Förord

Denna departementspromemoria har tagits fram på initiativ av Regeringskansliets beredningsgrupp för digitala signaturer. Den är avsedd att utgöra underlag för Regeringskansliets fortsatta arbete på en svensk politik inom området digitala signaturer.

Denna promemoria finns också tillgänglig på regeringens hemsida Information Rosenbad, på följande adress:

http://www.regeringen.se/info_rosenbad/departement/kommunikation/kommunikation_utredningar.html

Samtliga intresserade är välkomna att lämna synpunkter på promemorian. Dessa skall vara Regeringskansliet tillhanda senast den 20 april 1998, och kan inlämnas till följande adresser och nummer.

Kommunikationsdepartementet
103 33 Stockholm

Telefax: 08-411 89 43

E-post: registrator@communications.ministry.se

Innehållsförteckning

Sammanfattning

En digital signatur kan användas för att säkerställa att en elektroniskt överförd informationsmängd inte har förändrats, för att säkerställa vem informationens avsändare är samt förhindra att avsändaren senare förnekar meddelandet. I promemorian redogörs inledningsvis för den kryptografiska teknik som används för att skapa digitala signaturer. Därefter skildras den tekniska utrustning i form av programvara, hårdvara m.m. som erfordras för att använda digitala signaturer. Möjligheterna att separera funktionerna för signering och kryptering påvisas.

Kopplingen mellan en digital signatur och en bestämd person intygas i ett certifikat. Certifikatet utfärdas av en betrodd tredje part, ett certifieringsorgan (Certification Authority, CA). CA:s funktion och uppgifter för att systemet för digitala signaturer skall bli så tillförlitligt som möjligt skildras i promemorian. Vidare uppmärksammas de hot och risker som finns mot systemet.

Digitala signaturer har redan vunnit utbredd tillämpning, i Sverige och internationellt. Promemorian beskriver bl.a. svenska projekt som Allterminalen och det arbete som gjorts inom samarbetsorganet Säkrad Elektronisk Information i Samhället (SEIS).

Vidare behandlas i promemorian de rättsliga aspekterna av digitala signaturer. Härvid redogörs först för de krav svensk rätt ställer vad gäller skriftlighet och egenhändig namnteckning. Frågeställningarna kring bevisning i IT-miljö berörs. Datastraffrättsutredningens betänkande (SOU 1992:110) refereras kort beträffande straffrättsliga och straffprocessuella frågor, liksom den lagstiftning och de utredningsförslag inom det förvaltningsrättsliga området som finns. En ingående översikt av aktiviteten i internationella organ och i Italien, Tyskland, Danmark och USA vad avser digitala signaturer görs med syftet att presentera modeller som kan vara till ledning för

lagstiftaren. Behovet av regler för signaturnyckelcertifikatets innehåll och verkan samt för auktorisation och kontroll av CA analyseras. Frågor om ansvar för CA, den signerande parten, den förlitande parten och statens ansvar tas upp. Regler till skydd för individens personliga integritet belyses översiktligt.

Sårbarhetsaspekter för samhället granskas. Funktionshindrades problem och behov uppmärksammas.

Avslutningsvis skisseras tänkbara handlingsvägar för lagstiftaren. Sverige har hittills begränsat lagreglering av digitala signaturer till avgränsade områden. Utredningsförslag om generell reglering inom straff- och förvaltningsrätten av digitala signaturer har hittills inte föranlett lagstiftning. Om förslagen i nämnda utredningar kompletteras med en näringsrättslig reglering av CA-verksamhet skulle ett mer omfattande införande av digitala signaturer kunna underlättas. Samhällets behov av effektiv brottsbekämpning och säkerhetsskydd måste härvid beaktas, liksom Sveriges internationella åtaganden beträffande export av s.k. strategiska produkter.

1 Inledning

I det dagliga livet är vår namnteckning en nödvändighet för att genomföra olika transaktioner såväl i affärslivet, i förhållande till myndigheter och i privatlivet. För att få ett tillförlitligt hyresavtal, få ut paket på postkontoret, betala med check eller få ut kontanter av bankkassörskan fordras som regel en underskrift. Namnteckningen fungerar som en bekräftelse på att vi har mottagit pengarna eller accepterar villkoren i avtalet.

I takt med att vi utför allt fler affärstransaktioner över telenät behövs elektroniska ersättare för denna visuella bekräftelse. Sedan länge har vi t.ex. accepterat en fyrställig PIN-kod [1] som bekräftelse på att vi vill få ut kontanter från en bankomat. Genom ett avtal med vår bank har vi accepterat att dessa fyra siffror ersätter namnteckningen som bekräftelse på denna typ av transaktion från våra bankkonton. Meddelanden om t.ex. begäran om utbetalning befordras i ett privat, slutet, nät som förbinder de anslutna bankernas terminaler med varandra och som bankerna har kontroll över.

När vi i ökad utsträckning vill använda Internet eller andra allmänt tillgängliga telenät för bankaffärer och för i stort sett all form av informationsutbyte och alla typer av affärstransaktioner, är det nödvändigt med lösningar som ger åtminstone motsvarande säkerhet och trygghet som vid bankomatuttag. På samma sätt som vi kan använda namnteckningen för olika ändamål behöver vi generella lösningar för identifiering och bekräftelse som inte kräver speciell teknik och separata juridiska överenskommelser med varje part som vi skall göra affärer eller ha annat utbyte med.

En sådan lösning erbjuds genom användning av certifikat och kryptografiska nyckelpar, med vars hjälp digitala signaturer för ett

[1] Personal Identification Number

meddelande kan skapas och verifieras. Genom dessa kan en mottagare identifiera en sändare av ett signerat meddelande, t.ex. affärspartners och andra i deras egenskap av fysisk eller juridisk person, kontohavare, klubbmedlem, befattningshavare eller annan roll, i vilken den elektroniska transaktionen genomförs. Dessa digitala identitetsbevis motsvarar våra delvis visuella ID-kort, pass, magnetiska konto-, bank-, kredit-, medlems- och anställningskort och andra fysiska identitetshandlingar. De elektroniska certifikat som används utgör en slags motsvarighet till det kontobevis som informationen på magnetkortet utgör för våra uttag i bankomater. Magnetkortet ihop med den personliga PIN-koden avses ge tillräckligt hög säkerhet för att det är rätt kontohavare som gör bankomattransaktionen. Inför affärstransaktioner över allmänt tillgängliga nät kan samma metod användas för att signera handlingar. Därvid kan exempelvis ett certifikat användas för att lagra identitetsinformationen. Detta tillsammans med en PIN-kod kan ge en tillräckligt säker identifiering om avsändaren och säkerhet för innehållet i meddelandet. Det anses ibland mer ändamålsenligt att lagra informationen på annat sätt, t.ex. direkt tillgänglig för hårdvaran. De exempel som förekommer i promemorian innebär inget ställningstagande beträffande lämplig lagringsmetod i det enskilda fallet.

På samma sätt som vår namnteckning kan användas både som en bekräftelse på en avsiktsförklaring och för att styrka identiteten (genom att t.ex. jämföra med underskriften på baksidan av ett kreditkort) så kan en digital signatur användas för båda dessa funktioner. För att en användare skall vara fullt medveten om huruvida han identifierar sig för att genomföra en banktransaktion eller om han bekräftar sin avsikt att genomföra transaktionen brukar man skilja på elektronisk identifiering och digital signatur. Av praktiska och ekonomiska skäl kan, vid ett kortbaserat system, oftast de krypteringsnycklar som används för identifiering respektive signering lagras på samma aktiva kort. Elektroniska ID-kort kan således t.ex. rymma såväl information som används för att säkert identifiera en person som vill kontrollera sin elektroniska sjukjournal, men den kan också innehålla funktioner som behövs för att skapa hans

digitala signatur eller som bekräftelse på t.ex. en elektroniskt ifylld deklarationsblankett.

Ända sedan Internet-utvecklingen tog fart för ca fyra år sedan har bristande säkerhet framhållits som det stora hindret för ett effektivt nyttjande av Internet och andra öppna nät för elektronisk handel och andra transaktioner. Marknadstrycket från både leverantörer och användare har lett fram till en mycket snabb utveckling och acceptans av en rad de-facto-standarder för krypterad dataöverföring (SSL), e-post (S/MIME) och elektroniska avtalsslut (EDI) samt elektroniska certifikat (X.509).

Denna departementspromemoria behandlar problem och behov rörande digitala signaturer ur teknisk, administrativ och rättslig synvinkel. Promemorian innehåller även vissa förslag till handlingsvägar.

Promemorian behandlar delvis samma områden som Regeringskansliets rapport ”Kryptopolitik – möjliga svenska handlingslinjer” från oktober 1997 samt EG-kommissionens meddelande ”Om säkerhet och pålitlighet vid elektronisk kommunikation – Mot en europeisk ram för kryptering och digitala signaturer” (KOM(97) 503 slutlig). Promemorian gör emellertid en betydligt djupare analys, från ett specifikt svenskt perspektiv, av de rättsliga och praktiska aspekterna kring digitala signaturer.

Till stöd för arbetet med denna promemoria har en beredningsgrupp bildats inom Regeringskansliet, bestående av representanter från Justitie-, Utrikes-, Försvars-, Kommunikations-, Finans-, Inrikes- samt Närings- och handelsdepartementet.

I arbetet har det även ingått representanter från Post- och telestyrelsen. Samråd har skett med en bred grupp referenspersoner, *se bilaga 11.*

2 Vad en digital signatur är

2.1 Teknisk beskrivning av hur digitala signaturer skapas

2.1.1 Definition

Digital signatur är definierad i ISO 7498-2 standarden som:

Data appended to, or a cryptographic transformation of, a data unit that allows the recipient of that data to prove the source and integrity of the data unit. It protects against forgery, even by the recipient.

En annan definition kan hämtas ur SOU 1996:40:[2]

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.

En ytterligare förklaring har Statskontoret givit i skriften Svenska delen av Internet:[3]

Omvandling av ett meddelande (eller ett kondensat av detta) på ett sätt som endast avsändaren kan utföra och som låter mottagaren kontrollera meddelandets äkthet, innehåll och avsändarens identitet.

[2] SOU 1996:40 Elektronisk dokumenthantering, s. 39.
[3] Statskontorets rapport 1997:18 ”Svenska delen av Internet”, Stockholm oktober 1997.

En digital signatur kan användas både för att garantera att en informationsmängd inte har förändrats och för att säkert identifiera avsändaren.

Framställning och verifiering av digitala signaturer baseras på avancerade kryptografiska metoder och s.k. hashfunktioner. Nedan följer en översiktlig beskrivning av de tekniker som används.

