i denna del. Frågan är dock vad artikeln kan innebära för svensk del när det gäller kravet att en elektronisk signatur inte får förvägras rättslig verkan.

Lika lite som artikel 5.1 kan denna bestämmelse anses innebära att medlemsstaterna måste se till att en elektronisk signatur över huvud taget skall kunna användas för att uppfylla formkrav som finns i nationell lagstiftning. Det följer som tidigare nämnts redan av artikel 1.

Till skillnad från artikel 5.1 har inte artikel 5.2 någon hänvisning till ”handskrivna signaturer på papper”. Det sägs bara att elektroniska signaturer inte får förvägras rättslig verkan på grund av omständigheter som där anges. I svensk rätt finns inte några regler som kan sägas förvägra elektroniska signaturer rättslig verkan över huvud taget. Visserligen kan det finnas formkrav för rättshandlingar som utesluter användning av elektroniska signaturer, men detta är tillåtet enligt artikel 1. Vidare är det enbart kvalificerade elektroniska signaturer som måste anses uppfylla kraven på en handskriven underskrift när man i nationell rätt gör en sådan jämställelse. Artikel 5.2 torde därför inte kräva några lagstiftningsåtgärder i Sverige. Regeringens slutsats är alltså att det endast är artikel 5.1.a som kräver någon lagstiftningsåtgärd i svensk rätt.

Som framgått finns det ett antal formkravsregler i svensk rätt som innebär krav på underskrift, egenhändig namnunderskrift eller liknande. Dessa regler finns främst inom förvaltningsrätten, men det finns också ett begränsat antal sådana regler inom förmögenhets- och familjerätten. Reglerna kan i flera fall antas utesluta elektroniska rutiner eller i vart fall föranleda tveksamhet om sådana rutiner är tillåtna. Angående innebörden av krav på ”skriftlighet”, se prop. 1999/2000:89, s. 91, avsnitt 5.3 och 5.4 i SOU 1996:40 samt lagkommentaren till 11 §.

I denna situation bör utgångspunkten vara att det inte bör finnas otidsenliga formkrav som på ett onödigt sätt hindrar elektronisk kommunikation. I det förslag till direktiv om elektronisk handel som kommissionen lagt fram, och som rådet den 28 februari 2000 antog en gemensam ståndpunkt om, krävs att medlemsstaterna ser till att de rättsliga krav som är tillämpliga på avtalsprocessen inte skapar hinder för att träffa avtal i elektronisk form (artikel 9). Om direktivet antas i den delen kommer det att innebära att de krav på underskrift o.d. som finns på civilrättens område måste ses över och att en del av dessa krav kan behöva avskaffas. Någon generell regel i svensk lagstiftning som likställer vissa typer av elektroniska signaturer med egenhändiga namnunderskrifter torde dock inte vara möjlig (se avsnitt 9 i promemorian).

När artikel 5 genomförs i svensk rätt bör man därför inte generellt jämställa vissa elektroniska signaturer med egenhändiga namnunderskrifter i de författningar där det finns formkrav som kräver underskrifter. I stället bör det införas en regel som anger de kvalificerade elektroniska signaturernas särställning, i de fall det i lag eller andra författningar finns formkrav som får uppfyllas med hjälp av elektroniska signaturer. Det innebär alltså att det fortfarande är tillåtet att ha kvar formkrav som förhindrar användningen av elektroniska signaturer. I vissa fall kan dock tänkas att det, uttryckligen eller p.g.a. praxis, är eller kan bli tillåtet att uppfylla t.ex. krav på egenhändig namnunderskrift genom elektroniska rutiner. I sådana fall måste alltid en kvalificerad elektronisk signatur accepteras. Det kan också i vissa bestämmelser uttryckligen ställas krav på att en elektronisk signatur skall användas. Även i de fallen måste en kvalificerad elektronisk signatur godtas.

Den föreslagna bestämmelsen innebär alltså att det inte får ställas högre krav på en elektronisk signatur än vad som ställs på en kvalificerad elektronisk signatur. Såsom flera remissinstanser påpekar är det dock i många situationer fullt tillräckligt med en elektronisk signatur med en *lägre* säkerhetsnivå. Bestämmelsen hindrar inte på något sätt att även sådana elektroniska signaturer kan godtas. Det är tvärtom naturligt att olika slags elektroniska signaturer med olika säkerhetsnivå utvecklas och accepteras beroende på i vilket syfte de används.

Flertalet remissinstanser menar att den åsyftade innebörden av bestämmelsen inte framgår av promemorians förslag. Regeringen föreslår därför att bestämmelsen omformuleras i förhållande till promemorians förslag.

Bestämmelsen utgör självfallet inget hinder mot att ifrågasätta signaturens härkomst, dvs. om det är rätt person som ligger bakom signaturen.

Liksom vid användning av traditionella egenhändiga namnunderskrifter kan alltid härkomsten ifrågasättas om det finns anledning till det.

Lagrådet har föreslagit att bestämmelsens rubrik bör lyda ”Användningen av elektroniska signaturer i vissa fall”. Med hänsyn till att bestämmelsen dels endast avser kvalificerade elektroniska signaturer och inte elektroniska signaturer i allmänhet, dels inte rör användningen endast i vissa fall menar regeringen dock att en sådan rubrik skulle riskera att bli missvisande. Regeringen har därför inte följt Lagrådets förslag i denna del.

Användning av elektroniska signaturer vid kommunikation med myndigheter

I direktivets artikel 3.7 anges 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.

Inom den offentliga sektorn är det tänkbart att problem kan uppstå bl.a. om en myndighet inte har utrustning som kan tyda ett elektroniskt meddelande, om avsändaren eller innehållet efter en viss tid inte längre kan verifieras, om meddelandena inte är tidsstämplade eller om de inte kan arkiveras på det sätt som önskas.

Vissa typer av uppgifter, såsom tull- och inkomstdeklarationer, får i dag lämnas elektroniskt, men endast efter särskilt medgivande av respektive myndighet. Medgivandena kan då förenas med villkor om bl.a. det tekniska förfarandet för uppgiftslämnandet. Bland andra *Riksarkivet*, *Riksskatteverket* och *Patent- och registreringsverket* uttrycker viss oro för att den föreslagna 16 § skall hindra dem från att uppställa sådana villkor. De krav som ställs kan avse t.ex. tekniska beskrivningar över filinnehåll, format och adressering. Syftet med sådana krav kan vara att deklarationsuppgifter skall inges på ett enhetligt och kontrollerat sätt och att den elektroniska kommunikationen inte skall försvåra långtidslagring. *Lagerlöf & Leman* menar att bestämmelsen i 16 § torde få den effekten att hårt särreglerade myndigheter, som t.ex. tullen och skatteförvaltningen, skulle bli skyldiga att godta vilka kvalificerade signaturer som helst, även om myndigheten saknar utrustning för att hantera och lagra dem och även om de inte är kompatibla med myndighetens informationssystem. Lagerlöf & Leman menar vidare att detta riskerar att leda till att myndigheter ifrågasätter ett införande av IT, i stället för att stödja en utveckling mot elektroniska signaturer.

I den mån de krav som ställs inte utgör högre krav på den elektroniska signaturen än vad som krävs för att en signatur skall anses vara kvalificerad, så hindrar bestämmelsen inte att sådana krav ställs. Frågan om ett visst krav utgör ett krav på själva signaturen eller ett krav på något annat är dock inte helt lätt att besvara. Det torde finnas situationer där det är svårt att skilja mellan krav på själva signaturen och krav på den handling eller de data som signeras. Det är i detta sammanhang viktigt att beakta betydelsen av de tekniska formaten på dokument som signeras.

Regeringen gav den 23 juni 1999 i uppdrag åt Statskontoret att utreda behoven av åtgärder för att tillgodose kraven på säker elektronisk överföring av dokument och meddelanden till, från och inom statsförvalt-

ningen. En delrapport lämnades till regeringen den 2 februari 2000 (Statskontoret 2000:7). Statskontoret skall i det fortsatta arbetet närmare utreda frågor som rör bevarande av signerad information. Statskontoret skall därför – i samverkan med Riksskatteverket, Riksförsäkringsverket, Patent- och registreringsverket och Riksarkivet – närmare utreda detaljerna i de krav som bör ställas på en elektronisk signatur som kan accepteras i offentlig sektor. Arbetet skall redovisas för regeringen senast den 20 december 2000.

Med hänsyn till de möjliga problem som remissinstanserna pekar på och till att det fortfarande är oklart i vilken mån det kan finnas behov av att ställa ytterligare krav på elektroniska signaturer inom och vid kommunikation med myndigheter, föreslår regeringen att användningen av elektroniska signaturer skall kunna vara förenad med ytterligare krav. Vid avgörandet av om det på ett visst område eller i vissa sammanhang är nödvändigt att ställa högre krav bör utgångspunkten vara att kvalificerade elektroniska signaturer i normalfallet skall vara tillräckligt säkra för att kunna godtas. Endast om det kan pekas på särskilda problem eller behov bör bedömningen bli en annan. Genom den föreslagna bestämmelsen uppställs alltså en standard som innebär att kvalificerade elektroniska signaturer alltid måste godtas, så länge det inte på ett visst område uttryckligen ställs ytterligare krav på signaturen.

Enligt artikel 11.1.a i direktivet skall alla ytterligare krav som ställs anmälas till kommissionen och till de övriga medlemsstaterna.

En mer ingående diskussion om arkivfrågor återfinns i betänkandet Elektronisk dokumenthantering (SOU 1996:40, avsnitt 6.4) och i promemorian Digitala signaturer (Ds 1998:14, avsnitt 7.1.5.2).

6.12 Tillsyn

Regeringens förslag: En tillsynsmyndighet skall utöva tillsyn över efterlevnaden av denna lag och föreskrifter som har meddelats med stöd av lagen.

Promemorians förslag: Överensstämmer i huvudsak med regeringens förslag.

Remissinstanserna: Remissinstanserna tillstyrker förslaget eller lämnar det utan erinran.

Skälen för regeringens förslag

Direktivets förbud mot förhandstillstånd

Utgångspunkten i direktivet är att det inte får införas några krav på förhandstillstånd för att få verka som certifikatutfärdare. Frivilliga ackrediteringssystem får däremot förekomma. Samtidigt är medlemsstaterna skyldiga att införa ett system för övervakning av certifikatutfärdare. Kravet på övervakning begränsas till de certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten. Direktivet ger dock ingen möj-

lighet att begränsa övervakningen endast till dem som är ackrediterade eller certifierade. Det är således inte möjligt att tillfredsställa kravet på övervakning genom att nöja sig med den övervakning som utförs av ackrediterings- och certifieringsorgan. Däremot kommer naturligtvis tillsynsuppgifterna att i hög grad underlättas om ett system med frivillig ackreditering av aktörerna på marknaden får genomslag.

I den svenska diskussionen har ibland möjligheten och behovet av en s.k. toppnod förts fram. En sådan utgörs, förenklat beskrivet, av en (ev. statlig) certifikatutfärdare som utfärdar certifikat för andra certifikatutfärdare och signerar deras öppna nycklar. I ett sådant system skulle toppnoden på ett effektivt sätt kunna utöva tillsyn över anslutna certifikatutfärdare.

Direktivets regel om förbud mot förhandstillstånd innebär dock att man inte kan kräva att alla certifikatutfärdare som utfärdar kvalificerade certifikat skall ansluta sig till en toppnod och få sina öppna nycklar signerade av denne. Detta krav innebär ju att en certifikatutfärdare inte kan verka på marknaden utan att ansluta sig till toppnoden, vilket är att jämställa med ett krav på förhandstillstånd. Ett sådant krav innebär vidare att certifikatutfärdaren måste anpassa sina tekniska lösningar till toppnoden för att kunna verka i dess underliggande struktur. Detta strider mot direktivets strävan mot teknikneutralitet, vilket innebär att direktivets krav skall kunna uppfyllas på flera olika sätt med hjälp av olika typer av teknik.

Omfattningen av tillsynen

Anledning saknas att gå längre än direktivet och låta en tillsyn omfatta även de certifikatutfärdare som inte utfärdar certifikat till allmänheten. Ingenting hindrar emellertid att man i den svenska lagstiftningen föreskriver att övervakningen inte skall begränsas till att gälla dem som utfärdar kvalificerade certifikat, utan omfatta alla som utfärdar certifikat till allmänheten. Detta skulle dock kunna leda till att marknaden påverkas negativt. Det ekonomiska värdet av elektroniska signaturer ligger inte främst i utfärdande av certifikat, utan i en ökad säkerhet för undertecknaren och mottagaren av det signerade meddelandet (parterna). Det är därför viktigt att det finns en hög grad av valfrihet på marknaden så att parterna kan välja den form av certifikat som passar för olika typer av transaktioner. En transaktion som rör högre värden och där man önskar hög säkerhet kan motivera användandet av ett kvalificerat certifikat (eller ett certifikat med ännu högre säkerhet), även om detta leder till en viss kostnad för parterna. För många fall kan emellertid förutses att signaturer används på en marknad för masstransaktioner med lågt värde. Obligatoriska krav och en obligatorisk tillsyn av alla certifikatutfärdare skulle kunna innebära en alltför hög kostnad för certifikaten. Detta skulle i sin tur leda till att parterna väljer andra, mindre säkra lösningar, eller avstår från elektronisk kommunikation. Det finns därför inte anledning att gå längre vad gäller tillsyn än vad direktivet kräver.

I promemorian föreslogs att det skulle anges att tillsynsmyndigheten skall ha tillsyn över vissa certifikatutfärdare och anordningar för signaturframställning. På inrådan från *Lagrådet* föreslår regeringen dock att det i stället, som brukligt, anges att tillsynsmyndigheten skall ha

tillsyn över efterlevnaden av denna lag och föreskrifter som har utfärdats med stöd av lagen.