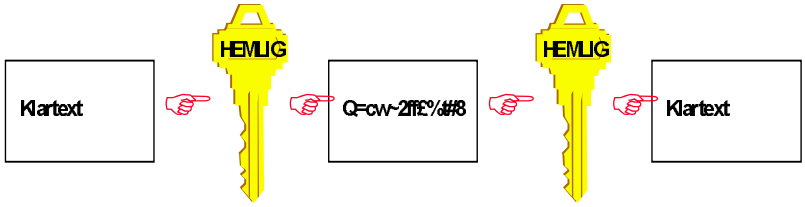
2.1.2 Kryptografiska tekniker

Kryptoteknik bygger på att innehållet i meddelandet omvandlas efter en i förväg bestämd metod, en algoritm. En sådan metod kan finnas i många varianter. Om två personer skall kommunicera måste de komma överens om både algoritm och variant. Varianten måste hållas hemlig men inte nödvändigtvis algoritmen. Kryptografiska tekniker har traditionellt sett använts för att skydda datamängder mot insyn, för att skapa konfidentialitet. På senare tid har nya kryptometoder utvecklats som gör det möjligt att även skapa ett upphovs- och förändringsskydd. Det är dessa senare metoder som öppnat vägen för digitala signaturer.

Det finns två sorters krypteringsalgoritmer, symmetriska och asymmetriska. Den kanske mest kända krypteringsalgoritmen som används i dag, Data Encryption Standard (DES), är symmetrisk. Den används vanligen för skydd av konfidentialitet, inte för signering och verifiering av dokumentets integritet.

Symmetrisk kryptering

Den symmetriska krypteringstekniken är den äldsta och mest beprövade tekniken. Tekniken baseras på att sändare och mottagare använder samma (gemensamma) nyckel för både kryptering och dekryptering. Genom att samma nyckel används måste denna nyckel hållas hemlig för alla andra som inte skall kunna kryptera/dekryptera den datamängd som sänds eller tas emot. Detta faktum har medfört att tekniken ibland även kallas för en-nyckelsystem eller hemlig-nyckelsystem.



Figur 1. Symmetrisk kryptering

Fördelen med symmetrisk kryptering är att den är beprövad och att krypteringsalgoritmerna kan begränsas i sin komplexitet. Det är därför en snabb krypteringsteknik. Den stora nackdelen med symmetrisk kryptering är emellertid problemet med nyckelhanteringen. Mottagaren av ett krypterat meddelande måste få vetskap om den hemliga nyckeln utan att någon obehörig också får det.

Några av de vanligaste krypteringsalgoritmerna är DES, RC2, RC4 och IDEA. Av dessa är DES vanligast och en sedan länge använd metod med 56-bitars nyckellängd som fortfarande anses säker. För att höja säkerheten ytterligare kan Triple-DES användas. Triple-DES kan enkelt beskrivas som DES-algoritmen upprepad tre gånger. Den effektiva nyckellängden blir då 112 bitar.

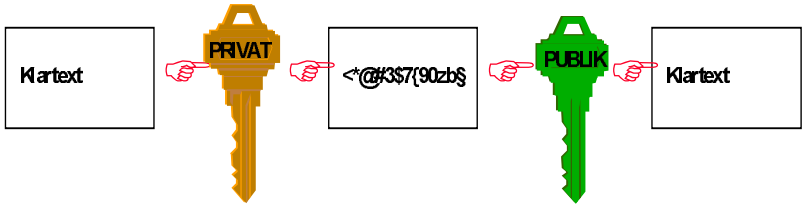
Asymmetrisk kryptering

Asymmetrisk kryptering är en förhållandevis ny teknik som utnyttjar två skilda nycklar vid kryptering respektive dekryptering. Nycklarna utgör ett par som består av en hemlig, privat, nyckel och en publik, öppen, nyckel. Asymmetrisk kryptering kallas även publik-nyckelsystem. Två viktiga faktorer definierar tekniken: 1) ett krypterat meddelande kan inte dekrypteras med samma nyckel i nyckelparet, 2) trots kunskap om den ena nyckeln i nyckelparet är det omöjligt att beräkna den andra nyckeln. De två nycklarna är därmed beroende av varandra och bildar ett unikt par. Den stora fördelen med tekniken är att den förenklar och säkrar nyckeladministrationen avsevärt. Den privata nyckeln bevaras hemlig hos ägaren medan den öppna görs tillgänglig för omvärlden. Därigenom

kan säkerheten bevaras samtidigt som man får en snabb och enkel distribution av nycklarna.

För kryptering kan man använda antingen den öppna eller den privata nyckeln. För att uppnå en konfidentiell meddelandeöverföring använder avsändaren mottagarens lättillgängliga öppna nyckel för kryptering. Den enda som sedan kan dekryptera detta meddelande är den som har tillgång till mottagarens privata nyckel.

Om avsändaren i stället använder sin privata nyckel för kryptering, så kan alla i omvärlden dekryptera meddelandet med hjälp av avsändarens öppna nyckel. Om meddelandet, efter dekryptering, verkar rimligt så är detta ett bevis på att meddelandet verkligen har krypterats med avsändarens privata nyckel. Det är denna funktion som används när digitala signaturer skapas.



Figur 2. Asymmetrisk kryptering

Asymmetrisk kryptering är alltså en förutsättning för digitala signaturer, där sändaren skapar signaturen med sin privata nyckel och mottagaren verifierar med den korresponderande öppna (publika).

Även om det finns ett antal olika asymmetriska krypteringsalgoritmer har RSA utvecklats till att bli en de facto-standard. RSA utvecklades 1978 av Rivest, Shamir och Adleman och fick sitt namn från deras initialer.

Nackdelen med RSA – och asymmetrisk kryptering generellt – är att algoritmerna är mycket komplexa och kräver mycket processorkraft för att beräknas. Det tar därför förhållandevis lång tid att kryptera data med hjälp av RSA. På grund av detta krypterar man ofta den symmetriska nyckeln med en asymmetrisk algoritm. Denna säkert överförda nyckel används sedan till att dekryptera den datamängd som skall utbytas.

Elliptiska kurvor

En matematisk grund för att skapa effektivare signaturalgoritmer finns redan. Algoritmer baserade på elliptiska funktioner håller på att utvecklas. Standarder tas f.n. fram.

2.1.3 Hashfunktioner

En digital signatur är en funktion som garanterar innehållet och äktheten hos en elektronisk handling. Funktionen uppnås genom en kombination av asymmetrisk krypteringsteknik och hashfunktionsteknik. Hashfunktionen används först för att skapa en komprimerad mängd av den elektroniska handlingen som därmed är hårt bunden till ursprungsmeddelandet medan den asymmetriska krypteringen (med den privata hemliga nyckeln) binder upphovsmannen till den komprimerade mängden.

En hashfunktion är en beräkningsalgoritm som omvandlar en variabel mängd data till ett värde av fix längd (ca 64 – 128 bitar). Värdet kallas kondensat, dvs. en komprimerad mängd, hashvärde, hashsumma, checksumma, fingeravtryck m.m. Hashfunktioner kan användas till flera ändamål där ett kondensat av en större mängd data är önskvärt. Ett användningsområde är digitala signaturer. Hashfunktioner som används till digitala signaturer måste vara s.k. envägs-hashfunktioner som skapar ett unikt och inte omvändbart hashvärde för varje ny mängd data. Hashfunktionen skall skapa ett hashvärde från ett meddelande så att det

- med utgångspunkt från meddelandet är lätt att beräkna hashvärdet,

- med utgångspunkt från hashvärdet är omöjligt att beräkna fram det ursprungliga meddelandet, samt att det

- med utgångspunkt från meddelandet är omöjligt att ta fram ett annat nytt meddelande som genererar ett identiskt hashvärde.

De vanligaste hashfunktionerna är MD2, MD5 och SHA-1, vilka alla uppfyller ovanstående krav. Hashfunktioner gör det möjligt att på ett effektivt sett skapa digitala signaturer på stora meddelanden genom att komprimera innehållet till en hanterbar mängd.

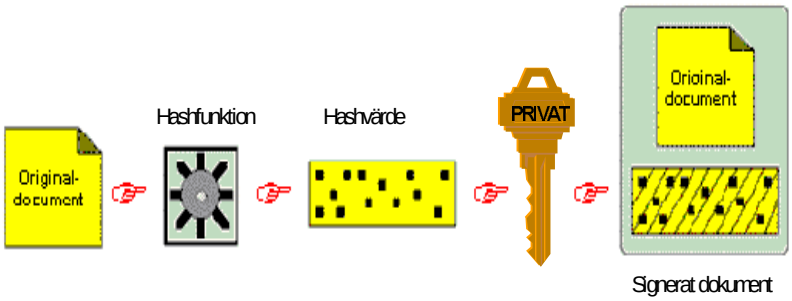
2.1.4 Signering

En digital signatur skapas i dag på följande sätt.

– Meddelandet/datamängden som skall signeras tas genom en hashfunktion, vilken skapar ett unikt, inte omvändbart och förhållandevis litet hashvärde (kondensat).

– Hashvärdet krypteras med hjälp av t.ex. en RSA-algoritm med upphovsmannens privata krypteringsnyckel.

– Det krypterade hashvärdet utgör den digitala signaturen och tillförs dokumentet.



Figur 3. Hur en digital signatur skapas

Signaturen och meddelandet kan nu öppet sändas till mottagaren. Den digitala signaturen kan i sig inte förhindra incidenter i form av att någon utomstående förändrar meddelandet etc. Däremot går det, med hjälp av signaturen, direkt att upptäcka om någon sådan

incident inträffat. Detta görs genom verifiering av den digitala signaturen.

2.1.5 Verifiering

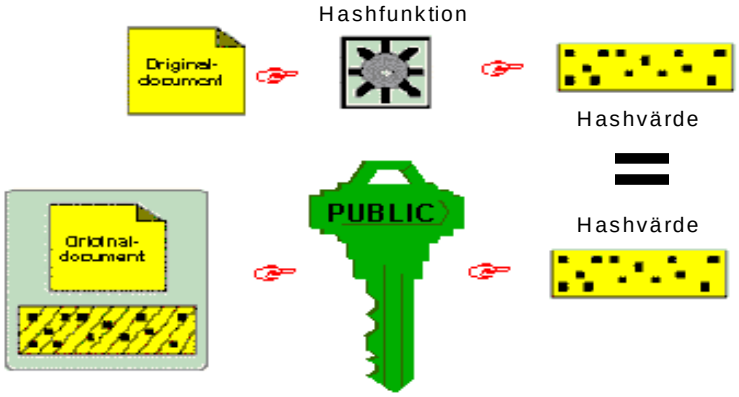
En digital signatur verifieras på följande sätt.

- Mottagaren separerar meddelandet och den medföljande signaturen.

- Samma hashfunktion som avsändaren använde används för meddelandet som därmed erhåller ett hashvärde.

- Signaturen, i form av ett krypterat hashvärde, dekrypteras av mottagaren med upphovsmannens öppna krypteringsnyckel och ett okrypterat hashvärde erhålls.

- Mottagaren jämför dessa två hashvärden. Skulle de vara identiska, vet mottagaren att meddelandet inte är förändrat samt att det verkligen härrör från avsändaren. Han kan vara säker på detta eftersom det bara är avsändarens privata nyckel som kan ha krypterat hashvärdet och det endast är ett identiskt meddelande som kan skapa ett identiskt hashvärde.



Figur 4. Verifiering av en digital signatur

2.2 Nyckelhantering och nyckellängder

Två viktiga aspekter för att elektronisk identifiering och digitala signaturer skall fungera är att man kan lagra den privata nyckeln på ett säkert sätt och att man kan komma åt och lita på den öppna nyckeln och dess certifikat som talar om vem innehavaren av den öppna nyckeln är. På så vis kan identiteten säkerställas.

Den digitala signaturens värde beror således till stor del på hur säkert och starkt kryptot är. Kryptots styrka beror i sin tur på den algoritm och de nycklar som används och på nycklarnas längd. Säkerheten i systemet är avhängigt av hanteringen av nycklarna.

Nycklar måste hanteras på ett säkert och effektivt sätt. I hanteringen ingår att tillse att nycklarna skapas på ett säkert sätt, att de fungerar, att de hålls hemliga (privat nyckel) respektive lättillgängliga (öppen nyckel) samt att nycklar som inte längre är giltiga spärras och förstörs.

Stora krav bör ställas på det system som producerar krypteringsnycklarna. Dels skall nycklarna vara unika, dels skall de behandlas på ett sådant sätt att de inte kommer i orätta händer. Privata nycklar lagras säkrast på smarta kort. Med hjälp av det smarta kortets mikroprocessor beräknas krypteringsalgoritmen på kortet. Den privata nyckeln behöver därmed aldrig lämna kortet, vilket annars skulle kunna innebära en risk för att nyckeln röjs.

Öppna nycklar samt spärrlistor (revokeringslistor) bör göras lättåtkomliga för snabb och lätt verifikation av digitala signaturer. Nycklarna förvaras lämpligen i en öppen X.500-katalog och lagras där skyddade som en del av ett certifikat (se nedan om certifikat). Även revokeringslistorna lagras lämpligen i en X.500-katalog.

Krypteringsnyckelns längd (antal bitar) bestämmer hur stark och säker krypteringen blir. Om nyckeln är alltför kort, går det att med matematiska metoder räkna ut den privata nyckelns värde utifrån en given signatur och den öppna nyckeln. Detta brukar kallas att

”knäcka nyckeln”. Den person som kommit över den privata nyckeln kan utfärda förfalskade digitala signaturer, vilket medför att den digitala signaturen i princip blir utan värde.

RSA-algoritmen behöver långa nycklar för att behålla sin säkerhet. RSA-laboratoriet i USA, som utvecklat algoritmen, rekommenderar att nycklarna bör vara 768 bitar långa vid personligt användande, 1024 bitar vid användande för företag samt 2048 bitar vid mycket känsligt användande. De bedömer att en 768-bitars nyckel kommer att vara säker åtminstone till år 2004.

2.3 Certifikat

Certifikatet binder samman en personlig identitet med en öppen nyckel och dess privata motsvarighet. Certifikatet beskriver med andra ord vem som är ägaren till ett visst nyckelpar. Certifikat ges ut av ett certifieringsorgan (Certification Authority, CA). Med tilliten till en CA skapas tillit till de certifikat som ges ut och därmed också till de signaturer som utförs med stöd av dessa certifikat.

Ett certifikat kan bestå av olika datamängder, men ett minimum är att det skall tala om vem som är innehavare av certifikatet, innehavarens öppna nyckel, vem som utgivit certifikatet, samt hur länge det är giltigt. Dessutom bör certifikatet innehålla uppgift om vilken policy för utgivning av certifikat som har följts. Certifikatet är i sin tur signerat med den utgivande CA:ns privata nyckel och kan alltså verifieras med CA:ns öppna nyckel.

Mjuka och hårda certifikat

Man skiljer på mjuka respektive hårda certifikat beroende på den fysiska bäraren av de privata nycklarna. Hårda certifikat är kopplade till att privata nycklar är lagrade på smarta kort. Nycklarna blir därigenom säkert hanterade och certifikatet får ofta ett högre värde.

De mjuka certifikatens privata nycklar är i stället lagrade på en vanlig datafil. Denna fil kan sedan föras på en diskett eller till en hårddisk och skyddas med ett lösenord eller på annat sätt, t.ex. förvaras i låst rum eller kassaskåp. Säkerheten i en sådan hantering är oftast lägre.

2.4 Distinktionen mellan digitala signaturer och kryptering

Digitala signaturer syftar definitionsmässigt till att säkerställa att förändring av ett meddelande inte gjorts samt till att verifiera vem som skapat det. Dock skyddas inte innehållet mot obehörig insyn, vilket kryptering för konfidentialitet gör.

Flera matematiska algoritmer för s.k. öppen nyckel-kryptering t.ex. RSA kan också användas för digitala signaturer (eller tvärtom om man vill se det så). Eftersom det finns olika typer av restriktioner för hantering av krypteringsalgoritmer har dessa restriktioner indirekt också drabbat signaturalgoritmer, t.ex. genom exportkontroll för RSA. Dessa restriktioner appliceras då på algoritmen som krypteringsalgoritm även om det primära (eller enda) intresset hos slutanvändaren är att använda algoritmen som en signaturalgoritm. Dessa omständigheter har fördröjt introduktionen av digitala signaturer i flera länder.

I USA har den federala förvaltningen genom lanseringen av DSA försökt att lösa detta dilemma genom att ta fram en algoritm som enligt uppgift endast kan användas för signering. En del hävdar att DSA med enkla modifieringar kan användas för kryptering. Andra hävdar att så inte är fallet.

Ett problem är emellertid det faktum att algoritmerna normalt ingår i ett sammanhang där en större uppgift än själva den matematiska transformationen skall lösas. Ett genomförande av en digital signatur omfattar typiskt sett en delprocess som innebär att meddelandet förbehandlas dels genom att lägga in redundans och lägga till information om var dokumentet börjar och slutar (s.k. header och trailers) samt anger meddelandets längd, användning av

algoritmer etc. Ofta sker en beräkning av hashvärdet (matematisk bearbetning) av hela meddelandet i en särskild process. Vissa delar av signaturprocessen kan bildas i förväg för vissa algoritmer. En motsvarande delprocess finns vid verifiering av signaturer då olika kontroller skall göras för att fastställa att signaturen är giltig. Dessutom kan den nyckel som skall användas för verifiering behöva kontrolleras. Nyckeln kan hämtas i ett certifikat och kontrollen sker normalt genom att certifikatet (utgivet av en CA) verifieras. (Det är dock inte säkert att certifikatet verifieras, detta beror på implementering och lokal miljö.) Om certifikatet verifieras kan även nyckelns användningsområde kontrolleras, t.ex. att den endast kan användas för verifiering av digital signatur och inte för kryptering.

I princip kan matematiken för digital signatur även användas för krypteringsändamål. Den öppna verifieringsnyckeln för signaturer blir således krypteringsnyckel och den privata signeringsnyckeln kommer att användas för dekryptering. I praktiken kommer det dock att vara svårt för den ovane att genomföra en digital signatur på det viset. Han behöver då särskilja vissa delar av programvaran och kanske modifiera dessa delar vilket dessutom måste göras ömsesidigt av sändare och mottagare. Det blir än svårare om vissa delar ligger inlagda i aktiva kort för att skydda genomförandet från obehörig påverkan. I dag ligger huvudsakligen signeringsalgoritmen i kortet medan beräkning av hashvärdet och annan förbehandling ligger utanför i PC-programvaran, vilket förenklar hanteringen.

Även om det alltså finns tekniska möjligheter att begränsa användningsområdena till signering så kan troligen inte begränsningarna göras hundraprocentigt säkra. För att ytterligare säkerställa att signaturnycklar inte används för konfidentialitetskryptering kan de tekniska begränsningarna kompletteras med regler för användningen. Ett lands policy kan uttryckligen förbjuda användning av signaturnycklar för konfidentialitet. Krav kan ställas på att användare, när de kvitterar ut certifikat och erhåller nyckelpar, skall skriva under på att de inte använder en nyckel på icke avsett vis. CA kan vidare åläggas att tillhandahålla separata certifikat och nyckelpar för de olika användningsområdena.

Exportkontrollen i flera länder tar stor hänsyn till paketeringen när licensfrågor avgörs. Teknik för integritetsskydd och signering, som inte utan svårighet kan ändras till krypteringsändamål, behandlas därför på ett enklare sätt än ren krypteringsutrustning.

Tillvägagångssätt för att hindra att nycklar för digitala signaturer används för kryptering beskrivs närmare i *bilaga 1*.

3 Utrustning

Digitala signaturer skapas genom ett antal processer. Dessa kan baseras på enbart programvara eller programvara i kombination med maskinvara, normalt chip i s.k. aktiva kort (smart card, smarta kort) eller kortläsare till aktiva kort. Övrig maskinvara lämnas i detta sammanhang utanför beskrivningen. Som underlag för beskrivningen av processer och komponenter används här den schematiska bilden från Allterminalprojektet (Projekt Allterminalen). Bilden används för att visa skillnaden mellan mjuka och hårda nyckelbärare och för att visa hur digitala signaturer förhåller sig till de två övriga säkerhetsfunktionerna, stark identifiering/autenticitet och kryptering/konfidentialitet. De tre grundläggande säkerhetsfunktionerna utnyttjar samma tekniska lösningar och man kan därför inte bortse från samverkan och beroende dem emellan.

3.1 Beskrivning av användningskedjan

3.1.1 Projekt Allterminalen – gränssnitt

I Projekt Allterminalen bedömdes att nyckeladministrationen måste bygga på användningen av aktiva kort. Det grundläggande kravet var att delar av processen måste kunna ersättas utan att hela kedjan påverkades.

3.1.2 Elektroniska ID-kort, Strategisk samverkan och SEIS

I det bankgemensamma projektet Strategisk samverkan ställdes krav på just samverkan så att olika aktiva kort, utgivna av skilda organisationer, skall kunna fungera i samma miljö. Detta krav var utgångspunkten för SEIS (Föreningen Säkrad Elektronisk Informationshantering i Samhället) arbete med att dokumentera tekniska och administrativa krav på ett generellt elektroniskt ID-kort.

3.1.3 Processer och komponenter

Utgångspunkten är att algoritmer är öppna medan krypteringsnycklar (i detta fall signeringsnycklar) måste hållas hemliga och väl skyddade. Signeringsprocessen sker i datormiljö.