Formen för tillsynen

För den som vill uppträda som certifikatutfärdare är det helt avgörande att han bygger upp en tillit till sina certifikat. Utan det förtroendet finns inget användningsområde för de elektroniska signaturer som är baserade på hans certifikat. Detta talar för att marknaden i hög grad kommer att reglera sig själv. Samtidigt kan det för tilliten till systemet i sin helhet vara värdefullt med en instans som kan ingripa mot missförhållanden. För att denna tillsyn skall ha något reellt innehåll bör instansen ha möjlighet till myndighetsutövning. Detta, i kombination med berättigade krav på insyn, rättssäkerhet, möjlighet till överprövning etc. talar för att övervakningen bör anförtros en statlig myndighet, även om direktivet ger en möjlighet till att låta övervakningen skötas av en privat institution. Frågan om vilken myndighet som skall utses diskuteras i avsnitt 7.

Den tillsyn som utövas bör vara så marknadsorienterad som möjligt. Med hänsyn till att verksamheten för en certifikatutfärdare är beroende av att det finns ett förtroende för certifikaten, kan tillsynssystemet utformas så att det inte lägger några onödiga administrativa bördor på certifikatutfärdaren, utan inriktas på att vid klagomål kontrollera en utfärdare närmare.

Regeringen har övervägt en mer ambitiös övervakningsmodell, som bl.a. skulle innefatta ett krav på certifikatutfärdaren att till tillsynsmyndigheten ge in ett ”certifikatsprogram”. Där skulle certifikatutfärdaren utförligt redogöra för hur han uppfyller kraven i lagstiftningen/direktivet. Detta program skulle ges in i samband med att verksamheten startade och därefter en gång per år. Detta system skulle möjligen, beroende på hur hårt tillsynsmyndigheten kan ingripa vid ett uteblivet program, kunna förenas med förbudet mot förhandstillstånd. Mer tveksamt är det dock med den tungrodda och kostsamma apparat detta skulle innebära, i viss mån för myndigheten men framförallt för certifikatutfärdaren. Det skulle stå i kontrast till de mer marknadsorienterade system som övervägs i andra länder.

Det får anses vara önskvärt att marknaden i så stor omfattning som möjligt begagnar sig av de kvalificerade certifikat som direktivet etablerar. Ett gemensamt europeiskt och i bästa fall globalt användande av dessa certifikat skulle leda till en allmän acceptans och förtroende för de signaturer som baseras på sådana certifikat, vilket skulle vara till fördel för elektronisk handel och andra användningsområden. För den certifikatutfärdare som önskar undgå den tillsyn som direktivet och lagen stipulerar kan det emellertid vara frestande att inte kalla sina certifikat för kvalificerade, trots att de uppfyller kraven i lagen. Om certifikatutfärdaren kan bygga upp ett förtroende för sina certifikat i alla fall, finns kanske inget behov av att kalla certifikaten kvalificerade. Stora administrativa krav på den som utfärdar kvalificerade certifikat till allmänheten skulle förstärka en sådan utveckling. Det skulle också kunna förhindra framväxandet av öppna system.

Slutsatsen av detta resonemang är att det bör införas ett tillsynssystem i statlig regi, men där tillsynen är marknadsorienterad och inte innebär en tung administration för dem som uppträder på marknaden.

Tillsynsmyndighetens befogenheter m.m.

En grundläggande förutsättning för att kunna utöva tillsyn är att veta vem som skall kontrolleras. Certifikatutfärdare som avser att utfärda kvalificerade certifikat till allmänheten bör därför i samband med att de startar verksamheten vara skyldiga att anmäla till tillsynsmyndigheten att så sker. Detta står inte i strid med förbudet mot förhandstillstånd.

Med utgångspunkt från den kravkatalog som ställs upp i lagen för certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten blir myndighetens uppgift att ingripa mot dem som inte uppfyller kraven. Myndigheten bör därvid ha befogenhet att kräva in de handlingar och upplysningar som behövs för tillsynen. Om anmälningspliktig verksamhet bedrivs utan att anmälan skett eller brister i verksamheten upptäcks bör myndigheten kunna utfärda förelägganden om rättelser. Dessa förelägganden bör också kunna förenas med vite. Till slut bör tillsynsmyndigheten, om inte föreläggande räcker, kunna förbjuda den som begår upprepade eller allvarligare överträdelser att utfärda certifikat till allmänheten som anges vara kvalificerade.

Myndighetens befogenheter får dock inte utövas på ett sådant sätt att de i praktiken utgör ett hinder för att ta sig in på marknaden och därmed liknar ett krav på förhandstillstånd. Ett gradvis upptrappat användande av förelägganden, så småningom förenade med vite torde dock inte anses utgöra sådana hinder. Vid någon tidpunkt måste det också anses rimligt att tvinga en certifikatutfärdare att upphöra med sin verksamhet, om denne t.ex. på ett flagrant sätt nonchalerar lagens krav eller efter upprepade förelägganden underlåter att följa dessa. Avgörande för om åtgärderna kan anses vara förenliga med direktivets förbud mot hinder som liknar krav på förhandstillstånd torde vara att det föreligger proportionalitet mellan överträdelserna och åtgärderna.

Tillsyn – certifiering

Tillsynen kan i praktiken utformas som stickprovskontroller och undersökningar sedan någon anmält misstänkta felaktigheter hos en certifikatutfärdare. I den mån en certifikatutfärdare valt att certifiera sin organisation eller sina produkter mot en vedertagen standard kan myndigheten i stor utsträckning nöja sig med den kontroll som certifieringen innebär. I det praktiska tillsynsarbetet kan myndigheten också använda sig av accepterade standarder för att jämföra om de tekniska lösningarna eller organisationen uppfyller föreskrivna krav. Det är dock väsentligt att myndigheten inte binder sig vid någon särskild teknik. Även system som inte ansluter sig till någon standard kan mycket väl uppfylla de krav på säkerhet m.m. som uppställs i lagstiftningen.

Reglerna i lagen om att anordningar som anges vara säkra anordningar för signaturframställning får släppas ut på marknaden eller användas endast om vissa organ bedömt att de överensstämmer med lagens krav (se avsnitt 6.8) innebär att tillsynsmyndigheten också har att utöva viss marknadskontroll.

7 Val av tillsynsmyndighet

Regeringens bedömning: Post- och telestyrelsen bör utses till tillsynsmyndighet.

Promemorians bedömning: Överensstämmer med regeringens bedömning.

Remissinstanserna: Flertalet remissinstanser delar bedömningen att Post- och telestyrelsen bör utses till tillsynsmyndighet. *Industriförbundet, Svensk Handel, Göteborgs universitet, Lagerlöf & Leman* och *IT-företagen* anser dock att Styrelsen för ackreditering och teknisk kontroll (SWEDAC) eller Finansinspektionen vore lämpligare. *IT-kommissionen* menar att Patent- och registreringsverket är mest lämpligt. Ingen remissinstans har förordat att en ny myndighet skall inrättas. *Post- och telestyrelsen* har ställt sig positiv till att utses till tillsynsmyndighet. Varken *SWEDAC, Finansinspektionen* eller *Patent- och registreringsverket* har haft någon erinran mot detta.

Skälen för regeringens bedömning

Som framgår av avsnitt 6.12 föreslår regeringen att direktivets krav på ett lämpligt system för övervakning av certifikatutfärdare skall genomföras genom att en statlig myndighet ges i uppdrag att utöva tillsyn. Vilken myndighet som skall utses till tillsynsmyndighet ankommer på regeringen att bedöma. Regeringen finner det dock lämpligt att för riksdagens information här avge sin syn på detta.

En möjlighet vore att inrätta en ny myndighet för den aktuella tillsynsuppgiften. Certifikatutfärdande för elektroniska signaturer är en ny verksamhet som för närvarande inte omfattas av den tillsyn som finns inom förvaltningen. En sådan myndighet skulle även kunna ta hand om andra uppgifter inom området för informationssäkerhet, som nu är spridda på flera myndigheter. Mot detta talar att kompetens på området redan har byggts upp inom dessa myndigheter. Det går vidare i dag inte att överblicka vilken omfattning tillsynsarbetet kommer att få. Det troliga är dock att det kommer att innebära en tämligen begränsad uppgift, som inte motiverar inrättandet av en ny myndighet. Ingen remissinstans har heller förordat en sådan lösning. Det lämpliga är därför att lägga uppgiften på en befintlig myndighet.

I promemorian föreslogs att Post- och telestyrelsen skulle utses till tillsynsmyndighet. Flertalet remissinstanser delar den bedömningen.

Några förordar dock i stället att SWEDAC, Finansinspektionen eller Patent- och registeringsverket utses.

Vid valet av myndighet bör bl.a. myndighetens vana vid hantering av tillsynsärenden och dess IT-kompetens beaktas. Vidare krävs en analys av myndighetens instruktion och karaktär. Se avsnitt 7 i promemorian där olika myndigheters uppgifter och verksamhet beskrivs.

Val av myndighet

Tillsynsmyndigheten skall kontrollera att de certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten uppfyller lagens krav, innebärande bl.a. att de bedriver verksamheten med den pålitlighet som krävs och att de kvalificerade certifikaten innehåller de uppgifter som stadgas i lagen. Myndigheten skall också ingripa mot den som betecknar ett certifikat som utfärdas till allmänheten som kvalificerat, utan att de förutsättningar som ges i lagen är uppfyllda samt utöva marknadskontroll beträffande säkra anordningar för signaturframställning.

Ingen av de ovan nämnda myndigheterna besitter idag helt den kompetens som krävs för att utföra de aktuella tillsynsuppgifterna. En förutsättning är att kompetens tillförs verksamheten och att kunskap byggs upp inom den myndighet som utses för ändamålet.

Patent- och registreringsverket är främst en registreringsmyndighet och har idag inga sedvanliga tillsynsuppgifter. Att utöva tillsyn över certifikatutfärdare ligger långt ifrån verkets nuvarande myndighetsuppgifter.

Finansinspektionen är en utpräglad tillstånds- och tillsynsmyndighet som verkar på ett område som kännetecknas av en mycket hög IT-användning. Tillsynen i fråga gäller dock verksamhet på ett vidare område än enbart den finansiella sektorn.

SWEDAC:s huvuduppgift att ackreditera bl.a. certifieringsorgan innebär kontroll och tillsyn av de ackrediterade organen. Såsom några remissinstanser anför kan praktiska skäl tala för att samma myndighet bör ansvara för tillsyn både över certifieringsorganen och över certifikatutfärdarna, såväl certifierade som icke certifierade. Kontrollen kan i praktiken komma att vila på internationella standarder som SWEDAC kan vara väl förtrogen med. Såsom flera andra remissinstanser påpekar skulle detta dock innebära en dubbelroll för SWEDAC, som enligt regeringens mening vore olämplig. SWEDAC skulle utöva tillsyn över certifikatutfärdare som är bedömda av organ som SWEDAC ackrediterat, dvs. bedömt som kompetenta. En liknande dubbelroll skulle gälla beträffande marknadskontrollen. Vidare skulle tillsynen inte bara avse de som certifierats eller ackrediterats utan *alla* som utfärdar kvalificerade certifikat till allmänheten. Det skulle därför framstå som onaturligt att tilldela SWEDAC uppgiften att utöva tillsyn av systemet i sin helhet.

Post- och telestyrelsen har erfarenhet av tillsynsuppgifter och övervakar redan idag den tekniska infrastrukturen som bärare av tele- och datakommunikation. Myndigheten har sedan en tid tillbaka byggt upp såväl juridisk som teknisk kompetens på området för elektroniska signaturer. Vidare har Post- och telestyrelsen stor erfarenhet av standardiseringsarbete inom telesektorn och en god insyn i standardiseringsarbetet för elektroniska signaturer. Tillsyn över certifikatutfärdare skulle bredda

Post- och telestyrelsens tillsynsuppgifter från att vara teknikinriktade till att också täcka en funktion där det förmedlade innehållet står i fokus. *Industriförbundet* har uttryckt oro för att certifikatutfärdare som utövar tillsynspliktig verksamhet och som vill bli certifierad riskerar att få genomgå dubbla kontroller under två parallella kontrollsystem. Tillsynsmyndighetens verksamhet torde dock i allt väsentligt kunna koncentreras på de icke certifierade certifikatutfärdarna. Ytterligare en omständighet som talar för att välja Post- och telestyrelsen som tillsynsmyndighet är att övriga nordiska länder har bestämt eller lutar åt att utse sina motsvarigheter till tillsynsmyndigheter. Det skulle därför underlätta det nordiska samarbetet på området att utse Post- och telestyrelsen.

En samlad bedömning leder enligt regeringens uppfattning till att Post- och telestyrelsen är mest lämpad för uppgiften att bedriva tillsyn över certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten. Såsom ett flertal remissinstanser påpekar är det dock viktigt att Post- och telestyrelsen samråder och samarbetar med SWEDAC, Finansinspektionen och andra berörda myndigheter.

8 Finansieringen av tillsynsmyndighetens verksamhet

Regeringens förslag: I lagen skall det införas en bestämmelse som ger regeringen rätt att föreskriva om skyldighet för certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten att betala en avgift för tillsynsmyndighetens verksamhet enligt lagen. Befogenheten skall kunna delegeras till myndigheten.

Promemorians förslag: Överensstämmer med regeringens förslag.

Remissinstanserna: *Kommunförbundet* anför att utvecklingen mot en bred användning av kvalificerade certifikat riskerar att hämmas om kostnaderna blir för höga. *Post- och telestyrelsen* menar att det möjligen är bäst att inledningsvis avvakta med att införa avgifter till dess verksamheten har nått en sådan omfattning att den själv kan bära kostnaderna för detta.

Skälen för regeringens förslag: Det framstår som mest naturligt att låta tillsynsverksamheten finansieras genom avgiftsuttag från dem som berörs av verksamheten och för vilka den i vissa avseenden får anses vara till nytta. Det bör därför i lagen öppnas en möjlighet för regeringen eller efter regeringens bemyndigande tillsynsmyndigheten, att införa ett avgiftssystem. Frågan om och i vilken omfattning det är lämpligt att ta ut avgifter får sedan avgöras av regeringen.

Regeringens förslag: Ett tillägg skall göras till 5 kap. 3 § sekretesslagen för att tillgodose behovet av sekretesskydd för sådana koder o.d. som möjliggör kontroll av om data i elektronisk form har förvanskats.

Promemorian: Frågan behandlades inte i promemorian. Regeringens förslag grundar sig i stället på betänkandet Elektronisk dokumenthantering SOU 1996:40 (se avsnitt 3).