Den datormiljö som finns tillgänglig är PC (workstation) med möjlighet att ansluta aktiva kort till denna. Teoretiskt sett kan fristående ”säkerhetsdosor” eller ”tokens” användas med längre nyckellängder, men eftersom nyckeln (sifferraden) skall matas in manuellt blir det praktiskt omöjligt att använda dessa.

Beräkning av hashvärdet sker i en särskild process eller som en del av en automatiserad signeringsprocess. Bankföreningen har publicerat en beskrivning av hur en självständig beräkningsprocess enligt standarden MD5 på ett enhetligt sätt skall genomföras i såväl PC- som stordatormiljö. I beskrivningen ingår regler och val av olika standarder.

I TCP/IP världen används ofta standarden S/MIME. Här skapas såväl hashvärdet som signeringen i en och samma process.

Standarden SSL gör det möjligt att i anslutningen (handskakningen mellan datorer) tala om vilka algoritmer som används, nyckellängder m.m. vilket medger samverkan mellan olika lösningar.

På motsvarande sätt används särskilda fält i ett meddelande enligt standarden för EDIFACT för att tala om vilken säkerhetsfunktion som utnyttjas och vilka algoritmer och nycklar som använts för att säkra det aktuella meddelandet.

Alla dessa lösningar bygger på att algoritmer och nycklar – eller resultat från sådana beräkningar – finns tillgängliga när användaren avser att kommunicera med omgivningen. I detta sammanhang spelar det ingen roll om all information finns i PC:n eller om en viss del av processen flyttats till ett till arbetsplatsen anslutet aktivt kort.

När en digital signatur produceras skapas samtidigt ett elektroniskt eller digitalt dokument. Det är viktigt att understryka detta eftersom en digital signatur inte kan uppträda i annan form. Signaturen är en del av dokumentets helhet. Därigenom blir det möjligt att använda flera tekniska lösningar. Även om det finns några huvudalternativ i dag för signering respektive beräkning av hashvärdet, så måste system byggas så att vi med hjälp av informationen i ”handskakningen” kan välja samma lösning som avsändaren valt att använda. Av detta skäl innehåller program som används för dessa ändamål ett bibliotek med uppsättningar av flera standarder för respektive funktion (signering, hashberäkning och kryptering).

3.2 Funktioner från användarens perspektiv

Syftet med en digital signatur är att användaren skall kunna ta ansvar för sin signering av ett digitalt dokument. Utöver de tekniska krav som redovisats ovan måste han förstå när och var signeringssituationen uppstår. Denna funktion benämns i detta sammanhang ”upplysningsfunktionen”. För att tillgodose detta krav skall användaren kunna ”se” de data som skall ingå i den beräkning av hashvärdet som föregår signeringen. Denna hashrutin kopplas normalt till en lösenordshantering, dvs. användaren måste ange PIN-koden till sitt aktiva kort eller ett lösenord för att komma åt signeringsnyckeln om den ligger på hårddisk eller diskett. På så sätt uppnås dels upplysningsfunktionen, dels skyddet mot att signeringsnyckeln används utan användarens uttryckliga önskan.

En viktig och ofta förbisedd funktion är att användaren skall kunna kontrollera sin egen signatur. I t.ex. Netscapes browsers

(4.X-versionen och senare versioner av webb-läsare) kan man numera använda standardrutiner för att kontrollera innehavaren av en digital signatur och vem som är utfärdare av certifikatet.

3.3 Programvara och maskinvara

3.3.1 Nyckeladministration i maskinvara

I detta fall låter man användaren själv skapa sina nyckelpar med hjälp av en befintlig programvara i dennes PC. Efter framställningen skyddas den privata delen med hjälp av traditionell kryptering eller genom att fördela datamängden så att informationen om den inte utan svårigheter skall kunna göras synlig. Genom att använda ett lösenord eller en användarfras återskapas nyckeln för sitt ändamål.

Den öppna delen av nyckelparet skickas till en CA för certifiering. Certifikatet lagras i användarens PC.

Utöver kravet på nycklar av god teknisk kvalitet gäller att dessa (dvs. den öppna delen av nyckelparet) skall kunna garanteras av en trovärdig CA. Nycklar som skapas i en programvara är utanför CA:s kontroll. Värdet av ett certifikat baserat på nycklar i en programvara blir därefter. Det finns inte heller något skydd för ren kopiering av det medium som används (hårddisk eller diskett).

3.3.2 Nyckeladministration med aktiva kort

Chipet i ett aktivt kort kan beskrivas som en liten dator. I dessa fall används chip av en typ som medger dels att lagrade nycklar kan skyddas mot exponering, dels att signeringsprocessen kan ske i en skyddad rutin. Tekniken för att skapa digitala signaturer i ett chip är den i dag bäst kända tekniken. Utöver den tekniska kvaliteten på skyddet tillkommer de sociala aspekterna. Förpackningen, dvs. att montera chipet på ett ID-kort av traditionellt slag, innebär att innehavaren har en större möjlighet att ta ansvar för den fysiska hanteringen av sin ”digitala identitet”.

Då en CA i detta fall har möjlighet att ta ansvar för hela processen fram till utfärdandet av ID-kortet, skapas förutsättningar för en certifiering med mycket hög trovärdighet. Det är denna situation som ligger till grund för SEIS Policy (S7)[4] för utfärdande av kombinerade elektroniska ID-kort enligt SIS-standard.

Kravet på att krypteringsnycklar skall förvaras och användas i en av utfärdaren kontrollerad miljö, ställdes redan för flera år sedan av bankerna och Posten. I regelverket för Swedifact Finans framgår att om en skriftlig s.k. utanordning skall få göras på elektronisk väg skall den signeras med hjälp av en namnsatt token (säkerhetsdosan) eller aktivt kort. Den utarbetade modellen beskriver samtidigt hur en datafil övergår till vad som definitionsmässigt är ett elektroniskt (eller digitalt) dokument.

Med hänsyn tagen till Bankföreningens publicering av hur MD5 kan implementeras samt SEIS Policy för elektroniska ID-kort, får modellen följande utseende.

3.3.3 Aktiva kort och kortläsare

Kort

Det finns fyra grundläggande krav på de smarta kort som skall användas. De skall ha en beräkningskapacitet som är tillräcklig för att göra en krypteringsberäkning på kortet. De skall ha tillräckligt med minneskapacitet för att lagra nödvändig information. De skall vara standardiserade till innehåll och format samt kunna lagra informationen på kortet på ett säkert sätt.

I dag finns kort som uppfyller alla dessa krav och utvecklingen av mer kraftfulla chip för smarta kort fortsätter. I dag kommersiellt tillgängliga kort kan göra en RSA-kryptering eller en DES-kryptering, men inte båda samtidigt. Standarder finns för såväl innehåll, format och utseende.

[4] Policyn finns tillgänglig på http://www.seis.se/arkiv.html

Vad gäller standard för innehållet i ett certifikat så är x.509-standarden helt dominerade. Kortens fysiska format är fastslagna i ISO 7816 med understandarder.

Det fysiska utseendet, chipets placering, kommunikationen, den elektriska spänningen samt ett antal kommandon är i dag väl definierade. Utvecklingen går nu mot standarder för operativsystem för att möjliggöra flera samtidiga funktioner (multifunction cards). Detta skapar ökad flexibilitet samtidigt som säkerhetskraven blir ännu högre. Ökad prestanda gör att det nu finns tillgång till chip som klarar nycklar om 1024 bitar med fullt acceptabla svarstider. Utvecklingen på chipsidan svarar därför väl mot de tekniska krav på nyckellängder m.m. som ovan redovisats.

I dag skapas nyckelparen utanför de aktiva korten i en särskild process. Detta sker innan kortet kopplas till sin blivande användare.

För närvarande används PIN-kod för att skydda kortet, eller den digitala identiteten, från missbruk. Om koden exponeras kan den missbrukas. Till skillnad från andra system krävs dock att missbrukaren, utöver koden, måste ha fysisk tillgång till kortet. Koden används endast för att starta den förbestämda processen i kortet. Koden har ingenting med framställningen av den digitala signaturen att göra. PIN-koden kommer förhoppningsvis att kunna ersättas med biometriska rutiner (se nedan).

Det går också att använda s.k. virtuella kort eller vanliga disketter för att få en säker identifiering och digitala signaturer. Då läggs motsvarande information som lagras på det smarta kortet antingen i en krypterad fil i datorn eller på en diskett. Det ger inte samma höga säkerhet för den lagrade informationen som man får med ett smart kort som ju dessutom fungerar som ett visuellt ID-kort. Det smarta kortet bär man ju med sig och det kan låsas vid missbruk. Å andra sidan behövs inte kortläsare, rutiner för kortframställning, distribution m.m. och följaktligen blir en sådan lösning billigare.

Läsare

Det finns för närvarande tre olika typer av läsare. Sådana läsare som är fristående från datorn med eller utan nummertangenter (pin pad), PCMCIA-läsare som sätts in i t.ex. den bärbara datorn eller inbyggda läsare, antingen i tangentbordet eller i datorn.

Kortläsare med separat tangentbord finns.

Standarder för läsare håller på att etableras vilket bl.a. gör att man lätt kan byta läsare utan att behöva omprogrammera systemen. Hittills har varje läsare krävt sin egen drivrutin men utvecklingen går mot mer standardiserade lösningar, vilket kommer att underlätta också för applikationsleverantörerna.

Priset på kortläsare har hittills effektivt stoppat utvecklingen av massmarknadstjänster. Kortspecifika läsare skapar små serier och höga priser. Företag som tidigare producerat säkerhetsdosor (tokens) till massmarknaden har nu emellertid börjat leverera billiga kortläsare.

Säkerheter i produktionskedjan

En beskrivning av de olika leden inom produktionskedjan och de problem som kan uppstå finns redovisade i*bilaga 2.*

3.4 Förväntad teknisk utveckling

3.4.1 Standarder

Fortsättningen på standardiseringsarbetet avseende ISO 7816 innebär att fler kommandon kan användas och fler tjänster ges en generell utformning. Standarder för operativsystem och användning av Java[5] kommer att snabbt förbättra flexibiliteten och därmed produktutvecklingen.

[5] Java: ett programmeringsspråk som är speciellt utvecklat för Internetmiljön.

Den stora uppslutningen kring PKI (Public Key Infrastructure, öppen-nyckel-infrastruktur), inte minst på grund av Internet och det genomslag som SSL och S/MIME fått, påskyndar det praktiska arbetet i PKIX. Arbetssättet gör att resultatet ger stort genomslag och acceptans.

Microsoft, Netscape m.fl. har enats om ett gränssnitt för att anropa kortläsare för aktiva kort. Standarden skall fastställas under första kvartalet 1998. Detta kommer att påverka PC-tillverkarna som nu kan bygga in läsaren i maskinen. Detta gränssnitt påverkar även de programvaruföretag som bygger säkerhetsfunktioner. De slipper i fortsättningen ta hänsyn till respektive leverantörs drivrutiner.

3.4.2 Chip som teknisk plattform

Även om chiptekniken är den bästa formen för nyckeladministration är det troligt att den, precis som PC:n kommer att utsättas för kraftiga förändringar. Eftersom tekniken skall skydda datamängder av stort värde kan tekniken komma att utsättas för hårda angrepp. Under senare tid har flera fall av angrepp visat sig medföra stora risker och detta har lett till att övriga aktörer har förbättrat kvaliteten på nästa generation. Som teknisk plattform har chiptekniken sin givna plats då den utöver rent tekniska kvaliteter även passar in bland dagens socialt accepterade ID-kort.

3.4.3 Biometriska lösningar

Att använda en PIN-kod som lås och skydd mot missbruk av ett elektroniskt ID-kort, anses som den svagaste länken i säkerhetskedjan. Om kortinnehavaren skriver sin PIN-kod på kortet och underlåter att hålla kortet under uppsikt, hjälper det föga hur sofistikerade algoritmer och långa krypteringsnycklar som används. Eftersom antalet koder ökar måste alternativ utvecklas.

Bevisvärdet för en signatur som skapas i ett aktivt kort skulle bli ännu högre om processen förutsatte att t.ex. kortinnehavarens

fingeravtryck kontrollerades inne i kortet. Bland de olika biometriska lösningarna anses just fingeravtrycket vara det mest framgångsrika. Flera omständigheter tyder på att praktiska lösningar, där fingeravtryck kan användas direkt på det aktiva kortet, finns att tillgå inom några år.

Eventuellt kan biometriska lösningar också användas för helt nya säkerhetsstrukturer.

4 Certifieringsorgan, CA

Nedan följer en beskrivning av CA-verksamheten efter den modell som har utarbetats inom TeleTrusT Sverige[6]. Beskrivningen är endast avsedd att exemplifiera hur en CA-policy kan se ut. Den här beskrivna CA-policyn bygger på användning av aktiva kort. Det finns emellertid också CA-policies som använder nyckeladministration i maskinvaran. Exempel på detta är VeriSign.

4.1 Uppgifter för en CA

Vilka uppgifter måste med nödvändighet läggas på en CA och vilka tillkommande uppgifter kan en CA få i en elektronisk kommunikationsmiljö?

En CA ger ut elektroniska certifikat, dvs. signerad information om en identitet, en roll eller något annat förhållande. En CA har också ansvar för certifikatens status under deras giltighetstid. Detta innebär bl.a. publicering av spärrinformation för certifikat som dragits in. En CA är således garant för den policy under vilken certifikaten ges ut och ansvarar som operatör för den kontinuerliga driften av de system som krävs för den dagliga användningen. Detta betyder att användarna skall kunna verifiera identiteter, signaturer och hämta krypteringsnycklar när helst detta behov finns.

En CA kan vara intern för ett företag eller en organisation eller erbjuda sina tjänster allmänt tillgängligt. Nedanstående gäller enbart de allmänt tillgängliga tjänsterna.

[6] Föreningen TeleTrusT Sverige verkar för främjande av användning av digitala signaturer i en rad olika tillämpningar. Jfr http://www.teletrust.se

En allmänt tillgänglig CA har ansvar för att publicera en policy som beskriver under vilket regelverk certifikaten ges ut, göra certifikaten allmänt tillgängliga i en katalog, tillhandahålla uppgifter om certifikatens status, dvs. uppgift om eventuell spärr samt dokumentera miljö, rutiner och tekniska system så att dessa kan verifieras mot den utgivna policyn.

En organisation som ikläder sig en allmänt tillgänglig CA-roll uppträder med ambitionen att vara en betrodd tredje part (TTP, Trusted Third Party). Utöver CA-rollen kan en sådan organisation erbjuda andra relaterade tjänster som organisationen inte behöver erbjuda men kan åta sig. Exempel på detta är tidsstämpling (en elektronisk variant av ”poststämpelns datum”), mottagningsbevis (tidsstämpla och signera dokument som levereras till t.ex. en myndighet och sedan returnera en kopia av det signerade dokumentet till avsändaren) och arkivtjänster.

I ISO 9594-8 (the directory – Authentication Framework) definieras en CA på följande sätt.

An authority trusted by one or more users to create and assign certificates. Optionally the Certification authority may create the users' keys.

För att en CA skall bli accepterad måste den följa en känd och accepterad policy för *hur* bl.a. certifikat skall skapas, både ur tekniskt och administrativt perspektiv.

En CA-funktion innefattar en roll och ett ansvarstagande. I SEIS policy S08[7] uttrycks det emellertid enligt följande.

Detta dokument beskriver de krav som måste uppfyllas och de regler som måste efterlevas av varje organisation (kortutfärdare) som önskar ge ut personliga, fotoförsedda elektroniska identitetskort för publik användning, producerade genom centraliserad personalisering. Organisation som utfärdar kort enligt denna policy är också CA för utfärdade certifikat.

[7] SEIS policy S8 finns tillgänglig på http://www.seis.se/arkiv.html

För att ytterligare förtydliga ansvaret för en CA kan följande passus från SEIS 08 användas om man för allmängiltighetens skull tänker sig att det gäller även enklare lagring av certifikat och kort.

En utfärdare av kort har alltid hela ansvaret för all administration och fysisk hantering i samband med kortens utfärdande, oavsett om vissa uppgifter utförs av annan organisation. Kortutfärdaren uppträder som beställare gentemot en underleverantör och köper t.ex. kortämnen, chipmontering, personalisering eller andra tjänster från denne. Det åligger utfärdaren att kontrollera att varje underleverantör uppfyller policyn i de delar som berör denne.

Utfärdare ansvarar för att en obruten säkerhetskedja skapas mellan beställare, utfärdare och tillverkare. Rutinerna måste ge spårbarhet så att vid behov kontroll kan ske om oriktig utfärdandehantering eller missbruk förekommit eller inte.

Utfärdaren påtar sig gentemot andra organisationer som använder korten i sina tjänster, att garantera att kortens uppgifter är korrekta vid utfärdandet. Detta gäller både den visuellt läsbara informationen och det maskinläsbara chipet.

Detta visar att man för att kunna åstadkomma en fungerande infrastruktur använder sig av en CA-funktion endast som en liten del i den totala processen. En vanlig, om än inte nödvändig, modell är att en CA på uppdrag av en utfärdare tar ansvar för samtliga moment utom det slutgiltiga utlämnandet till användaren.

För att kunna ha en infrastruktur för användning av digitala signaturer måste ett antal delfunktioner finnas. Om vi antar att infrastrukturen inkluderar elektroniska ID-kort så finns följande funktioner som alla måste inkluderas i den policy som styr verksamheten. Funktionerna definieras i policyn.

Korttillverkning: Konstruktör av operativsystem, chiptillverkare, modultillverkare, korttryckning och inbäddning.

Kortutfärdare: Beställningar av kort, kontroll av ID-uppgifter, auktorisation av roll (t.ex. behörighet), utlämnande av kort, spärrning/återtagning av kort.

Nyckelgenererare: Applikationsinitiera kortet, skapa nycklar, skapa nyckel-PIN-kod.

CA: Certifikatbindning, certifikatdistribution, spärrlistehantering.

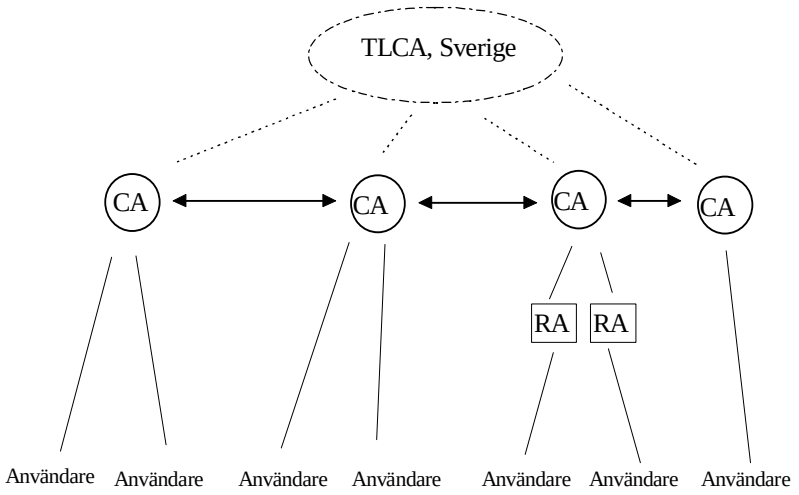
Grafisk personaliserare: Kontrollera ID-uppgifter, påföra grafiska ID-uppgifter.

Kortinnehavare: Förvara kort och PIN-kod, anmäla förlorat kort, återlämna ogiltigt kort.

Elektrisk personaliserare: Påföra certifikat, påföra annan applikationsinformation.

Applikationsleverantör: Skapa tillförlitliga applikationer som använder infrastrukturen.

4.1.1 Funktioner



Samspelet mellan olika CA kan skötas med korscertifiering eller med hjälp av en toppnod, Top Level CA (TLCA). Båda varianterna fungerar lika bra när antalet CA är begränsat, men en TLCA underlättar hanteringen när antalet CA är mycket stort.

Top Level CA, TLCA

En TLCA utgör den gemensamma roten för hierarkin i landet. Via TLCA kan alla användare i hierarkin kommunicera med varandra. TLCA har följande huvudsakliga uppgifter, nämligen att

- definiera övergripande policies för hierarkin,
- kontrollera att identiteter för CA är unika,
- certifiera underliggande CA, distribuera dessa certifikat,
- revokera (återkalla) de CA-certifikat den gett ut, distribuera revokeringsinformation,
- distribuera sin öppna nyckel till den som i underliggande nivå behöver denna i samband med kontroll, samt
- kontrollera att de CA den certifierat följer given policy samt agera mot dessa om så inte är fallet.

CA

CA certifierar användare i sin domän. Detta görs i enlighet med den policy som är definierad. Uppgifter för CA är att

- korscertifiera andra CA,
- certifiera användare i enlighet med given policy och distribuera certifikat,
- revokera (återkalla) de certifikat den gett ut och distribuera revokeringsinformation,

– distribuera sin öppna nyckel till den som i underliggande användarledet behöver denna i samband med kontroll, samt

– kontrollera att de certifierade följer given policy samt att agera mot dessa om så inte är fallet.

4.1.2 Hot

CA:s grundläggande uppgift är att garantera säkerheten i systemet.