Utredningens förslag: Överensstämmer i huvudsak med regeringens förslag.

Remissinstanserna: Flertalet av de remissinstanser som yttrat sig över promemorian lämnar frågan om behovet av sekretess utan kommentar. *Riksdagens ombudsmän (JO)* kritiserar dock att promemorian saknar en diskussion om behovet av sekretessbestämmelser hos tillsynsmyndigheten och menar att situationer skulle kunna uppkomma där sekretessbestämmelser behövs. Flertalet av de remissinstanser som yttrat sig över betänkandet tillstyrker förslaget eller lämnar det utan erinran. *Riksarkivet* menar dock att sekretessen borde vara tidsbegränsad.

Skälen för regeringens förslag: Användningen av elektroniska signaturer på myndighetsområdet förutsätter att hemliga nycklar och anknytande uppgifter för bl.a. elektronisk signering och autenticering kan skyddas mot insyn. Behovet av sekretess kan finnas såväl hos tillsynsmyndigheten som hos en statlig certifikatutfärdare eller något annat offentligt organ.

Enligt 5 kap. 2 § sekretesslagen gäller sekretess för uppgift om säkerhetsåtgärd med avseende på bl.a. telekommunikation (punkt 3) och behörighet att få tillgång till upptagning för ADB eller annan handling (punkt 4), om det kan antas att syftet med åtgärden motverkas om uppgiften röjs. Enligt 3 § samma kapitel gäller sekretess också för uppgift som lämnar eller kan bidra till upplysning om chiffer, kod eller liknande metod som har till syfte att underlätta befordran eller användning i allmän verksamhet av uppgifter utan att föreskriven sekretess åsidosätts, om det kan antas att syftet med metoden motverkas om uppgiften röjs.

I den mån s.k. smarta kort eller liknande används så att signering och liknande sker i kortet utan att nyckeln exponeras, torde nyckeln inte anses vara förvarad hos myndigheten, eftersom den inte är tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avslyssnas eller annars uppfattas (2 kap. 3 § TF).

När nyckeln är tillgänglig för överföring i uppfattbar form är den visserligen en allmän handling, men den är sekretessbelagd om den används på sätt som sägs i 5 kap. 3 § sekretesslagen. Används den för informationssäkerhet vid telekommunikation i t.ex. ett allmänt datanät eller i s.k. behörighetskontrollsystem kan i stället 5 kap. 2 § sekretesslagen tillämpas.

Beträffande säkerhetsåtgärder som är inriktade endast på att verifiera om en handling härrör från angiven utställare – utan att samtidigt bereda sekretesskydd, skydd för telekommunikation eller skydd för åtkomst till

ADB-upptagningar – torde det emellertid inte finnas någon tillämplig bestämmelse om sekretess. Detsamma gäller om hemliga koder m.m., utan att en viss utställare pekas ut, används för att skydda vissa datamängder mot manipulation. Det är väsentligt för tilltron till elektroniska signaturer att sådana uppgifter kan hållas hemliga. Regeringen menar därför att det för sådana koder o.d. behövs ett skydd och föreslår ett tillägg till 5 kap. 3 § sekretesslagen om sekretess för koder m.m. som har till syfte att göra det möjligt att kontrollera om data i elektronisk form har förvanskats. I betänkandet föreslogs att ordet ”uppgifter” skulle användas. På inrådan från *Lagrådet* föreslår regeringen dock att det mer adekvata begreppet ”data i elektronisk form” används. Det begreppet används också i definitionen av elektronisk signatur (se avsnitt 6.3) Det saknas skäl att tidsbegränsa sekretessen.

Av 16 kap. 1 § sekretesslagen framgår att den grundlagsskyddade rätten att fritt meddela uppgifter och underrättelser för publicering (meddelarfriheten) är begränsad när tystnadsplikten följer av bl.a. 5 kap. 3 § samma lag. Regeringen menar att meddelarfriheten bör begränsas även för de uppgifter som nu är aktuella.

10 Ikraftträdande

Regeringens förslag: Lagen om kvalificerade elektroniska signaturer skall träda i kraft den 1 januari 2001. Certifikatutfärdare som redan före ikraftträdandet utfärdar sådana certifikat som medför anmälningsplikt enligt 8 § skall dock inte behöva göra anmälan före den 1 februari 2001. Vidare skall 15 § inte tillämpas i fråga om avtal som träffats före ikraftträdandet.

Promemorians förslag: Överensstämmer i huvudsak med regeringens förslag.

Remissinstanserna: *iD2 Technologies* anför att kvalificerade certifikat inte kan finnas förrän lagen trätt i kraft och att punkt 2 i den föreslagna övergångsbestämmelsen därför inte fyller någon funktion.

Skälen för regeringens förslag: Enligt artikel 13 i direktivet skall medlemsstaterna sätta i kraft de bestämmelser i lagar och andra författningar som är nödvändiga för att följa direktivet senast ett och ett halvt år efter det att direktivet har trätt i kraft. Enligt artikel 14 träder direktivet i kraft samma dag som det offentliggörs i Europeiska gemenskapernas officiella tidning, vilket skedde den 19 januari 2000. Det skall således vara genomfört i medlemsstaterna senast den 19 juli 2001. Den svenska lagen bör emellertid kunna träda i kraft redan den 1 januari 2001.

I promemorian angavs att certifikatutfärdare som redan före ikraftträdandet utfärdar kvalificerade certifikat till allmänheten bör få rådrum att uppfylla kravet att anmäla verksamheten till tillsynsmyndigheten och att det därför borde anges att skyldigheten inträder först en månad efter det att lagen trätt i kraft. Såsom *iD2 Technologies* anger i sitt remissyttrande kan det dock inte utfärdas några kvalificerade certifikat innan lagen trätt i kraft. Däremot kan det naturligtvis utfärdas certifikat som

uppfyller alla krav och som så fort lagen träder i kraft skulle få kallas för kvalificerade. Sådana certifikat skulle utan en övergångsbestämmelse behöva anmälas redan på nyårsdagen 2001. Regeringen föreslår därför att för sådana certifikat som medför anmälningsskyldighet enligt lagen skall anmälningsskyldigheten gälla först den 1 februari 2001.

Förslaget att 15 § – som innebär att skadeståndsbestämmelsen är tvingande till förmån för den som förlitar sig på ett certifikat – inte skall tillämpas på eventuella avtal som träffats före ikraftträdandet har tillkommit på inrådan från *Lagrådet*. Med hänsyn till att det endast i undantagsfall torde finnas ett sådant avtal i de öppna system som lagen avser (se avsnitt 6.2 och 6.9.2), torde bestämmelsen dock inte få någon större praktiskt betydelse.

11 Kostnader

Regeringens bedömning: De föreslagna ändringarna torde inte leda till några ökade kostnader för det allmänna.

Promemorian: Frågan behandlades inte i promemorian.

Remissinstanserna: *Domstolsverket* efterlyser en analys av förslagets betydelse för måltillströmningen i de allmänna förvaltningsdomstolarna. *Kammarrätten i Stockholm* menar att en prövning av mål enligt lagen kan komma att ta i anspråk ”icke helt obetydliga resurser” hos domstolen.

Skälen för regeringens bedömning: Domstolsprövning med anledning av lagen förväntas bli ytterst begränsad och bedöms därför inte påverka förvaltningsdomstolarnas resursbehov. Den verksamhet som tillsynsmyndigheten skall bedriva enligt lagen kommer att finansieras genom avgifter. Regeringen bedömer att förslaget inte heller på något annat sätt kommer att leda till ökade kostnader för det allmänna.

12 Författningskommentar

12.1 Förslaget till lag om kvalificerade elektroniska signaturer

Allmän bestämmelse

1 §

I paragrafen lämnas upplysning om lagens syfte, huvudsakliga innehåll och tillämpningsområde. Angivandet av lagens syfte har tillkommit på förslag från *Lagrådet* och bidrar till att förklara valet av lagens namn.

Lagen gäller sådana certifikatutfärdare som är etablerade i Sverige och som utfärdar kvalificerade certifikat till allmänheten (se avsnitt 6.2). Inga krav ställs alltså på certifikattjänster med ursprung i andra länder. Därigenom genomförs delvis artikel 4 i direktivet, som bl.a. stadgar att varje medlemsstat skall tillämpa de nationella bestämmelserna på

tillhandahållare av certifikattjänster som är etablerade på dess territorium. Se även kommentaren till 7 §.

Definitioner

2 §

Paragrafen, som motsvaras av artikel 2 i direktivet, upptar definitioner av vissa begrepp som återkommer i lagen och har kommenterats utförligt i avsnitt 6.3.

Beträffande *elektronisk signatur* kan anmärkas att lagtexten, liksom direktivet, inte begränsar sig till digitala data, vilket var fallet i kommissionens ursprungliga förslag till direktiv. Den helt övervägande delen av den praktiska tillämpningen av elektroniska signaturer kommer emellertid under överskådlig tid att avse digitala data. Definitionen torde innebära att alla elektroniska ”identifieringar” som är logiskt knutna till ett elektroniskt meddelande omfattas, från biometriska identifieringsmetoder till enkla engångskoder. Även elektronisk post omfattas av begreppet.

Med definitionen av *undertecknare* avses inte den som orättmätigt kommit över en anordning för signaturframställning, utan den som utpekas i certifikatet och som därmed rätteligen innehar anordningen.

Signaturframställningsdata är vad som i det öppna nyckelsystemet benämns den hemliga nyckeln.

En *anordning för signaturframställning* är den utrustning som används för att frambringa en elektronisk signatur. Anordningen använder signaturframställningsdata och kan i praktiken utgöras av t.ex. ett s.k. smart kort där signaturframställningsdata finns lagrade. När en elektronisk signatur skall framställas förs kortet in i en kortläsare som är kopplad till en datamaskin och en särskild kod anges. På det sättet skapas viss garanti för att den elektroniska signaturen inte kan användas utan att innehavaren av kortet är närvarande.

Signaturverifieringsdata motsvaras i det öppna nyckelsystemet av den öppna nyckeln.

För att kunna använda en elektronisk signatur i ett öppet system, såsom Internet, där parterna inte känner varandra i förväg, finns det ett behov för parterna att kunna inhämta information om varandras signaturverifieringsdata (öppna nyckel). Ett *certifikat* innehåller uppgifter om vem som är innehavare av en elektronisk signatur. Certifikatet är ett elektroniskt intyg som anger sambandet mellan en undertecknares (nyckelinnehavares) identitet och dennes signaturverifieringsdata (öppna nyckel).

Säkra anordningar för signaturframställning

3–5 §§

3 § motsvarar artikel 2.6 samt bilaga III till direktivet. 4 § motsvarar artikel 3.5 och 5 § motsvarar artikel 3.4 och delvis artikel 4.2. Genom hänvisningen till bestämmelserna i lagen (1992:1119) om teknisk kontroll genomförs också artikel 11.1.b delvis. Med uttrycket ”i praktiken” menas att risken för att de signaturframställningsdata som avses skulle

förekomma mer än en gång skall vara försvinnande liten. Bestämmelserna har behandlats i avsnitt 6.8.

Kvalificerade certifikat

6 §

Genom första stycket genomförs artikel 2.10 samt bilaga I till direktivet. Bestämmelsen behandlas i avsnitt 6.4.

Av *första punkten* följer att det måste framgå av själva certifikatet att det är ett kvalificerat sådant. Det räcker alltså inte med att certifikatutfärdaren bara anger detta i sin marknadsföring eller på annat sätt.

I *andra punkten* i första stycket krävs det bl.a. att certifikatutfärdaren anger i vilket land utfärdaren är etablerad. Etableringslandet har betydelse bl.a. för om certifikatutfärdaren omfattas av lagen. Dennes egna angivande av etableringsland är ett led i bedömningen av vilka nationella bestämmelser som är tillämpliga (jfr kommentaren till 1 §), vilket kan vara en viktig upplysning för den som skall förlita sig på certifikatet.

I *tredje punkten* ges möjligheten att ange undertecknaren med en pseudonym, om det framgår att det är fråga om en pseudonym. Värdet av en sådan signatur kan emellertid antas vara begränsat. Det avgörande för om en mottagare skall förlita sig på en signatur torde vara att det omedelbart framgår vem som innehar signaturen (jfr kommentaren till 17 §).

Enligt *fjärde punkten* krävs att om det finns särskilda uppgifter om undertecknaren som är relevanta för ändamålet med certifikatet, så skall dessa anges. Det kan t.ex. vara fråga om certifikat som skall användas för kommunikation med vissa organisationer och det är väsentligt att ange kundnummer, försäkringsnummer eller dylikt.

Kravet i *femte punkten* innebär att signaturverifieringsdata (den öppna nyckeln i PKI-lösningar) måste finnas i certifikatet. Det är alltså inte acceptabelt att den mottagare som skall förlita sig på certifikatet utöver den information han eller hon kan hämta i detta måste vända sig särskilt till certifikatutfärdaren eller någon annan för att få tillgång till signaturverifieringsdata.

I *sjätte punkten* stadgas att certifikatets giltighetstid måste anges. Av paragrafens inledning framgår också att certifikaten alltid skall vara utfärdade för en bestämd tid. Teknikutvecklingen på området kan förväntas vara fortsatt snabb och en elektronisk signatur som är säker i dag kan mycket väl sakna samma skydd mot förfalskningar inom några år. Det finns anledning att överväga om handlingar, där det finns behov av att säkert identifiera undertecknaren även efter det att certifikatets giltighetstid löpt ut, lämpar sig för att kommuniceras elektroniskt. Under alla förhållanden bör man i sådana fall på annat sätt dokumentera att identifiering skett (jfr avsnitt 6.11).

Kravet i *åttonde punkten* innebär att certifikatutfärdaren skall signera certifikatet med sin avancerade elektroniska signatur eller motsvarande. Därigenom kan den som förlitar sig på certifikatet identifiera certifikatutfärdaren och avslöja om det skett några förändringar i certifikatet sedan certifikatutfärdaren signerat det.

Enligt *andra stycket* kan regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten precisera kraven och ange hur de skall uppfyllas.

Kraven i 6 § har nära samband med skadeståndsbestämmelserna, se kommentaren till 14 §.

7 §

Genom bestämmelsen genomförs andra meningen i artikel 4.1 och artikel 7.1 i direktivet. Bestämmelsen innebär att även certifikat utfärdade av någon etablerad i något annat EES-land (punkt 1) och – under vissa förutsättningar – även i tredje land (punkterna 2 och 3), skall anses vara kvalificerade om de uppfyller kraven i 6 § första stycket 1–9.

Utfärdande av kvalificerade certifikat

8 §

I paragrafen föreskrivs en skyldighet för den som vill utfärda kvalificerade certifikat till allmänheten att anmäla detta hos den myndighet regeringen bestämmer (tillsynsmyndigheten). Detta står inte i strid med direktivets förbud mot förhandstillstånd för certifikatutfärdare. Det är inte fråga om att certifikatutfärdaren skall godkännas eller ges något tillstånd av tillsynsmyndigheten. Syftet är endast att tillsynsmyndigheten skall kunna veta vilka certifikatutfärdare myndigheten skall ha tillsyn över. Tillsynsmyndigheten ges endast förutsättningar att kontrollera efterlevnaden av lagen. Om en certifikatutfärdare underlåter att anmäla sin verksamhet och detta kommer till tillsynsmyndighetens kännedom torde det sällan finnas anledning att i det läget förelägga utfärdaren att anmäla verksamheten.

Frågan om vilka certifikatutfärdare som omfattas av anmälningsskyldigheten behandlas i avsnitt 6.5 och 6.12.

9 §

Genom paragrafen genomförs delvis artiklarna 2.10 och 3.5 samt punkterna a, b, d, e, f, g, h och j i bilaga II till direktivet. Bestämmelsen, som innehåller krav på en sådan certifikatutfärdare som utfärdar kvalificerade certifikat, behandlas i avsnitt 6.5–6.7.

Första stycket innehåller en allmän regel om att certifikatutfärdarens verksamhet måste bedrivas tillförlitligt. På förslag från *Lagrådet* används begreppet ”tillförlitligt” i stället för ”med den pålitlighet som krävs” som anges i punkt a i bilaga II till direktivet. Någon saklig skillnad avses dock inte.

Kraven i *första* och *andra punkterna* första stycket motsvarar tillsammans med det inledande allmänna kravet i paragrafen i praktiken de krav som återfinns i befintliga standarder vad gäller ledning för informationssäkerhet (se avsnitt 6.7). På förslag från *Lagrådet* anges att personalen inte bara skall ha tillräcklig kompetens utan även tillräcklig erfarenhet. Därigenom följs direktivtexten i bilaga II punkt e på ett bättre sätt.

Tredje punkten korresponderar med tredje stycket där det stadgas att sådana produkter som uppfyller vissa standarder som Europeiska kom-

missionen senare skall referera till skall presumeras uppfylla kraven i tredje punkten (jfr avsnitt 6.5) För att närmare följa direktivtexten i bilaga II punkt f klargörs, på *Lagrådets* inrådan, att det är certifikatutfärdaren som har ansvar för att teknisk och kryptografisk säkerhet upprättshålls.

På vilket sätt certifikatutfärdaren skall uppfylla kravet i *fjärde punkten* varierar givetvis med vilken typ av certifikat utfärdaren tillhandahåller. Är det fråga om certifikat som kan komma att användas för transaktioner som kan innebära stora ekonomiska konsekvenser för parterna måste den ekonomiska beredskapen vara högre än om certifikaten endast kan användas för smärre transaktioner. Kravet kan exempelvis, som också anges i direktivet, uppfyllas genom att certifikatutfärdaren tecknar en lämplig försäkring.

I *femte punkten* föreskrivs en skyldighet för certifikatutfärdaren att säkert kontrollera identiteten hos den undertecknare till vilken ett kvalificerat certifikat utfärdas.

I *sjätte punkten* åläggs certifikatutfärdaren att ha ett snabbt och säkert system för registrering och återkallelse av certifikat, jfr 10 §.

Kraven i *sjunde punkten* kan delvis uppfyllas genom att certifikatutfärdaren påför certifikatet sin egen avancerade elektroniska signatur eller motsvarande (jfr 6 § 8). Andra ledet i punkten tar sikte på det fallet att certifikatutfärdaren också framställer signaturframställningsdata (den hemliga nyckeln). Genereringen av dessa data måste då ske på ett sådant sätt att de inte röjs för obehöriga. På förslag från *Lagrådet* används ordet framställandet i stället för tillhandahållandet som regeringen först föreslog. Ordet framställandet torde stämma bättre överens med ordet ”genereringen” som används i direktivtexten.

Regeringen eller tillsynsmyndigheten kan enligt 13 § utfärda närmare bestämmelser om kraven i paragrafen.

10 §

Genom paragrafen genomförs punkten c i bilaga II och delvis artikel 6.1 c och 6.2 i direktivet.

Av *första punkten* framgår att certifikatutfärdaren är skyldig att omedelbart återkalla ett certifikat när undertecknaren begär det eller när det annars finns anledning till det. En sådan anledning kan vara att det står klart för certifikatutfärdaren att den hemliga nyckeln används av någon annan än den rättmätige innehavaren. På *Lagrådets* inrådan används ordet återkalla i stället för spärra som regeringen först föreslog. Med ordbytet avses dock ingen saklig förändring. Återkallelsen kan vara antingen temporär eller permanent.

Andra punkten innebär att det skall vara möjligt att slå fast när ett certifikat är utfärdat eller återkallat. Detta kan vara av betydelse vid eventuella tvister mellan undertecknaren och mottagaren.

Det typiska fall som kraven i *tredje punkten* tar sikte på är att certifikatutfärdaren framställer både signaturframställningsdata och signaturverifieringsdata, exempelvis genom att utställa ett s.k. smart kort där den elektroniska signaturen finns. Det är då certifikatutfärdarens skyldighet att försäkra sig om att endast sådana signaturframställningsdata och

signaturverifieringsdata framställs som kan användas som komplement till varandra.

Kraven i 10 § har nära samband med skadeståndsbestämmelserna, se kommentaren till 14 §.

Regeringen eller tillsynsmyndigheten kan enligt 13 § utfärda närmare bestämmelser om kraven i paragrafen.

11 §

Genom paragrafen, som behandlar certifikatutfärdarens skyldighet att registrera relevant information om ett kvalificerat certifikat samt använda tillförlitliga system för lagring av certifikat, genomförs punkterna i, j och l i bilaga II till direktivet.

Det inledande kravet på registrering av information syftar bl.a. till att vid rättsliga förfaranden kunna lägga fram bevis om utfärdande av certifikat. Registreringen får ske elektroniskt.

Det är önskvärt att parter som inte har något tidigare avtal om hur man skall kommunicera kan kommunicera elektroniskt på ett säkert sätt. En metod för att möjliggöra detta är att man kan hämta t.ex. en framtida avtalspartners certifikat i en öppen databas. Direktivet föreskriver emellertid att certifikatutfärdaren får göra certifikaten offentligt tillgängliga för hämtning av uppgifter endast i de fall för vilka certifikatinnehavarens uttryckliga samtycke har inhämtats (jfr 16 §).

Andra stycket tar sikte på det fallet att certifikatutfärdaren tillhandahåller signaturframställningsdata. Det är väsentligt för tilltron till elektroniska signaturer att det verkligen bara är undertecknaren som har tillgång till signaturframställningsdata. Certifikatutfärdaren förbjuds därför att bevara eller kopiera sådana data.

Regeringen eller tillsynsmyndigheten kan enligt 13 § utfärda närmare bestämmelser om kraven i paragrafen.

12 §

Genom paragrafen genomförs punkten k) i bilaga II till direktivet.

Paragrafen ålägger certifikatutfärdare som utfärdar kvalificerade certifikat att till den som certifikatet utfärdas till ge de upplysningar som gör det möjligt för denne att värdera tjänsten. Upplysningarna skall lämnas ”skriftligt”, dvs. i betydelsen ”inte muntligt” och med ett språkbruk som är lättbegripligt. Inget hindrar att de lämnas elektroniskt. Att hänvisa till en webbplats på Internet under certifikatutfärdarens kontroll, där denne från tid till annan kan ändra i villkoren, är givetvis inte tillräckligt.

Informationen skall också tillhandahållas andra som begär att få den, t.ex. mottagaren av en signatur baserad på certifikatet.

På *Lagrådets* inrådan utformas bestämmelsen i närmare överensstämmelse med direktivtexten, jämfört med den utformning som föreslogs i lagrådsremissen.

Regeringen eller tillsynsmyndigheten kan enligt 13 § utfärda närmare bestämmelser om kraven i paragrafen.

13 §

Paragrafen ger regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten, möjlighet att närmare reglera kraven i 9–12 §§.

Skadestånd

Genom bestämmelsen i 14 § genomförs artikel 6 i direktivet. Genom 15 § klargörs att bestämmelsen är tvingande till förmån för den som förlitar sig på certifikatet. Bestämmelserna behandlas i avsnitt 6.9.

Förhållanden som inte omfattas av det särskilda skadeståndsansvaret i paragraferna får bedömas i enlighet med allmänna skadeståndsrättsliga regler.

14 §

I paragrafen anges vilka certifikatutfärdare som omfattas av den särskilda skadeståndsskyldighet som anges i direktivet, se närmare avsnitt 6.9.2. Det bör betonas att även certifikat som inte uppfyller kraven på ett kvalificerat certifikat – dvs. inte uppfyller kraven i 6 § – omfattas, om de utges för att vara kvalificerade certifikat.

Även certifikatutfärdare som garanterar att någon annan certifikatutfärdares certifikat är kvalificerade omfattas, i de fall certifikatet inte uppfyller kraven i 6 § eller vid utfärdandet innehåller felaktiga uppgifter. Detta har samband med den särskilda möjlighet som beskrivs i artikel 7 i direktivet, nämligen att en certifikatutfärdare inom Europeiska unionen garanterar ett certifikat som utfärdats av en certifikatutfärdare som är etablerad utanför unionen.

Den skada som kan bli aktuell att ersätta enligt 14 § torde vara ren förmögenhetsskada. Huvudregeln vad gäller utomkontraktuella förhållanden enligt svensk skadeståndsrätt är enligt 2 kap. 4 § skadeståndslagen (1972:207) att ren förmögenhetsskada endast ersätts om skadan vållats genom brott. Enligt förarbetena till skadeståndslagen är dock inte avsikten att denna bestämmelse skall utgöra hinder för en utveckling i praxis i riktning mot ett vidgat ansvar för ren förmögenhetsskada. Som nämnts i avsnitt 6.9.1 har skadeståndsansvar för vissa felaktiga intyg godtagits i praxis sedan lång tid. De här aktuella skadeståndsreglerna är inte heller avsedda att läsas motsatsvis på sådant sätt att skadeståndsskyldighet för ren förmögenhetsskada enligt allmänna principer är utesluten utanför deras tillämpningsområde, t.ex. när det är en certifikatutfärdare som utfärdar ett certifikat som inte utges för att vara kvalificerat. Se vidare avsnitt 6.9.2.

Artikel 6.1.a i direktivet stadgar att en tillhandahållare av certifikattjänster som till allmänheten utfärdar certifikat som anges vara kvalificerade eller garanterar att någon annans certifikat är kvalificerade, genom det särskilda skadeståndsansvaret svarar för att all information i certifikatet är korrekt vid tidpunkten för utfärdandet och att certifikatet innehåller alla de uppgifter som föreskrivs för ett kvalificerat certifikat. I 6 § första stycket föreskrivs vad ett kvalificerat certifikat skall innehålla. Genom att det i denna paragrafs *första stycke* föreskrivs att certifikatutfärdaren är skadeståndsskyldig om certifikatet innehåller

felaktiga uppgifter vid utfärdandet eller inte uppfyller kraven i 6 § första stycket, täcks artikel 6.1.a i direktivet.

I artikel 6.1.b stadgas att certifikatutfärdaren svarar för att den undertecknare som anges i det kvalificerade certifikatet vid tidpunkten för utfärdandet var i besittning av de signaturframställningsdata som motsvarar de signaturverifieringsdata som anges i certifikatet. Genom 6 § första stycket 5 föreskrivs att det är certifikatutfärdarens skyldighet att se till att certifikatet innehåller signaturverifieringsdata som motsvarar de signaturframställningsdata som undertecknaren vid tidpunkten för utfärdandet har kontroll över. Om inte undertecknarens signaturframställningsdata motsvarar de signaturverifieringsdata som anges i certifikatet, innehåller certifikatet felaktiga uppgifter och certifikatutfärdaren är således skadeståndsskyldig för den skada detta kan orsaka.

I artikel 6.1.c stadgas att certifikatutfärdaren svarar för att signaturframställningsdata och signaturverifieringsdata kan användas som komplement till varandra om certifikatutfärdaren framställer båda dessa. Genom att det genom 10 § 3 fastställs att det är certifikatutfärdarens skyldighet att, i förekommande fall, säkerställa att sådana signaturframställningsdata och signaturverifieringsdata som utfärdaren framställer kan användas som komplement till varandra, täcks även detta fall av 14 §.

I artikel 6.2 stadgas att en certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten också skall svara för skada som åsamkats genom underlåtenhet att registrera återkallande av certifikatet. Om certifikatutfärdaren inte iakttar sin skyldighet enligt 10 § 1 att omedelbart återkalla ett certifikat, eller enligt 10 § 2 att säkerställa att exakt tidpunkt för när så har skett kan anges, innebär det att certifikatutfärdaren kan vara skadeståndsskyldig enligt 14 §.

Uttrycket ”den som förlitar sig på certifikatet” är inte begränsat till mottagaren av en elektronisk signatur. Även undertecknaren, som ingått avtal med certifikatutfärdaren att den sistnämnde skall möjliggöra för undertecknaren att kunna identifiera sig vid elektronisk kommunikation, kan lida skada på grund av t.ex. felaktigheter eller brister i ett certifikat. Även detta regleras i viss mån genom paragrafen. Det är således inte möjligt för certifikatutfärdaren att genom avtal med undertecknaren begränsa sitt ansvar för att en hemlig och en öppen nyckel (ett nyckelpar) som certifikatutfärdaren tillhandahållit verkligen fungerar, dvs. kan användas som komplement till varandra.