Hot mot säkerheten när digitala signaturer används uppkommer om en signatur kan skapas av obehörig på ett sådant sätt att den verifieras och godtas som giltig, om data kan dekrypteras av obehörig och om en digital signatur därmed kan förnekas på trovärdigt sätt. Dessa hot kan bli en realitet om de administrativa rutinerna är bristfälliga eller om de program och den utrustning som hanterar kort och certifikat (inklusive utrustning för CA-funktion) är skadade eller felkonstruerade. Dessutom kan de kort som används vara av dålig kvalitet.

Följande punkter beskriver mer detaljerat ett antal exempel.

En annan person än kortägaren använder kortet: Om detta är möjligt kan signaturer skapas och data dekrypteras av obehörig.

Fel data signeras omedvetet, eller signaturen skapas på felaktigt sätt: Med detta menas att information som användaren inte hade för avsikt att signera signeras, eller att signaturen skapas med annan persons privata nyckel.

Fel öppen nyckel används omedvetet: Om detta sker kan ogiltiga signaturer komma att godtas som giltiga eller tvärtom. Dessutom finns en risk att krypterade data kan dekrypteras av obehörig.

Privat nyckel används av obehörig: Signaturer kan förfalskas och data dekrypteras av obehörig.

Ogiltig öppen eller privat nyckel eller återkallat certifikat används: Med ogiltig menas här att nyckeln blivit ogiltig genom att certifikatet blivit återkallat.

Falska, användbara kort i omlopp: Det strukturella innehållet i kortet är i allmänhet känt och kan skapas av vem som helst, säkerheten ligger i det signerade certifikatet. Med användbara menas här

att de applikationer som hanterar kort och certifikat godkänner det som giltigt.

Falska, användbara certifikat i omlopp: Certifikatinnehållet är allmänt känt och kan skapas av vem som helst; säkerheten ligger i CA:s signatur. Med användbara menas här att de applikationer som hanterar certifikat godkänner det som giltigt.

Certifiering sker på felaktiga grunder: Med detta menas att en certifikatbindning sker för en identitet och nyckel som inte skall certifieras i CA:s namn. Detta kan innebära att en signatur som godtas som giltig inte är skapad på ett tillräckligt säkert sätt.

Möjlighet till förnekande av digital signatur: En korrekt utförd digital signatur skall inte kunna förnekas. För att systemet över huvud taget skall fungera krävs regler som behandlar giltighet av digital signatur utan att detta är föremål för särskilt avtal mellan parterna. Ett exempel på problem beskrivs i följande scenario: En användare signerar digitalt ett dokument vilket han vid en senare tidpunkt ångrar. För att ge tyngd åt sitt förnekande kan han exempelvis "tappa" sitt smarta kort tillsammans med PIN-koden. Det torde ofta inte gå att skilja detta fall från det, då en användare som verkligen tappat sitt kort och PIN-kod inte anmäler detta innan missbruket äger rum. Båda har dock brutit mot regeln att kort och kod inte får förvaras tillsammans (förutsatt att en sådan regel upprättats).

Tillgänglighetsbrister: Dålig tillgänglighet av revokeringsinformation kan vara ett hot. Med korrekt certifikathanterande applikationer som beaktar revokering utan tidsutdräkt kan riskerna minimeras.

I övrigt är dålig tillgänglighet inget direkt säkerhetshot, men kan indirekt vara det. Om en användare exempelvis inte kan använda sitt kort på grund av att det är trasigt, kanske han väljer att skicka data utan att signera det. På samma sätt kan han välja att skicka data okrypterat om mottagarens certifikat inte finns tillgängligt.

4.1.3 Krav på hanteringen – huvudmomenten

Det följande beskriver de moment som en utfärdare/CA måste kunna beskriva beträffande sin hantering, för att det skall vara möjligt att lita på funktionen.

Identifiering av användare: För aktiva kort som skall användas för identifiering är det av största vikt att användaren är identifierad innan sådana kort ges ut och certifiering sker. Det vill säga att de personuppgifter som läggs i certifikatet är korrekta och att personen verkligen är den han utger sig för att vara. Hela konceptet med certifikat och öppen-nyckel-teknik står och faller med en säker identifiering. En sådan funktion är också en förutsättning för att CA skall kunna lita på certifikat utställda av andra CA.

Beställning av certifiering: Med beställning menas de användaruppgifter som måste vara kända för att certifiering och kortutgivning skall kunna ske. Dessa uppgifter kan nå CA-funktionerna på en rad olika sätt, t.ex. via en till CA-utrustningen ansluten terminal eller i form av en datafil.

Certifiering, personalisering och revokering: När förutsättningarna för certifiering är uppfyllda kan certifiering och personalisering genomföras. Då denna fas är mycket kritisk finns en rad tekniska och administrativa krav som måste vara uppfyllda. Förenklat består denna fas av att nycklar skapas, certifikat sammanställs och signeras samt att kortet personaliseras. Krav ställs bl.a. på att korrekta data skapas samt på fysisk och logisk säkerhet liksom krav på återkallelse (revokering) av certifikat, samt på distribution av certifikat och revokeringsinformation.

Användaridentiteter: Identifieringsfunktionen skall unikt identifiera en användare. Vissa krav kan ställas på hur denna skall vara sammansatt. Dessutom är det viktigt att varje utgivet certifikat innehåller en unik identitet.

Revokeringsinformation: Revokeringsinformation kan antingen bestå av revokeringslistor eller revokeringscertifikat. En revokeringslista sammanställs med en viss periodicitet av CA och innehåller referenser till samtliga av CA revokerade certifikat. Ett revokeringscertifikat är ett ”vanligt” användarcertifikat som kan användas som vanligt för att verifiera signaturer. Skillnaden består i

att det i revokeringscertifikatet finns uppgifter om att certifikatet är revokerat, när det revokerades samt ibland även orsak till att det revokerades.

För att kunna skapa revokeringsinformation kan CA vara beroende av tillgång till tidigare utgivet certifikat. Om CA skall kunna revokera certifikat oberoende av förbindelse med extern katalog, måste kopior av samtliga utgivna certifikat finnas hos CA:n.

Skydd av användares privata nyckel: Den privata nyckeln skall kunna användas endast av sin ägare. Aktiva kort rekommenderas för lagring och användning av privata nycklar. I vissa fall kan det av prestandaskäl vara nödvändigt att lagra och använda en privat nyckel utanför ett aktivt kort (t.ex. om en maskin skall autenticiera sig mot många användare inom en kort tidsrymd).

Aktiva kort: Då det aktiva kortet innehåller information av mycket känslig natur är det viktigt att det fungerar på korrekt sätt. Kontroll av chiptillverkare och konstruktörer av operativsystem är några sätt att förvissa sig om detta. En lista av "godkända" kort kan upprättas.

Logg och arkivering: Säkerheten i CA-utrustningen kan höjas genom att logg och arkiv förs över relevanta händelser. Dessutom kan uppgifterna användas för att kunna urskilja eventuella personer som missbrukat sitt ansvar.

Bootstrap/uppstart: Uppstarten av en ny CA-utrustning är en speciell händelse. Vid uppstart skall bl.a. systemet konfigureras och initiala behörigheter sättas. Eventuellt skall även CA:s privata nyckel genereras och sättas i drift samt CA och säkerhetsansvarig certifieras.

Samverkan mellan CA: Beskrivning av hur och om certifiering av annan CA kan göras.

Kopior av privata nycklar: I de fall en öppen nyckel använts för att kryptera data, blir dekryptering omöjlig om motsvarande privata nyckel försvunnit eller på annat sätt blivit obrukbar. Därför finns ibland önskemål om att spara en kopia av den privata nyckeln. Att spara en kopia innebär naturligtvis en säkerhetsrisk.

Fysiskt skydd: CA-utrustningen kan behöva ett fysiskt skydd för att tillgodose de säkerhetskrav som ställs. Ett fysiskt skydd består

exempelvis av ett låst rum eller säkerhetsskåp med begränsat tillträde.

Logiskt skydd: Ett logiskt skydd finns som en funktion i mjukvaran och består av behörighetskontrollsystem (BKS) och identifiering av användare. Till BKS hör en databas i vilken de olika behörigheterna för användare beskrivs samt funktioner för administration (management) av denna databas.

Implementeringsutrustning: Med implementering menas den hård- och mjukvara som tillsammans utgör CA-funktionen. Utöver de krav som finns i en policy kan krav på användarvänlighet, flexibilitet, val av komponenter och enkelhet att underhålla finnas. Dessa krav ställs ofta av den organisation som har för avsikt att driva en CA gentemot en leverantör, men kan även vara krav från säkerhetsansvarig en nivå upp i systemet.

Certifikatdistribution: Alla användare i ett öppen-nyckel-system måste ha tillgång till certifikat för dem de önskar kommunicera med. På vilket sätt är distributionen ordnad?

Distribution av revokeringsinformation: Distribution av revokeringsinformation är en viktig uppgift för CA. Olika krav på säkerhet ställer olika krav på hur och när revokeringsinformationen skall distribueras. Om man exempelvis skall göra en transaktion på miljontals kronor, är det viktigt att färsk information om vilka certifikat som revokerats finns tillgänglig. Gäller det mindre känsliga dokument kan det räcka med äldre revokeringsinformation som lagrats i det egna systemet.

Distribution av kort och koder: Då en användare blivit certifierad och ett nytt aktivt kort skapats skall det nya kortet förmedlas till den nye användaren. Dessutom skall användaren få kännedom om sin personliga kod.

Användarinstruktioner: Klara instruktioner om när och hur kortets olika funktioner skall användas behövs för att stötta användaren. Även regler för hantering och förvaring av PIN-kod och av kort är nödvändiga.

Riktlinjer för applikationer: Applikationer som hanterar kort och certifikat bör göra detta på ett riktigt sätt. Speciellt viktigt är det att kontrollera revokeringsinformation samt att implemente-

ringen görs på ett sådant sätt att påverkan från andra program och applikationer minimeras.

Administration av PIN-koder: Aktiva kort som hanterar PIN-koder brukar tillåta ett maximalt antal felaktiga försök. Om fler försök görs blockeras kortet. På många kort finns funktioner för att återställa blockerat kort.

Administration av certifikat: Viss uppdatering av information i certifikat kan i vissa fall behövas. Exempel på detta är förlängning av giltighetstid och ändring av användaruppgifter. I och med att ett certifikat uppdateras skall det gamla revokeras.

Begäran om revokering av certifikat: Att revokera ett certifikat innebär att det återkallas och att informationen följaktligen inte längre får åberopas. Anledningen till att ett certifikat skall revokeras kan bl.a. vara att kortet försvunnit, att nyckeln röjts eller att användaren misskött sig på något sätt. En risk med revokeringar är att en obehörig person begär certifikatet revokerat för att på detta sätt vinna egen fördel. Därför bör begäran om revokering föregås av identifiering. Revokering kan begäras av användaren själv, den säkerhetsansvarige som tidigare hanterat en beställning av certifikat för användaren eller av säkerhetsansvarig en nivå upp i systemet.