Av första meningen i *andra stycket* framgår att certifikatutfärdaren kan undgå skadeståndsansvar om utfärdaren kan visa att skadan inte beror på vårdslöshet hos denne. Certifikatutfärdaren har således ett s.k. presumtionsansvar med möjlighet att exculpera sig. Enligt allmänna skadeståndsrättsliga principer är det dock alltid den skadelidande som i dessa fall har att bevisa skadan och sambandet mellan skadan och exempelvis felet i certifikatet, se avsnitt 6.9.

Enligt artikel 6.3 och 6.4 i direktivet skall medlemsstaterna säkerställa att det i viss mån är möjligt för certifikatutfärdarna att genom att i certifikatet ange begränsningar för användningsområde eller transaktionsbelopp begränsa sitt skadeståndsansvar. Begränsningarna måste då vara tydliga

för tredje man. Genom andra meningen i andra stycket i paragrafen regleras denna möjlighet.

I 6 § 9 anges att eventuella begränsningar måste anges i certifikatet. I förevarande paragraf anges att begränsningarna måste vara tydliga. Detta innefattar att de måste vara tydliga för den som certifikatet utfärdas till och, inte minst, för den mottagare som skall förlita sig på certifikatet. Certifikatutfärdaren är inte skadeståndsskyldig för skada som härrör från att certifikatet använts i strid med de begränsningar som på detta sätt angivits för det.

Av *tredje stycket* framgår att även den som garanterar att någon annans certifikat är kvalificerat omfattas av skadeståndsbestämmelsen med möjlighet att exculpera sig. Av begränsningen till punkterna 2 och 3 i första stycket följer dock att garanten inte kan göras skadeståndsskyldig för att utfärdaren inte har uppfyllt sina skyldigheter enligt 10 §.

Se vidare avsnitt 6.9.2.

15 §

Normalt torde det inte finnas något avtalsförhållande mellan certifikatutfärdaren och den som förlitar sig på ett certifikat. I undantagsfall kan det dock förekomma att parterna har ett avtal där certifikatet utgör ett moment. Av bestämmelsen följer att certifikatutfärdaren i dessa fall inte kan avtala bort någon del av sitt skadeståndsansvar. Naturligtvis är dock parterna fria att träffa avtal om ett större ansvar för certifikatutfärdaren om så önskas. Se avsnitt 6.9.2.

Behandling av personuppgifter

16 §

Genom paragrafen, som behandlas i avsnitt 6.10, genomförs artikel 8.2 i direktivet.

Personuppgiftslagen (1998:204) är tillämplig på certifikatutfärdare. I paragrafen anges i vilka avseenden begränsningarna för hur den som utfärdar certifikat till allmänheten får behandla personuppgifter är snävare än vad som stadgas i personuppgiftslagen. Bestämmelsen är inte begränsad till att avse endast den som utfärdar kvalificerade certifikat.

Självfallet gäller bestämmelsen endast i den mån inte annat följer av yttrandefrihetsgrundlagen eller tryckfrihetsförordningen.

Kvalificerade elektroniska signaturer

17 §

Första meningen i bestämmelsen behandlar den särställning som kvalificerade elektroniska signaturer ges enligt artikel 5 i direktivet. Frågan om i vilken mån artikel 5 i direktivet kräver lagstiftningsåtgärder i Sverige behandlas i avsnitt 6.11.

Bestämmelsen innebär att kvalificerade elektroniska signaturer – dvs. elektroniska signaturer som uppfyller en viss säkerhetsnivå – ges en viss särställning i de fall krav på underskrift, egenhändigt undertecknande och motsvarande får uppfyllas med elektroniska medel. I de fall det över

huvud taget är tillåtet att använda en elektronisk signatur så får det i författningar inte ställas högre krav på den elektroniska signaturen i sig, än vad som ställs på en kvalificerad elektronisk signatur.

Det kan vara tillåtet att använda en elektronisk signatur antingen genom att det i en viss bestämmelse uttryckligen anges att en elektronisk signatur får eller t.o.m. måste användas. Det kan också vara tillåtet att använda en elektronisk signatur genom att ett krav på egenhändig underskrift eller något liknande uttryck i rättstillämpningen har tolkats så att kravet kan uppfyllas genom en elektronisk signatur. Med uttrycket ”krav på egenhändig underskrift eller motsvarande” avses alltså såväl krav på underskrift, undertecknande och liknande uttryck, som krav på elektronisk signatur.

Bestämmelsen påverkar alltså inte formkrav i lag eller annan författning som utesluter användning av elektroniska medel. Om det i en författning ställs krav på att en handling skall vara försedd med underskrift torde det normalt innebära att elektroniska medel – och därmed elektroniska signaturer – är uteslutna (jfr SOU 1996:40 s. 95). Om det däremot av författningen, uttryckligen eller genom tolkning, följer att kravet på underskrift kan uppfyllas med en elektronisk signatur får 17 § sin betydelse. Paragrafen utgör vidare inget hinder mot att, när elektroniska signaturer får användas, godta elektroniska signaturer med *lägre* säkerhetsnivå än kvalificerade. Det får dock inte i författningar – utom i de fall som avses i andra stycket – ställas *högre* krav på elektroniska signaturer än vad som ställs på kvalificerade elektroniska signaturer.

Enligt direktivet skall en pseudonym kunna anges i ett certifikat. Denna möjlighet anges också i 6 §. Detta innebär givetvis inte att formkrav på underskrift vid användningen av elektroniska medel kan uppfyllas genom att en pseudonym används, annat än om detta till äventyrs godtas även i övrigt.

Andra meningen avser användningen av elektroniska signaturer vid kommunikation med eller mellan myndigheter. På förslag från *Lagrådet* används begreppet ”myndigheter” i stället för ”den offentliga sektorn”, eftersom det sistnämnda begreppet är vagt och kan ge upphov till tolkningssvårigheter. Begreppet myndighet har samma innebörd som i regeringsformen, dvs. samtliga statliga och kommunala organ med undantag av riksdagen och de kommunala beslutande församlingarna (Holmberg m.fl, Grundlagarna, s. 55). Bestämmelsen, som grundar sig på artikel 3.7 i direktivet, innebär att det vid sådan kommunikation får ställas högre krav på elektroniska signaturer än vad som ställs på kvalificerade elektroniska signaturer, dock endast i de fall det är uttryckligen tillåtet. Bestämmelsen har behandlats i avsnitt 6.11.

Tillsyn

Genom tillsynsbestämmelserna genomförs direktivets artikel 3.3. Bestämmelserna har behandlats utförligt i avsnitt 6.12.

18 §

Första stycket i bestämmelsen har på inrådan av *Lagrådet* fått en annan utformning. Någon saklig förändring avses dock inte med detta. Tillsynsmyndigheten har i uppgift att övervaka att de certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten uppfyller lagens krav, inbegripet att de kvalificerade certifikaten uppfyller kraven. Däri ligger också att myndigheten skall kunna ingripa mot den som felaktigt påstår att ett certifikat är kvalificerat. Myndigheten skall också utöva marknadskontroll över anordningar som anges vara säkra anordningar för signaturframställning, genom att övervaka att de uppfyller lagens krav och är godkända av ett sådant organ som anges i 5 §.

Avsikten är att genom den statliga tillsynen bidra till att certifikat som betecknas som kvalificerade får en sådan kvalitets- och säkerhetsnivå att allmänheten, företagen och andra har förtroende för dem och för de signaturer som baseras på dem.

Någon praktisk möjlighet för myndigheten att i detalj granska varje certifikatufärdare och dennes certifikat torde inte finnas och är knappast heller önskvärd. Myndigheten kommer däremot att kunna fungera som en garant för att uppdagade missförhållanden åtgärdas.

Myndigheten kommer att kunna ta befintliga och kommande standarder till hjälp för att bedöma certifikatutfärdarnas verksamhet. Det skall dock vara möjligt att klara lagens krav utan att använda sig av de standarder som finns.

De certifikatutfärdare som väljer att certifiera sig och sina produkter kommer genom certifieringsorganet att i många avseenden stå under tillräcklig löpande kontroll, även om de givetvis också står under myndighetens tillsyn. Tillsynsmyndigheten har också sanktionsmöjligheter som inte står certifieringsorganen till buds.

Vidare finns möjlighet för myndigheten att anlita externa konsulter. Det finns anledning att förutse förekomsten av organisationer som i och för sig kommer att ha erforderlig kompetens att certifiera certifikatutfärdarna, men av olika skäl inte kommer att uppträda som certifieringsorgan, t.ex. revisionsbolag och datakonsultföretag. Denna kompetens bör kunna utnyttjas.

I *andra stycket* åläggs tillsynsmyndigheten att föra och offentliggöra en förteckning över anmälda certifikatutfärdare som får utfärda kvalificerade certifikat. I denna förteckning torde myndigheten även kunna ange vilka certifikatutfärdare som förelagts att upphöra med verksamheten eller att kalla sina certifikat för kvalificerade. En sådan förteckning skulle också kunna innehålla signaturverifieringsdata (den öppna nyckeln) för certifikatutfärdarens avancerade elektroniska signatur eller motsvarande, som skall finnas i de kvalificerade certifikaten (jfr kommentaren till 6 §). För att inte riskera att sådana register kommer i strid med personuppgiftslagen (1998:204) har tillsynsmyndigheten, på *Lagrådets* inrådan, ålagts en skyldighet att föra och offentliggöra dessa register (jfr PUL 10 § e). Vidare torde bestämmelsen, såsom Lagrådet påpekar, även fylla funktionen att förstärka intresset hos dem som vill utfärda kvalificerade certifikat att fullgöra sin anmälningsskyldighet enligt 8 §.

19 §

I paragrafen ges myndigheten vissa befogenheter som är nödvändiga för att en effektiv tillsyn skall kunna utövas. Det kan vara fråga om att inhämta uppgifter som myndigheten anser att den behöver för att kunna bedöma verksamheten. Initiativet kan vara myndighetens eget, men det kan också ha sin grund i en anmälan till myndigheten.

Uppgifter torde i många fall kunna hämtas in formlöst vid kontakter mellan myndigheten och aktörer på marknaden. Enligt 20 och 21 §§ finns dock möjlighet för myndigheten att begära uppgifter efter föreläggande som får förenas med vite. I sista hand kan myndigheten få verkställighet hos kronofogdemyndigheten. Genom hänvisningen till utsökningsbalken blir bl.a. dennas bestämmelser om tvång i 2 kap. 17 § tillämpliga.

20–21 §§

20 § *första stycket* anger tillsammans med 21 § vilka sanktioner som får tillgripas av myndigheten. Den får själv bestämma när ett föreläggande skall förenas med vite. Det normala torde vara att myndigheten dessförinnan försökt få till stånd en frivillig rättelse.

Enligt 20 § *andra stycket* ges tillsynsmyndigheten möjlighet att förelägga den som utfärdar certifikat till allmänheten och påstår att de är kvalificerade certifikat, att upphöra med verksamheten. Möjligheten är således inte begränsad till att avse endast dem som anmält sig enligt 8 §. Ett sådant beslut kan givetvis i vissa fall få långtgående konsekvenser och får därför meddelas endast sedan andra mindre ingripande åtgärder visat sig verkningslösa. Detta är inte minst viktigt med hänsyn till att ett alltför snabbt eller svagt motiverat ingripande skulle kunna strida mot direktivets förbud mot krav på förhandstillstånd.

Tillsynsmyndigheten kan, och bör, därvid föreskriva hur verksamheten skall avvecklas. Ett föreläggande skall givetvis inte avse mer än den del av verksamheten som omfattas av tillsynen. Det väsentliga är att certifikatutfärdaren inte utan att uppfylla lagens krav påstår att till allmänheten utfärdade certifikat är kvalificerade. Det är därför naturligt att tillsynsmyndigheten koncentrerar sig på detta. Om certifikatutfärdaren väljer att fortsätta att utfärda certifikat till allmänheten, men inte längre påstår att de är kvalificerade, omfattas verksamheten inte av tillsyn enligt denna lag.

I fråga om föreläggande och utdömande av vite är lagen (1985:206) om viten tillämplig.

Avgifter

22 §

Paragrafen ger möjlighet för regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten att införa ett avgiftssystem för bekostande av tillsynsmyndighetens verksamhet, se avsnitt 8.

Överklagande

23 §
Paragrafen reglerar rätten att överklaga tillsynsmyndighetens beslut enligt lagen och enligt föreskrifter som meddelats med stöd av lagen. Myndighetens beslut får överklagas till allmän förvaltningsdomstol. Krav på prövningstillstånd gäller vid överklagande till kammarrätten.

Övergångsbestämmelserna

Lagen föreslås träda i kraft den 1 januari 2001. För att certifikatutfärdare som redan före ikraftträdandet utfärdar sådana certifikat som medför anmälningsplikt enligt 8 § skall få en rimlig tid på sig att hinna anmäla sin verksamhet till tillsynsmyndigheten stadgas i punkt 2 att de inte behöver anmäla verksamheten före den 1 februari 2001. Tredje punkten, som har tillkommit på *Lagrådets* inrådan, innebär att villkor i avtal som har träffats före den 1 januari 2001 inte kan förklaras utan verkan med stöd av 15 §.

12.2 Förslaget till lag om ändring i sekretesslagen

5 kap. 3 §
I en ny punkt föreskrivs om sekretess för uppgift som lämnar eller kan bidra till upplysning om chiffer, kod eller liknande metod som har till syfte att göra det möjligt att kontrollera om data i elektronisk form har förvanskats. Härigenom sekretessbeläggs t.ex. hemliga nycklar som används för att verifiera om en handling härrör från angiven undertecknare eller för att skydda vissa datamängder mot manipulation.

Skälen för bestämmelsen redovisas i avsnitt 9.

På förslag från *Lagrådet* används begreppet ”data i elektronisk form” i stället för ”uppgifter”, eftersom bestämmelsen inte avser alla typer av uppgifter utan just elektroniska sådana, och för att detta begrepp överensstämmer med det som används i bl.a. definitionen av elektronisk signatur i 2 §.