Avslutade kort: Indragna eller avslutade kort kan behöva återlämnas eller makuleras. I samband med detta är det även nödvändigt att revokera användarens certifikat.

Röjd, förstörd eller planerat byte av CA-nyckel: Byte av CA-nyckelpar skall i möjligaste mån undvikas eftersom detta innebär en komplicerad process. Alla användarcertifikat skall revokeras och återskapas, kort måste uppdateras m.m. Beredskap för detta bör finnas. Nyckeln kan t.ex. röjas, bli obrukbar eller behöva bytas för att uppfylla ny policy. Rutiner för hur detta skall gå till måste utarbetas.

4.2 Organisations- och säkerhetsfrågor

4.2.1 Krav som måste ställas på CA:s interna organisation och uppbyggnad

Organisationen och säkerheten för en CA är beroende av vilken eller vilka policy/policies (riktlinjer) den stöder. Det viktiga är dock att dessa regler är väl dokumenterade och verifierbara. Följande måste vara dokumenterat och implementerat i detalj.

- Krav på drift och driftmiljö.
- Klara rutinbeskrivningar måste finnas och tillämpas.
- Klara regler för vilket ansvar var och en i organisationen har och på vilket sätt delegering sker.
- För varje befattning måste en klar befattningsbeskrivning finas.
- Dokumentationen måste vara skriven så att revision av organisation och rutiner, för att kontrollera att organisationen följer sin policy, kan genomföras.

Den organisation som önskar verka som CA måste vara ekonomiskt sund och bedömas ha långsiktig varaktighet. Långsiktighet är viktigt eftersom certifikat skall kunna verifieras i flera år efter det att giltighetstiden för certifikatet gått ut.

4.3 Möjliga strukturer

4.3.1 Sverige och internationellt

Det är möjligt att använda såväl en hierarki av CA som korsvis certifiering vid uppbyggnaden av en CA-struktur. Internationellt torde det vara mycket omständligt att skapa ett hierarkiskt system.

Kulturella skillnader kommer också att påverka lösningarna. Den globala strukturen kommer därför troligtvis att utvecklas genom samarbetsavtal och korsvis certifiering. Man kan t.ex. tänka sig lösningar för vissa marknadssegment. Ett exempel på ett sådant är den samverkan som i dag utvecklas mellan olika nationella post-bolag och postverk.

5 Svagheter i systemet

I avsnittet 4.1.2 redogjordes för de olika hot som finns mot säkerheten i ett system för digitala signaturer. Här avses att åskådliggöra vissa av dessa säkerhetsrisker.

5.1 Kryptologiska metoder och kryptologiska attacker

En del matematiska metoder som används till digitala signaturer har funnits i två decennier, andra enbart under några år. Centralt för digitala signaturer är asymmetrisk kryptering.

Att knäcka den matematiska metod som utgör kärnan i den digitala signaturen är möjligt, men oftast mycket resurskrävande. Intrång i datasystem med hjälp av knäckt kryptering är ytterst ovanligt. Matematiker och kryptologer utvecklar konstant nya typer av kryptologiska attacker för att testa kryptosystemen.

Det är rimligt att anta att det alltid kommer att finnas asymmetriska krypteringsmetoder som bedöms ha tillfredställande säkerhet, dvs. som rent praktiskt kommer att kräva så stora resurser att knäcka att kostnaderna överstiger vinsterna med att angripa systemet. Det är dock viktigt att bygga systemen så att kryptosystemen enkelt kan bytas ut vid behov. Om inte, finns risk för en ny ”millenie-problematik” när en viss använd kryptoteknik har åldrats.

Om det skulle visa sig att alla praktiskt tillämpliga asymmetriska kryptosystem har omfattande brister så kan detta komma att kräva ett ingripande från statligt håll. Detta är i så fall inte ett isolerat problem för Sverige, utan för hela den IT-beroende västvärlden.

5.2 Utfärdande av certifikat och CA-systemet

Vid användning av en CA som intygar äktheten hos ett certifikat introduceras såväl organisatoriska som tekniska svagheter och hot. De mjukare hoten i form av insiderhot, slarviga CA, dålig identifikation av personer vid utlämnande av smarta kort, osv. skall inte underskattas.

Tekniskt sett finns risk för att en angripare förvärvar möjligheten att utfärda falska certifikat i CA:ns namn. Detta kan genomföras på flera sätt. Ett sätt är att genomföra en kryptologisk attack mot en CA, och därigenom lyckas gissa den hemliga nyckel som en CA använder för att signera certifikaten med. Detta hot kan inte ignoreras.[8]

Ett annat sätt att komma åt den hemliga nyckeln är att bryta sig in i den dator där signering av certifikat görs. En angripare kan där få tag på den hemliga nyckeln, och omärkligt kopiera den. Om detta skulle lyckas innebär det att angriparen i princip har lyckats skaffa sig en ”identitetskortmaskin”. Det skulle antagligen dröja innan ett sådant tilltag upptäcktes vilket allvarligt skulle skada tilltron till CA:n. Nackdelen med att kopiera CA:ns hemliga nyckel är att de förfalskade certifikaten inte kommer att finnas i de centrala katalogerna, vilket begränsar deras användbarhet. En angripare kan därför i stället försöka attackera CA-systemets administrationsrutiner genom att initiera ett ärende i affärsprocessen, ”utfärda nytt identitetskort”, och sedan få tag på resultatet. En CA måste alltså också ha mycket god kontroll över de kringsystem som är knutet till det centrala systemet som utfärdar certifikatet. Det är osäkert ifall ett intrång i en CA eller dess kringsystem alltid skulle upptäckas. Risken för upptäckt vid intrång är mycket liten i dagens IT-system. Såväl främmande makt som kriminella organisationer

[8] Dan Boneh, De Millo, Lipton, Bellcore Ltd, ”On the importance of checking computations”. Dokumentet finns tillgängligt på http://jya.com/smart.pdf

kan vilja skaffa sig möjlighet att omärkligt få ut falska identitetshandlingar även om det finns billigare och enklare sätt.

Ett intrång i en CA behöver inte innebära att den hemliga nyckeln komprometterats, men kan medföra att det blir svårt att avgöra om en kopiering skett eller inte. Fråga uppkommer då om ogiltigförklaring av utfärdade certifikat.

Organisationer kommer också att utfärda lokalt skapade certifikat, antagligen med en behörighetsbeskrivning. En stor del av dessa certifikat kommer att användas enbart inom organisationen, men de kan också användas i relationer med omgivande organisationer, t.ex. för att visa att en viss anställd vid företaget har attesträtt vid elektronisk handel. Det finns en risk att en angripare bryter sig in i ett företags lokala CA, skaffar sig ett falskt elektroniskt anställningsbevis och beställer varor falskeligen.

5.3 Granskning av en digital signatur (verifikation)

För att granska en digital signatur måste man ha kunskap om att rätt öppen nyckel används och vem nyckeln tillhör. För att granska ett certifikatintyg från en CA krävs den korrekta öppna nyckeln för denna CA. CA:ns öppna nyckel kan granskas med hjälp av ett intyg från en annan (högre) CA. Granskningsprocessen kan pågå i flera nivåer. Oavsett hur många nivåer som används måste granskningskedjan slutligen innehålla en av användaren känd nyckel som erhållits direkt från innehavaren. Detta brukar beskrivas som att CA:ns öppna nyckel ”publiceras”, men detta är något missvisande, eftersom en sådan nyckel är för lång och konstig för att den skall fastna i något slags ”kollektivt medvetande”. Det ligger ett implicit antagande att användare skulle omedelbart ”se” ifall han har fel nyckel, men det är inte nödvändigtvis sant. I stället är det viktigt att varje användare får CA-nyckeln på ett säkert sätt, förslagsvis i samband med registering hos CA:n.

Det finns många möjliga punkter längs en granskningskedja där integriteten hos systemet kan ha komprometterats. Om de övre

nivåerna i en granskningskedja sköts av ett mindre antal operatörer med hög teknisk och administrativ kompetens, med fullständig integritet i förhållande till de transaktioner som signeras, bör det dock kunna fungera.

Angrepp på granskningskedjan påverkar egentligen inte de tekniska egenskaperna hos signaturen, snarare luras den som använder signaturen att tro att en falskeligen anbringad signatur är äkta, dvs. härrör från den utpekade avsändaren. Ofta kan sådana ”tillfälliga” angrepp vara tillräckliga, eftersom granskningen av signaturen av mjukvarumoduler normalt leder till automatiserade beslut, exempelvis vid åtkomstkontroll.

5.4 Katalogfunktionen

Vid mottagarens eller någon annans granskning av digitala signaturer behöver granskaren hitta rätt certifikat från CA:n. Detta sker med hjälp av en katalog. Katalogen kan föras av CA. En angripare kan angripa kommunikationen mellan användaren och katalogen för att kunna påverka informationen som användaren får från katalogen. Om detta lyckas kan användaren tro att han/hon har direktkontakt med katalogen, allt medan angriparen i själva verket sitter i mitten och filtrerar informationen åt båda hållen. En angripare kan också försöka bryta sig in i den dator där katalogen finns. Om detta lyckas kan samma effekter som vid attacken ovan uppnås, fast enklare.

Ett antal effekter kan uppstå när en katalogfunktion angrips. Användaren kan få t.ex. ett revokerat eller felaktigt certifikat vid en förfrågan, felaktiga personuppgifter eller en felaktig behörighetsbeskrivning. Annan väsentlig information som återkallande av certifikatintyg (CRL) kan blockeras så att användaren inte kan ta del av den aktuella informationen. Dessa angrepp får effekter som liknar de ovanstående, men effekterna blir endast temporära. Många effekter kan dock upptäckas och därigenom undvikas om användarens programvara dubbelkontrollerar uppgifterna i det

emottagna certifikatet mot den ställda frågan till katalogen. Dessutom måste certifikatets signatur granskas varje gång det används.

En annan fråga är om listan för återkallade certifikat skall kontrolleras mot katalogen varje gång. Ett förslag är att den användare som väljer att inte kontrollera listan får ta risken om signaturen inte är giltig. Om sådan kontroll sker beror givetvis på vem som utformat programvaran (Om användaren inte kan påverka huruvida denna kontroll görs kan detta leda till otillfredsställande resultat).

Det vore önskvärt ur säkerhetssynpunkt att man inte byggde in administrativa rutiner som onödigtvis skapade återkallade certifikat.