Av 16 kap. 1 § sekretesslagen följer att meddelarfriheten är begränsad när tystnadsplikt följer av 5 kap. 3 § sekretesslagen.

Sekretess för uppgifter om bl.a. enskilds affärs- och driftförhållanden och vissa andra ekonomiska eller personliga förhållanden som tillsynsmyndigheten får tillgång till kan föreskrivas med stöd av 8 kap. 6 § sekretesslagen.

Bilaga 1 finns endast i den tryckta upplagan.

Promemorians lagförslag

Förslag till lag om vissa elektroniska signaturer m.m.

Inledande bestämmelse

1 § Denna lag innehåller bestämmelser om vissa elektroniska signaturer, om certifikat för elektroniska signaturer och om certifikatutfärdare som är etablerade i Sverige.

Definitioner

2 § I lagen avses med

elektronisk handling: en bestämd mängd data i digital form som kan läsas, avlyssnas eller på annat sätt uppfattas med tekniskt hjälpmedel,

elektronisk signatur: data i elektronisk form som är fogade till eller logiskt knutna till en elektronisk handling och som används för att kontrollera om innehållet härrör från den som framstår som undertecknare,

avancerad elektronisk signatur: en elektronisk signatur som

a) är knuten uteslutande till undertecknaren,

b) undertecknaren kan identifieras genom,

c) är skapad med medel som endast undertecknaren kontrollerar, och

d) är knuten till en elektronisk handling på ett sådant sätt att alla efterföljande ändringar av den elektroniska handlingen kan upptäckas,

kvalificerad elektronisk signatur: en avancerad elektronisk signatur som är baserad på ett kvalificerat certifikat och som är skapad av en säker anordning för signaturframställning,

undertecknare: den som har kontroll över en anordning för signaturframställning,

signaturframställningsdata: unika data, såsom koder eller privata krypteringsnycklar, som undertecknaren använder för att skapa en elektronisk signatur,

anordning för signaturframställning: en konfigurerad maskin- eller programvara för att använda signaturframställningsdata,

signaturverifieringsdata: data, såsom koder eller öppna krypteringsnycklar, som används för att verifiera en elektronisk signatur,

certifikat: ett intyg i elektronisk form som kopplar ihop signaturverifieringsdata med en undertecknare och bekräftar dennes identitet,

certifikatutfärdare: den som utfärdar certifikat.

Kvalificerade certifikat

3 § Ett kvalificerat certifikat skall vara utfärdat för viss tid av en certifikatutfärdare som uppfyller kraven i 8–12 §§ och innehålla

1. uppgift om att det utfärdats som ett kvalificerat certifikat,
2. certifikatutfärdarens identitet och hemvist,
3. undertecknarens namn eller pseudonym med uppgift om att det är en pseudonym,
4. särskilda uppgifter om undertecknaren, om de är relevanta för ändamålet med certifikatet,

5. signaturverifieringsdata som motsvarar de signaturframställningsdata som undertecknaren vid tidpunkten för utfärdandet har kontroll över,
6. start- och sluttidpunkt för certifikatets giltighet,
7. certifikatets identifieringskod,
8. certifikatutfärdarens avancerade elektroniska signatur, och
9. uppgift om eventuella begränsningar av certifikatets användningsområde eller av värdet på de transaktioner för vilka certifikatet kan användas (transaktionsbelopp).

Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten, får meddela närmare föreskrifter om krav enligt första stycket.

Säkra anordningar för signaturframställning

4 § En säker anordning för signaturframställning skall säkerställa att signaturen är tillfredsställande skyddad mot förfalskning samt att signaturframställningsdata

1. praktiskt taget kan förekomma endast en gång och att sekretessen beträffande dessa data är tillfredsställande,
2. med rimlig säkerhet inte kan härledas, och
3. kan skyddas på ett tillfredsställande sätt av undertecknaren så att obehöriga inte kan använda dem.

Anordningen får inte förändra den elektroniska handling som skall signeras eller hindra att handlingen presenteras för undertecknaren före signeringen.

5 § Kraven på en säker anordning för signaturframställning i 4 § skall anses uppfyllda beträffande sådan maskin- eller programvara som överensstämmer med standarder för produkter för elektroniska signaturer som Europeiska gemenskapernas kommission fastställt och offentliggjort referensnummer till i Europeiska gemenskapernas officiella tidning.

6 § En anordning som anges vara en säker anordning för signaturframställning får släppas ut på marknaden eller användas för att skapa en kvalificerad signatur endast om ett för ändamålet anmält organ avgjort att anordningen uppfyller kraven i 4 §.

Organ som avses i första stycket utses enligt bestämmelserna i lagen (1992:1119) om teknisk kontroll.

Med ett avgörande enligt första stycket likställs ett avgörande av ett organ, som utsetts för detta ändamål i en annan stat inom Europeiska ekonomiska samarbetsområdet.

Utfärdande av kvalificerade certifikat

7 § En certifikatutfärdare får utfärda kvalificerade certifikat till allmänheten först efter anmälan hos den myndighet som regeringen bestämmer (tillsynsmyndigheten).

8 § En certifikatutfärdare som utfärdar kvalificerade certifikat skall bedriva verksamheten med den pålitlighet som krävs för att utfärda certifikat. Certifikatutfärdaren skall därvid

1. ha personal med erforderlig kompetens för de tjänster som erbjuds, särskilt vad avser ledning, teknik och säkerhetsrutiner,
2. använda adekvata administrativa rutiner och ledningsrutiner som uppfyller erkända standarder,
3. använda pålitliga system och produkter som är skyddade mot ändringar och garanterar teknisk och kryptografisk säkerhet i de förfaranden som stöds av dem,
4. förfoga över tillräckliga medel för att kunna bedriva verksamheten enligt denna lag och bära risken för skadeståndsskyldighet,
5. genom säkra rutiner kontrollera identiteten hos den undertecknare till vilken ett kvalificerat certifikat utfärdas,
6. förfoga över ett snabbt och säkert system för registrering och omedelbar spärrning av certifikat, och
7. vidta åtgärder mot förfalskning av certifikat och i förekommande fall garantera att tillhandahållandet av signaturframställningsdata sker konfidentiellt.

Certifikatutfärdaren får inte lagra eller kopiera signaturframställningsdata.

Kraven i första stycket 3 skall anses uppfyllda beträffande sådan maskin- eller programvara som överensstämmer med standarder för produkter för elektroniska signaturer som Europeiska gemenskapernas kommission fastställt och offentliggjort referensnummer till i Europeiska gemenskapernas officiella tidning.

9 § En certifikatutfärdaren som utfärdar kvalificerade certifikat skall

1. omedelbart spärra ett certifikat när undertecknaren begär det eller när det annars finns anledning till det
2. säkerställa att exakt tidpunkt kan anges för utfärdande och spärrning av certifikat, och
3. i förekommande fall endast framställa signaturframställningsdata och signaturverifieringsdata som kan användas som komplement till varandra.

10 § En certifikatutfärdaren som utfärdar kvalificerade certifikat skall registrera all relevant information om ett kvalificerat certifikat under rimlig tid samt använda tillförlitliga system för lagring av kvalificerade certifikat i verifierbar form så att

1. endast behöriga personer kan göra tillägg och ändringar,
2. uppgifternas äkthet kan kontrolleras,
3. ett certifikat är offentligt tillgängligt endast när innehavaren av certifikatet har lämnat sitt samtycke, och
4. tekniska förändringar som äventyrar säkerhetskraven är uppenbara för den som handhar systemet.

11 § Innan en certifikatutfärdare ingår avtal om att utfärda ett kvalificerat certifikat skall certifikatutfärdaren skriftligen informera motparten om

1. villkoren och begränsningarna för användning av certifikatet,

2. förekomsten av ett frivilligt ackrediterings- eller certifieringssystem, och

3. förfaranden för klagomål och avgörande av tvister.

Informationen enligt första stycket får överföras elektroniskt, om det sker i en för motparten omedelbart läsbar form. Informationen skall på begäran också göras tillgänglig för annan.

12 § Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får utfärda närmare bestämmelser om krav enligt 8–11 §§.

Skadestånd

13 § När en certifikatutfärdare till allmänheten utfärdar certifikat som anges vara kvalificerade eller när en certifikatutfärdare till allmänheten garanterar en annan certifikatutfärdares certifikat som kvalificerade är utfärdaren skadeståndsskyldig i enlighet med 14 §.

14 § Om en certifikatutfärdare inte har uppfyllt kraven i 9 § eller om ett certifikat vid utfärdandet innehåller felaktiga uppgifter eller inte uppfyller kraven i 3 § första stycket, skall certifikatutfärdaren ersätta den skada som därigenom åsamkas den som har rimlig anledning att förlita sig på certifikatet. Certifikatutfärdaren är dock inte skyldig att utge ersättning om utfärdaren kan visa att skadan inte har orsakats av vårdslöshet hos denne.

Trots vad som föreskrivs i första stycket är certifikatutfärdaren inte ersättningsskyldig för skada som härrör från att ett certifikat använts i strid med tydliga begränsningar avseende användningsområde eller transaktionsbelopp som angetts i certifikatet.

Behandling av personuppgifter

15 § En certifikatutfärdare som utfärdar certifikat till allmänheten får endast inhämta personuppgifter direkt från den som uppgifterna avser eller med dennes uttryckliga samtycke och endast i den utsträckning som är nödvändig för att utfärda eller upprätthålla ett certifikat. Uppgifterna får inte samlas in eller behandlas för andra ändamål utan uttryckligt samtycke från den som uppgifterna avser.

Rättslig verkan för elektroniska signaturer

16 § Om det av lag eller annan författning följer vissa formkrav för att en rättshandling skall anses giltig eller en förpliktelse fullgjord och om dessa krav kan uppfyllas genom elektronisk kommunikation med användning av någon form av elektronisk signatur, skall en kvalificerad elektronisk signatur godtas.

Tillsyn

17 § Tillsynsmyndigheten skall ha tillsyn över certifikatutfärdare som till allmänheten utfärdar certifikat som anges vara kvalificerade och över anordningar som anges vara säkra anordningar för signaturframställning.

18 § Tillsynsmyndigheten har rätt att på begäran få de upplysningar och handlingar som behövs för tillsynen.

Tillsynsmyndigheten har också rätt att få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, där verksamhet som står under tillsyn bedrivs.

Tillsynsmyndigheten har rätt att få verkställighet hos kronofogdemyndigheten av de beslut som avser åtgärder för tillsynen enligt första och andra styckena. Därvid gäller bestämmelserna om sådan verkställighet som avses i 16 kap. 10 § utsökningsbalken.

19 § Tillsynsmyndigheten får meddela de förelägganden och förbud som behövs för efterlevnaden av denna lag eller av föreskrifter som meddelats med stöd av lagen.

20 § Tillsynsmyndigheten får förelägga certifikatutfärdare som till allmänheten utfärdar certifikat som anges vara kvalificerade att helt eller delvis upphöra med verksamheten. Myndigheten får därvid besluta hur verksamheten skall avvecklas.

21 § Förelägganden och förbud enligt denna lag får förenas med vite.

Avgifter

22 § Regeringen eller, om regeringen bestämmer det, tillsynsmyndigheten får föreskriva om skyldighet för certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten att betala avgift för tillsynsmyndighetens verksamhet enligt denna lag.

Överklagande

23 § Tillståndsmyndighetens beslut enligt denna lag eller enligt föreskrifter som meddelats med stöd av lagen får överklagas hos allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Tillståndsmyndigheten får bestämma att beslut enligt denna lag skall gälla omedelbart.

---

1. Denna lag träder i kraft den 1 januari 2001.

2. Beträffande certifikatutfärdare som redan före ikraftträdandet utfärdar kvalificerade certifikat till allmänheten skall föreskriften i 7 § om anmälan tillämpas först den 1 februari 2001.

Förteckning över remissinstanserna avseende Ds 1999:73

Följande remissinstanser har beretts tillfälle att avge synpunkter på departementspromemorian Ds 1999:73 Elektroniska signaturer.

Riksdagens ombudsmän (JO), Hovrätten över Skåne och Blekinge, Kammarrätten i Stockholm, Uppsala tingsrätt, Länsrätten i Stockholms län, Justitiekanslern, Domstolsverket, Rikspolisstyrelsen, Datainspektionen, Statskontoret, Styrelsen för ackreditering och teknisk kontroll (SWEDAC), Kommerskollegium, Försvarsmakten, Försvarets Forskningsanstalt, Riksförsäkringsverket, Tullverket, Finansinspektionen, Riksskatteverket, Konsumentverket, Juridiska fakultetsnämnden vid Uppsala universitet, Juridiska institutionen vid Handelshögskolan vid Göteborgs universitet, Centrala Studiestödsnämnden, Post- och telestyrelsen, Närings- och teknikutvecklingsverket, Patent- och registreringsverket, Tekniska nomenklaturcentralen, SIS – Standardiseringen i Sverige, IT-kommissionen, Svenska Kommunförbundet, Landstingsförbundet, Stockholms handelskammare, Industriförbundet, Svensk Handel, Gemenskapen för elektroniska affärer (GEA), SEIS, IT-företagen, Svenska Bankföreningen, Sveriges advokatsamfund, Sveriges försäkringsförbund, Svenska Arbetsgivareföreningen, Sveriges Akademikers Centralorganisation, Landsorganisationen, Posten AB, Telia AB, Tele2 AB, Telefonaktiebolaget LM Ericsson, IBM Svenska AB, Setec Card AB, iD2 Technologies AB, Network Information Center, ISOC-SE, Network Associates AB, Wineasy AB, Nexus AB, Advokatfirman Lagerlöf & Leman, Nordbanken AB, FöreningsSparbanken, OM-gruppen AB, VPC AB och Bankgirot BGC AB.

Härutöver har synpunkter lämnats in av Finansbolagens förening, Svenska Inkassoföreningen och Riksarkivet.

Förteckning över remissinstanserna avseende SOU 1996:40

Följande remissinstanser har beretts tillfälle att avge synpunkter på betänkandet SOU 1996:40 Elektronisk dokumenthantering.

Riksdagens ombudsmän (JO), Svea hovrätt, Malmö tingsrätt, Kammarrätten i Göteborg, Länssrätten i Stockholms län, Justitiekanslern, Domstolsverket, Riksåklagaren, Rikspolisstyrelsen, Datainspektionen, Kommerskollegium (endast avd. III), Riksförsäkringsverket, Spri, Barnombudsmannen (endast avd. III), Post- och telestyrelsen, Vägverket (endast avd. III), Kommunikationsforskningsberedningen, Statskontoret, Generaltullstyrelsen, Statistiska centralbyrån, Finansinspektionen, Riksrevisionsverket, Riksskatteverket, Statens löne- och pensionsverk, Skolverket (endast avd. III), Centrala studiestödsnämnden, Arbetsmarknadsstyrelsen, Ombudsmannen mot etnisk diskriminering (endast avd. III), Riksarkivet, Närings- och teknikutvecklingsverket, Sprängämnesinspektionen (endast avd. III), Patent- och registreringsverket, Konsumentverket, Länsstyrelsen i Jämtlands län, Lantmäteriverket, Juridiska fakultetsnämnden vid Uppsala universitet, Juridiska fakultetsnämnden vid Stockholms universitet, Umeå universitet (endast avd. III), Svenska kommunförbundet, Stockholms kommun, Linköpings kommun, Kalmar kommun, Landstingsförbundet, Svenska kyrkans församlings- och pastoratsförbund, Sveriges Advokatsamfund, Sveriges Köpmannaförbund, Industriförbundet, Tjänstemännens centralorganisation, Centralorganisationen SACO/SR, Landsorganisationen i Sverige, Svenska Arbetsgivareföreningen, Företagens Uppgiftslämnardelegation, Föreningen Auktoriserade Revisiorer, Publicistklubben (endast avd. III), Svenska Journalistförbundet (endast avd. III), Svenska Tidningsutgivareföreningen (endast avd. III), Allmänhetens pressombudsman (endast avd. III), Svenska Bankföreningen, Föreningen Säkrad Elektronisk Informationshantering i Samhället, Dataföreningen i Sverige, Intresseföreningen TeleTrusT Sverige, Svenska IT-företagens Organisation, Informationsproducentföreningen i Sverige, EDI i Sverige, Posten AB, Telia AB, Näringslivets Telekommitté (endast avd. III), Tele2 AB (endast avd. III), FC Sweden AB (endast avd. III), BAS (endast avd. III), Agora Nätverket (endast avd. III), SAPnet (endast avd. III), NUBBS (endast avd. III), BBS-Moderat (endast avd. III), Business Software Alliance (endast avd. III), Swebizz, Jacob Palme, Svensk byggtjänst, Arkivrådet, Swedman och Advokatfirman Delphi Lawyers.

Lagrådsremissens lagförslag

Lagtext

Regeringen har följande förslag till lagtext.

Förslag till lag om kvalificerade elektroniska signaturer

Härigenom föreskrivs följande[1].

Allmän bestämmelse

1 § Denna lag innehåller bestämmelser om kvalificerade certifikat för elektroniska signaturer, om anordningar för signaturframställning och om certifikatutfärdare som är etablerade i Sverige och som utfärdar kvalificerade certifikat till allmänheten.

Definitioner

2 § I lagen avses med

elektronisk signatur: data i elektronisk form som är fogade till eller logiskt knutna till andra elektroniska data och som används för att kontrollera att innehållet härrör från den som framstår som utställare och att det inte har förvanskats,

avancerad elektronisk signatur: elektronisk signatur som är

a) knuten uteslutande till en undertecknare,

b) möjlig att identifiera undertecknaren genom,

c) skapad med hjälpmedel som endast undertecknaren kontrollerar, och

d) knuten till andra elektroniska data på ett sådant sätt att ändringar av dessa data kan upptäckas,

kvalificerad elektronisk signatur: avancerad elektronisk signatur som är baserad på ett kvalificerat certifikat och som är skapad av en säker anordning för signaturframställning,

undertecknare: fysisk person som innehar en anordning för signaturframställning,

signaturframställningsdata: unika data, såsom koder eller hemliga krypteringsnycklar, som används för att skapa en elektronisk signatur,

anordning för signaturframställning: maskin- eller programvara för användning av signaturframställningsdata,

säker anordning för signaturframställning: anordning för signaturframställning som uppfyller kraven i 4 §,

signaturverifieringsdata: data, såsom koder eller öppna krypteringsnycklar, som används för att verifiera en elektronisk signatur,

[1] Jfr Europaparlamentets och rådets direktiv 1999/93/EG av den 13 december 1999 om ett gemenskapsramverk för elektroniska signaturer (EGT L 13, 19.1.2000, s. 12, Celex 399L0093).

certifikat: intyg i elektronisk form som kopplar ihop signaturverifieringsdata med en undertecknare och bekräftar dennes identitet,

kvalificerat certifikat: certifikat som uppfyller kraven i 3 §,

certifikatutfärdare: den som utfärdar certifikat eller som garanterar att någon annans certifikat uppfyller vissa krav.

Kvalificerade certifikat

3 § För att ett certifikat skall få kallas kvalificerat skall det vara utfärdat för viss tid av en certifikatutfärdare som uppfyller kraven i 8–11 §§ och föreskrifter meddelade med stöd av 12 § samt innehålla

1. uppgift om att det utfärdats som ett kvalificerat certifikat,
2. certifikatutfärdarens namn och adress samt uppgift om etableringsland,
3. undertecknarens namn eller pseudonym med uppgift om att det är en pseudonym,
4. särskilda uppgifter om undertecknaren, om de är relevanta för ändamålet med certifikatet,
5. signaturverifieringsdata som motsvarar de signaturframställningsdata som undertecknaren vid tidpunkten för utfärdandet har kontroll över,
6. uppgift om certifikatets giltighetstid,
7. certifikatets identifieringskod,
8. certifikatutfärdarens avancerade elektroniska signatur eller en elektronisk signatur med motsvarande säkerhetsnivå, och
9. uppgift om eventuella begränsningar av certifikatets användningsområde eller av värdet på de transaktioner för vilka certifikatet kan användas (transaktionsbelopp).

Om ett certifikat som uppfyller kraven i första stycket utfärdats av en certifikatutfärdare som inte är etablerad i Sverige skall certifikatet anses kvalificerat om

1. certifikatutfärdaren är etablerad inom Europeiska ekonomiska samarbetsområdet,
2. certifikatutfärdaren uppfyller kraven i 7–11 §§ och föreskrifter meddelade med stöd av 12 § och har ackrediterats inom Europeiska ekonomiska samarbetsområdet, eller
3. certifikatet garanteras vara kvalificerat av en certifikatutfärdare som uppfyller kraven i 7–11 §§ och föreskrifter meddelade med stöd av 12 § och som är etablerad inom Europeiska ekonomiska samarbetsområdet.

Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela närmare föreskrifter om krav enligt första stycket.

Säkra anordningar för signaturframställning

4 § En anordning för signaturframställning som anges vara säker skall säkerställa att signaturen är tillfredsställande skyddad mot förfalskning. Anordningen skall även säkerställa att signaturframställningsdata

1. i praktiken kan förekomma endast en gång,
2. med rimlig säkerhet inte kan härledas, och

3. på ett tillfredsställande sätt kan skyddas, så att obehöriga inte kan komma åt eller använda dem.

Anordningen får inte förändra de uppgifter som skall signeras eller hindra att de presenteras för undertecknaren före signeringen.

5 § Kraven på en säker anordning för signaturframställning i 4 § skall anses uppfyllda för sådan maskin- eller programvara som överensstämmer med standarder för produkter för elektroniska signaturer som Europeiska gemenskapernas kommission fastställt och offentliggjort referensnummer till i Europeiska gemenskapernas officiella tidning.

6 § En anordning som anges vara en säker anordning för signaturframställning får släppas ut på marknaden eller användas för att skapa en kvalificerad elektronisk signatur endast om ett för ändamålet anmält organ bedömt att anordningen uppfyller kraven i 4 §.

Organ som avses i första stycket utses enligt bestämmelserna i lagen (1992:1119) om teknisk kontroll.

Med ett avgörande enligt första stycket likställs ett avgörande av ett organ som utsetts för detta ändamål i en annan stat inom Europeiska ekonomiska samarbetsområdet.

Utfärdande av kvalificerade certifikat

7 § En certifikatutfärdare som avser att utfärda kvalificerade certifikat till allmänheten är skyldig att anmäla detta hos den myndighet som regeringen bestämmer (tillsynsmyndigheten) innan verksamheten påbörjas.

8 § En certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten skall bedriva verksamheten med den pålitlighet som krävs. Detta innebär att certifikatutfärdaren skall

1. ha personal med tillräcklig kompetens för de tjänster som erbjuds, särskilt vad avser ledning, teknik och säkerhetsrutiner,
2. använda sådana rutiner för administration och ledning som uppfyller erkända standarder,
3. använda pålitliga system och produkter som är skyddade mot ändringar och som garanterar teknisk och kryptografisk säkerhet,
4. förfoga över tillräckliga ekonomiska medel för att kunna bedriva verksamheten enligt denna lag och bära risken för skadeståndsskyldighet,
5. ha säkra rutiner för identitetskontroll av de undertecknare som kvalificerade certifikat utfärdas till,
6. förfoga över ett snabbt och säkert system för registrering och omedelbar spärrning av kvalificerade certifikat, och
7. vidta åtgärder mot förfalskning av kvalificerade certifikat och i förekommande fall garantera att tillhandahållandet av signaturframställningsdata sker konfidentiellt.

Kraven i första stycket 3 skall anses uppfyllda för sådan maskin- eller programvara som överensstämmer med harmoniserade standarder för produkter för elektroniska signaturer till vilka Europeiska gemenskapernas kommission fastställt och offentliggjort referensnummer i Europeiska gemenskapernas officiella tidning.

9 § En certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten skall

1. omedelbart spärra ett certifikat när undertecknaren begär det eller när det annars finns anledning till det,
2. säkerställa att exakt tidpunkt kan anges för utfärdande och spärrning av certifikat, och
3. endast framställa signaturframställningsdata och signaturverifieringsdata som kan användas som komplement till varandra.

10 § En certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten skall bevara all relevant information om certifikaten under rimlig tid. Certifikatutfärdaren skall även använda tillförlitliga system för lagring av kvalificerade certifikat i verifierbar form, så att

1. endast behöriga personer kan göra tillägg och ändringar,
2. uppgifternas äkthet kan kontrolleras,
3. certifikaten är offentligt tillgängliga endast när innehavarna av certifikaten har lämnat sitt samtycke, och
4. tekniska förändringar som äventyrar säkerhetskraven är synbara för den som handhar systemet.

Certifikatutfärdaren får inte lagra eller kopiera signaturframställningsdata.

11 § Innan en certifikatutfärdare ingår avtal om att utfärda ett kvalificerat certifikat skall certifikatutfärdaren skriftligen informera motparten om

1. villkoren och begränsningarna för användning av certifikatet,
2. förekomsten av frivilliga ackrediterings- eller certifieringssystem enligt lagen (1992:1119) om teknisk kontroll, och
3. förfaranden för klagomål och avgörande av tvister.

Informationen enligt första stycket får överföras elektroniskt, om det sker i en för motparten omedelbart läsbar form. Informationen skall på begäran också göras tillgänglig för annan som är beroende av certifikatet.

12 § Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får utfärda närmare bestämmelser om krav enligt 8–11 §§.

Skadestånd

13 § En certifikatutfärdare som till allmänheten utfärdar certifikat som anges vara kvalificerade skall ersätta den skada som åsamkats den som förlitat sig på certifikatet, om skadan uppkommit genom att

1. certifikatutfärdaren inte har uppfyllt kraven i 9 §,
2. certifikatet inte uppfyller kraven i 3 § första stycket, eller
3. certifikatet vid utfärdandet innehöll felaktiga uppgifter.

Vad som sägs i första stycket 2 och 3 gäller även en certifikatutfärdare som garanterar att en annan certifikatutfärdares certifikat är kvalificerade.

Certifikatutfärdaren är dock inte skyldig att betala ersättning om utfärdaren kan visa att skadan inte har orsakats av vårdslöshet hos utfärdaren själv. Certifikatutfärdaren är inte heller ersättningsskyldig för en skada som härrör från att ett kvalificerat certifikat använts i strid med

begränsningar som gäller användningsområde eller transaktionsbelopp och som tydligt angetts i certifikatet.

14 § Avtalsvillkor som i jämförelse med 13 § är till nackdel för den som förlitar sig på certifikatet är utan verkan mot denne.

Behandling av personuppgifter

15 § En certifikatutfärdare som utfärdar certifikat till allmänheten får inhämta personuppgifter endast direkt från den som uppgifterna avser eller med dennes uttryckliga samtycke och endast i den utsträckning som är nödvändig för att utfärda eller upprätthålla ett certifikat. Uppgifterna får inte samlas in eller behandlas för andra ändamål utan uttryckligt samtycke från den som uppgifterna avser.

Kvalificerade elektroniska signaturer

16 § Om det i lag eller annan författning ställs krav på egenhändig underskrift eller motsvarande och om det är tillåtet att uppfylla kravet med elektroniska medel, skall en kvalificerad elektronisk signatur alltid anses uppfylla kravet.

Användningen av elektroniska signaturer inom eller vid kommunikation med den offentliga sektorn kan vara förenad med ytterligare krav.

Tillsyn

17 § Tillsynsmyndigheten skall ha tillsyn över certifikatutfärdare som till allmänheten utfärdar certifikat som anges vara kvalificerade och över anordningar som anges vara säkra anordningar för signaturframställning.

18 § Tillsynsmyndigheten har rätt att på begäran få de upplysningar och ta del av de handlingar som behövs för tillsynen.

Tillsynsmyndigheten har också rätt att få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, där verksamhet som står under tillsyn bedrivs.

Tillsynsmyndigheten har rätt att få verkställighet hos kronofogdemyndigheten av de beslut som avser åtgärder för tillsynen enligt första och andra styckena. För sådana beslut gäller bestämmelserna i utsökningsbalken.

19 § Tillsynsmyndigheten får meddela de förelägganden och förbud som behövs för efterlevnaden av denna lag eller av föreskrifter som meddelats med stöd av lagen.

20 § Tillsynsmyndigheten får förelägga certifikatutfärdare som till allmänheten utfärdar certifikat som anges vara kvalificerade att helt eller delvis upphöra med denna verksamhet. Sådana beslut får dock fattas endast om mindre ingripande åtgärder visat sig vara verkningslösa. Myndigheten får besluta hur verksamheten skall avvecklas.

21 § Förelägganden och förbud enligt denna lag får förenas med vite.

Avgifter

22 § Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får föreskriva om skyldighet för certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten att betala avgift för tillsynsmyndighetens verksamhet enligt denna lag.

Överklagande

23 § Tillsynsmyndighetens beslut enligt denna lag eller enligt föreskrifter som meddelats med stöd av lagen får överklagas hos allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Tillsynsmyndigheten får bestämma att beslut enligt denna lag skall gälla omedelbart.

---

1. Denna lag träder i kraft den 1 januari 2001.

2. Bestämmelsen i 7 § skall inte börja tillämpas förrän den 1 februari 2001 i fråga om certifikatutfärdare som redan före ikraftträdandet utfärdar sådana certifikat som medför anmälningsplikt.

Förslag till lag om ändring i sekretesslagen (1980:100)

Härigenom föreskrivs att 5 kap. 3 § sekretesslagen (1980:100)[1] skall ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
5 kap.	
3 §[2]	
Sekretess gäller för uppgift som lämnar eller kan bidra till upplysning om chiffer, kod eller liknande metod som har till syfte att underlätta befordran eller användning i allmän verksamhet av uppgifter utan att föreskriven sekretess åsidosätts, om det kan antas att syftet med metoden motverkas om uppgiften röjs.	Sekretess gäller för uppgift som lämnar eller kan bidra till upplysning om chiffer, kod eller liknande metod som har till syfte att *1.* underlätta befordran eller användning i allmän verksamhet av uppgifter utan att föreskriven sekretess åsidosätts, *eller* *2. göra det möjligt att kontrollera om uppgifter har förvanskats,* om det kan antas att syftet med metoden motverkas om uppgiften röjs.

Sekretess gäller i verksamhet som avser förande av eller uttag ur körkortsregistret för uppgift om körkorts referensnummer, om det inte står klart att uppgiften kan röjas utan fara för att kontrollen av körkorts äkthet motverkas om uppgiften röjs.

Denna lag träder i kraft den 1 januari 2001.

[1] Lagen omtryckt 1992:1474.
[2] Senaste lydelse 1994:595.

Lagrådets yttrande

Utdrag ur protokoll vid sammanträde 2000-04-11

Närvarande: f.d. justitierådet Lars Å. Beckman, regeringsrådet Susanne Billum, justitierådet Göran Regner.

Enligt en lagrådsremiss den 30 mars 2000 (Näringsdepartementet) har regeringen beslutat inhämta Lagrådets yttrande över förslag till

1. lag om kvalificerade elektroniska signaturer,
2. lag om ändring i sekretesslagen (1980:100).

Förslagen har inför Lagrådet föredragits av hovrättsassessorn Lena Klintefall Råssjö.

Förslagen föranleder följande yttrande av *Lagrådet:*

Förslaget till lag om kvalificerade elektroniska signaturer

Enligt 1 § innehåller lagen bestämmelser om kvalificerade certifikat för elektroniska signaturer, om anordningar för signaturframställning och om certifikatutfärdare som är etablerade i Sverige och som utfärdar kvalificerade certifikat för allmänheten. Det vore en mera adekvat benämning på lagen om denna fick rubriken ”lag om kvalificerade certifikat för elektroniska signaturer”, vilket är lagens huvudsakliga ämnesområde.

1 §

Den allmänna bestämmelsen i 1 § skall enligt författningskommentaren ange lagens tillämpningsområde. Därvid åsyftas det sista ledet i bestämmelsen som avser certifikatutfärdare som är etablerade i Sverige och som utfärdar kvalificerade certifikat. Tidigare led av bestämmelsen är närmast att uppfatta som någon form av innehållsdeklaration, som dock inte är fullständig. För att skilja de två olika delarna av paragrafen åt torde det sista ledet böra bilda ett andra stycke i paragrafen med förslagsvis följande lydelse: ”Lagen gäller sådana certifikatutfärdare som utfärdar kvalificerade certifikat och som är etablerade i Sverige.” I så fall kan första stycket ange att syftet med lagen är att underlätta användningen av elektroniska signaturer genom bestämmelser om säkra anordningar för signaturframställning, kvalificerade certifikat för sådana signaturer och utfärdare av certifikat.

3 §

I paragrafen finns föreskrifter om vad ett kvalificerat certifikat skall innehålla. I de följande 4–6 §§ har tagits in bestämmelser om säkra anordningar för signaturframställning. Därefter har i 7–12 §§ förts in regler om certifikatutfärdare. Enligt Lagrådets mening skulle förståelsen av bestämmelserna underlättas om de paragrafer som behandlar certifikat och certifikatutfärdare fördes samman i ett avsnitt. Lagrådet föreslår därför att 3 § flyttas ner efter 6 § i lagförslaget.

Första stycket i 3 § innehåller bestämmelserna om vad ett kvalificerat certifikat skall innehålla. Andra stycket däremot reglerar när certifikat utfärdade av någon som är etablerad i annat EES-land eller i tredje land skall anses vara kvalificerade. Med hänsyn till att styckena reglerar helt olika frågor bör andra stycket brytas ut till en särskild paragraf. Den nya paragrafen bör efter en viss omredigering ges följande lydelse:

”Om ett certifikat som uppfyller kraven i (3 §) första stycket 1–9 utfärdats av en certifikatutfärdare som inte är etablerad i Sverige skall certifikatet anses kvalificerat om

1. certifikatutfärdaren är etablerad i en annan stat inom Europeiska ekonomiska samarbetsområdet och där får utfärda kvalificerade certifikat,

2. certifikatutfärdaren uppfyller krav som motsvarar dem som anges i (8–11 §§) och föreskrifter meddelade med stöd av (12 §), och är ackrediterad i en annan stat inom Europeiska ekonomiska samarbetsområdet, eller

3. certifikatet garanteras vara kvalificerat av en certifikatutfärdare som avses i 1 eller i (3 § första stycket).”

10 §

I paragrafen föreskrivs en skyldighet för certifikatutfärdare att bevara all relevant information om certifikaten under ”rimlig tid”. Enligt författningskommentaren får vad som är rimlig tid avgöras med hänsyn till vilken typ av certifikat som utfärdas och med beaktande av krav som kan följa av t.ex. bokföringslagen. Lagrådet anser att lagtexten bör innehålla någon mer ledning för tillämparen än enbart uttrycket rimlig tid. Förslagsvis kan första meningen ges följande lydelse.

”En certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten skall bevara all relevant information om certifikaten under den tid som är motiverad med hänsyn till typen av certifikat och övriga omständigheter.”

11 §

Paragrafen innehåller bestämmelser om information som certifikatutfärdaren skall lämna. Genom paragrafen implementeras punkten k) i bilaga II till direktivet. Lagtexten bör emellertid utformas i närmare överensstämmelse med direktivtexten. Lagrådet förordar att paragrafen ges följande lydelse:

”Innan en certifikatutfärdare ingår avtal om att utfärda ett kvalificerat certifikat skall certifikatutfärdaren skriftligen och på ett lättbegripligt språk informera motparten om

1. begränsningar och andra villkor för användning av certifikatet,

2. frivillig ackreditering eller certifiering som avses i lagen (1992:1119) om teknisk kontroll, och

3. förfaranden för klagomål och avgörande av tvister.

Informationen enligt första stycket får överföras elektroniskt.

Informationen skall göras tillgänglig också för annan som är beroende av certifikatet och som begär att få den.”

16 §

I andra stycket av den föreslagna paragrafen anges att användningen av elektroniska signaturer inom eller vid kommunikation med den offentliga sektorn kan vara förenad med ytterligare krav. Formuleringen ansluter till uttryckssättet i det aktuella EG-direktivet. Uttrycket ”den offentliga sektorn” är dock vagt. Det synes t.ex. tveksamt om avsikten är att strängare bestämmelser skall kunna uppställas för statliga eller kommunala bolag med enbart affärsmässig eller förvaltande verksamhet. Enligt Lagrådets mening bör övervägas att ge bestämmelsen en något snävare utformning vilken tydligare anknyter till myndighetsfunktionen snarare än till ett offentligt ägande. Detta synes bättre överensstämma med såväl direktivets syfte som svensk lagstiftningstradition. Lagrådet föreslår att första och andra styckena i paragrafen sammanförs, varefter bestämmelsen kan formuleras enligt följande.

”Vid kommunikation med eller mellan myndigheter kan dock användningen av elektroniska signaturer vara förenad med ytterligare krav.”

Rubriken närmast före paragrafen bör samtidigt omformuleras så att den bättre återspeglar innehållet i paragrafen. Lagrådet föreslår att rubriken ges följande lydelse.

”Användning av elektroniska signaturer i vissa fall”

17 §

I paragrafen finns bestämmelser om tillsyn. Denna skall enligt förslaget omfatta dels certifikatutfärdare som till allmänheten utfärdar certifikat som anges vara kvalificerade, dels anordningar som anges vara säkra anordningar för signaturframställning. Enligt Lagrådets mening bör undvikas att utforma bestämmelsen så att tillsynen tycks avse de tekniska anordningarna som sådana. Svårigheten kan undvikas genom att tillsynen anges avse efterlevnaden av lagen och med stöd därav utfärdade föreskrifter.

I författningskommentaren till paragrafen anges vidare att tillsynsmyndigheten torde kunna offentliggöra en förteckning över anmälda certifikatutfärdare och även ange vilka certifikatutfärdare som förelagts att upphöra med verksamheten eller att kalla sina certifikat för kvalificerade. Lagrådet vill med anledning härav framhålla att myndigheten självfallet har rätt att föra de förteckningar som den behöver för sin verksamhet. Sådana förteckningar torde i allmänhet bli att betrakta som allmänna handlingar. Härmed är dock inte sagt att myndigheten på eget initiativ kan offentligöra den ifrågavarande förteckningen (t.ex. på Internet), vari kan finnas uppgifter som eventuellt omfattas av personuppgiftslagen. Om avsikten är att förteckningen skall offentliggöras - vilket förefaller rimligt med hänsyn till allmänhetens behov av att kunna kontrollera någon som uppger sig utfärda kvalificerade certifikat - bör enligt Lagrådets mening paragrafen kompletteras med en bestämmelse som klargör detta. En sådan bestämmelse fyller även funktionen att förstärka intresset hos dem

som vill utfärda kvalificerade certifikat att fullgöra sin anmälningsskyldighet enligt 7 §.

Lagrådet förordar med hänvisning till det anförda att paragrafen ges följande lydelse.

”Tillsynsmyndigheten skall ha tillsyn över efterlevnaden av denna lag och föreskrifter som utfärdats med stöd av lagen.

Tillsynsmyndigheten skall föra och ge offentlighet åt en förteckning över certifikatutfärdare som anmält sig enligt 7 § och som enligt denna lag får utfärda kvalificerade certifikat.”

18 §

I tredje stycket talas om verkställighet av beslut som avser åtgärder för tillsyn enligt första och andra styckena i paragrafen. Det synes mindre adekvat att använda detta uttryckssätt eftersom det inte är fråga om verkställighet av några egentliga beslut utan om biträde att genomföra tillsynen. Enligt Lagrådets mening bör tredje stycket lyda: ”Tillsynsmyndigheten har rätt att få biträde av kronofogdemyndigheten för tillsyn enligt första och andra styckena.”

Övergångsbestämmelserna

Enligt 14 § är avtalsvillkor, som i jämförelse med 13 § är till nackdel för den som förlitar sig på certifikatet, utan verkan mot denne. Bestämmelsen bör inte vara tillämplig på avtal som ingåtts före ikraftträdandet. Något annat torde inte heller ha avsetts i lagrådsremissen. I övergångsbestämmelserna bör emellertid tas in en uttrycklig bestämmelse härom. Lagrådet föreslår att till övergångsbestämmelserna fogas en punkt 3 av följande lydelse:

”3. 14 § tillämpas inte på avtal som ingåtts före ikraftträdandet.”

Förslaget till lag om ändring i sekretesslagen

Den nya punkten 2 i första stycket av 5 kap. 3 § gäller sekretessbeläggning av uppgifter om metoder som har till syfte att göra det möjligt att kontrollera om uppgifter har förvanskats. Ändringen är föranledd av behovet att kunna skydda hemliga nycklar och anknytande uppgifter för bl.a. elektronisk signering och autenticering mot insyn (se avsnitt 9). Den avfattning som punkten har fått gäller dock uppgifter över huvud taget, vilket kan föra för långt. Det bör därför övervägas om inte det i punkten 2 bör talas om ”data i elektronisk form” eller liknande (jfr 2 § i den nya lagen) i stället för ”uppgifter”.

Lagrådet vill anmärka att behov av sekretess i tillsynsmyndighetens verksamhet kan föreligga också beträffande annan information än sådan som avses i punkten 2. I så fall kan sekretess föreskrivas genom ett tillägg till bilagan till sekretessförordningen (1980:657), jfr t.ex. punkt 109 i denna bilaga.

Näringsdepartementet

Utdrag ur protokoll vid regeringssammanträde den 18 maj 2000.

Närvarande: statsministern Persson, ordförande, och statsråden Hjelm-Wallén, Thalén, Lindh, Sahlin, von Sydow, Pagrotsky, Östros, Messing, Engqvist, Rosengren, Larsson, Lejon, Lövdén och Ringholm.

Föredragande: statsrådet Sahlin

Regeringen beslutar proposition 1999/2000:117 Lag om kvalificerade elektroniska signaturer, m.m.

Rättsdatablad

Författningsrubrik	Bestämmelser som inför, ändrar, upphäver eller upprepar ett normgivningsbemyndigande	Celexnummer för bakomliggande EG-regler
Lag om kvalificerade elektroniska signaturer	6, 13, 22 §§	399L0093