Många av de ovan beskrivna svagheterna och riskerna med granskningskedjor, kataloger, CA-nycklar osv. kan bli upptäckta vid en senare tidpunkt eller vid fortsatt användning av systemet. Det innebär inte att riskerna kan negligeras. Bedrägliga aktiviteter kan ske mycket snabbt i IT-system, i synnerhet om de är automatiserade.

5.5 Inkapsling av smarta kort

Det är av central betydelse för hela signatursystemet att användarens hemliga nyckel inte kommer på avvägar genom olovlig kopiering.

Ett aktivt kort kan utsättas för en rad olika fysiska angrepp; varierad klockhastighet till kortet, varierade och onormala spänningsnivåer, onormal temperatur, kraftig bestrålning av kortet, fysisk manipulation av kiselytan osv.

Även mjukvaran inuti det smarta kortet kan ha olika tålighet mot angrepp. Det smarta kortets operativsystem kan utsättas för påfrestningar på olika sätt; felaktiga transaktioner matas till kortet, avbrutna transaktioner, försök att uttömma interna resurser och därigenom orsaka feltillstånd osv. Det är viktigt att mjukvaran i kortet har mycket hög kvalitet.

Olika kort har olika stor motståndskraft mot denna typ av attacker. De smarta kortens säkerhetskvalitet varierar kraftigt, och

rent generellt är säkerhetsegenskaperna hos de billigaste korten väsentligt lägre än hos de dyrare.

Tillverkarna av smarta kort kan antas komma att lämna vissa garantier för kortens funktion, exempelvis en detaljspecifikation över vilken funktionalitet som garanteras.

Angrepp mot inkapslingen av den hemliga nyckeln kan ske i samband med att kortet fysiskt stjäls från dess ägare eller under normal användning av kortet. Det är allvarligt ifall kortet kan dyrkas upp och den hemliga nyckeln kopieras utan att ägaren kan upptäcka detta vilket skulle kunna ske då ägaren sätter in kortet i en främmande kortläsare i samband med betalning via kortet. Kortläsaren skulle kunna manipulera kortet och därigenom eventuellt dyrka upp kortet. Det är inte säkert att användaren efteråt skulle veta vilken av alla främmande kortläsare som hade manipulerat kortet.

Ett aktivt kort måste motstå manipulationsförsök tillräckligt länge för att användaren skall kunna upptäcka att kortet är stulet, att transaktionen tar för lång tid, osv. Därefter måste användaren ha tid att blockera kortet och denna blockering måste hinna förmedlas till de som granskar och använder den digitala signaturen.

Hur skall användaren förfara med gamla dokument om han misstänker att den hemliga nyckeln har kommit på avvägar? Om detta har skett, kan ett signerat meddelande med vilken lydelse som helst framställas. En datumangivelse i det signerade dokumentet ger då inget skydd för gamla dokument. Det är därmed viktigt att en säker och oberoende tidsstämplingsfunktion används, med hjälp av en neutral och betrodd tredje part.

Det kan också vara värt att notera att den hemliga nyckeln kan exponeras medvetet av endera parten i ett digitalt signerat affärskontrakt, så att därigenom ett kontrakts autenticitet kan ifrågasättas.

5.6 Användarens närvaro: PIN-kod och biometri

Det smarta kortet med den hemliga signaturnyckeln måste vara oanvändbart utan individens närvaro, annars är det inte en personlig signatur. För att tillgodose detta krav utformas kortet så att det är blockerat tills individen har visat sin närvaro.

Att visa individens närvaro kan vara svårt och det finns flera olika sätt att använda. Den vanligaste metoden är att ha en kort hemlig siffersekvens, en PIN-kod, på samma sätt som till bankomatkort. Tyvärr matas i dag denna PIN-kod ofta in via PC:ns mjukvara, vilket innebär att en angripare som har fått in en ”trojansk häst” i PC-systemet kan ta reda på den hemliga PIN-koden. Koden kopieras av den trojanska hästen under transporten från tangentbordsinmatningen till kortet.

Det finns i dag kortläsare med separat tangentbord. Om användaren matar in PIN-koden via detta tangentbord i stället, och koden skickas direkt till kortet utan att passera PC:ns mjukvara finns ingen möjlighet att kopiera PIN-koden.

Ett annat sätt att visa att användaren är närvarande är att använda biometriska identifikationsmetoder (se avsnitt 3.4.3), vilket torde ge betydligt högre säkerhet i identifikationen.

Vid biometrisk identifiering får inte avläsning och inmatning av biodata vara separerade från kortet via PC:ns mjukvara eftersom en trojansk häst i PC:n kan kopiera biodata på samma sätt som den kan kopiera PIN-koden.

5.7 Programvarumodulers distribution

Programvaran i signatursystemet måste distribueras på ett säkert sätt till användaren. Det finns en risk att användare laddar mjukvarumoduler från sekundära källor och att vissa av dessa källor har manipulerats av en angripare. För att förhindra detta får användaren lämpligen mjukvaran och CA-systemets huvudnyckel i samband med mottagande av det smarta kortet.

5.8 Kortets användning av applikationer

Det finns strukturella problem i den mjukvaruarkitektur som omger ett aktivt kort. Den digitala signaturen som äkthetsmärke i digitala dokument behandlas i Datastraffrättsutredningen (SOU 1992:110) och ur denna utredning kan man dra en del viktiga slutsatser runt vilka krav som måste ställas på signeringsförfarandet.

Ur utredningen framgår, att för en digital signatur skall kunna jämställas med en traditionell underskrift och därigenom kunna binda bäraren av en viss identitet till de åtaganden och viljeyttringar som framgår av det som signerats, så krävs att

- signatären är ensam om att kunna utfärda en signatur i signatärens namn (I-kravet),

- signatären tagit del av den informationsmängd som signerats (V-kravet), samt att

- signaturen beräknas som en följd av en aktiv handling från signatären där signatären är medveten om att detta medför att signaturen beräknas samt vilket ansvar det innebär (S-kravet).

Signaturfunktionen i ett elektroniskt ID-kort förmår i sig själv enbart garantera att det första kravet (I) enligt ovan uppfylls nämligen att innehavaren är den enda som kan generera en signatur i innehavarens namn just genom sitt exklusiva innehav av sitt elektroniska ID-kort.

De övriga punkterna (V,S) kan enbart garanteras som en kombination av funktionaliteten i ett elektroniskt ID-kort och funktionaliteten i det tekniska system som används vid signeringstillfället.

Med den digitala signaturen skapas egentligen en elektronisk personlig stämpel. En angripare kan bryta sig in i PC:n och använda stämpeln utan den rättmätige användarens tillstånd och vetskap. Även en användare som ”äger” datorn kan ha dålig kontroll över vad som sker i den. Aktiviteter i PC:n kan ha initierats av ett antal olika parter; mjukvarutillverkare, tjänsteleverantörer, motparter

osv. En angripare kan bryta sig in i datorn och få den att utföra uppgifter för angriparens räkning.

PC:n är en osäker plattform. Det finns många olika sätt att bryta sig in i den – via e-post, via Web, genom trojanska hästar i nedladdade program och genom virus av såväl konventionell sort som makrovirus. Dessutom har användaren oftast en låg datasäkerhetskompetens, vilket gör att det lätt kan bli fel på inställningen av säkerhetskritiska parametrar. En strid ström av nya applikationer och tjänster tillkommer hela tiden och dessa kan innehålla säkerhetshål. Olika tekniska säkerhetslösningar och säkerhetsarkitekturer måste med nödvändighet utvecklas för PC:n, antingen direkt i operativsystemet eller som tilläggsmoduler.

Det kan inom en snar framtid bli vanligt att användaren använder kortet för att handla i olika näringsidkares lokaler. Denna användning har en annan hotbild. De ovan diskuterade kraven ”identifiera (I), verifiera innehåll (V), signera medelst en viljeyttring (S)” kan inte tillfredställas till fullo om den terminal som kortet används i kontrolleras av någon annan än kortinnehavaren. Det finns ingen garanti för att det belopp som kunden tror att han/hon exempelvis betalar är det belopp som terminalen begär underskrift på från kortet. Det finns heller ingen garanti för att terminalen inte skapar fler transaktioner än kunden godkänt eller är medveten om. Om certifikat på ett kort skall kontrolleras vid användning så görs det oftast genom att data som skall signeras eller krypteras skickas ner till kortet tillsammans med en PIN-kod som ger access till kortet. Detta innebär att speciell hårdvara behövs, hårdvara som måste kontrolleras så att den inte ger möjlighet till att samtidigt genomföra mer än en transaktion mot kortet utan kortinnehavarens uttryckliga medgivande.

5.9 Tekniska komplikationer med öppen-nyckelsystem

Tilltron till distributionen av certifikat är ett speciellt problem när två parter som aldrig kommunicerat med varandra skall initiera en kommunikation.

En hemlig nyckel kan komma på villovägar. Detta innebär att falska nycklar kan signeras som därmed inkluderas i kedjor av förtroende. För att vara säker på att alla certifikat som ingår i en förtroendekedja är aktuella och giltiga måste giltigheten för dessa certifikat verifieras vid varje transaktion. Detta innebär en stor mängd transaktioner som därför resursmässigt måste vara mycket billiga (i form av t.ex. bandbreddsåtgång).

För att verifiera det öppna certifikatet behöver tredje man det öppna certifikatet för den CA som signerat det certifikat som skall verifieras. Detta certifikat kan i sin tur verifieras av någon topp-CA eller motsvarande. Denna kontroll bakåt i systemet upprepas till dess att man påträffar ett certifikat som man tror på.

De öppna certifikat som behövs för att verifiera hela kedjan måste vara på en gång tillgängliga. Detta kan göras genom att certifikaten är ordnade i en strikt hierarki och ges ut i samband med att det ursprungliga certifikatet signeras. Denna förtroendekedja måste följas varje gång som man vill verifiera ett certifikat som man inte litar på.

Ett globalt system som används av en icke oväsentlig andel av invånarna i ett land ett par gånger per dygn innebär en så stor mängd transaktioner mot en spärrlista, att genomförandet av själva spärrlistan måste tänkas igenom i detalj. Vilken kryperingsalgoritm och vilken nyckellängd som används bestäms av en policy som dock måste uppdateras. Det enda man köper med kryptering och signering är tid. Allteftersom kunskapen om algoritmer blir bättre och datorerna blir snabbare måste de nyckellängder och krypteringsalgoritmer som används bytas ut. Detta måste kunna ske utan att det fungerande systemet måste byggas upp från början.

Lagring av certifikat på ett kort kan vara ett sätt att se till att certifikaten inte kan kopieras. I samband med detta bör alla öppna

nycklar som behövs för att verifiera certifikatet på kortet lagras på kortet hela vägen upp till topp-CA.

I en strikt nyckelhierarki, vilket är det som är enklast att hantera, certifieras alla nycklarna successivt genom vertikala förtroendekedjor i hierarkistrukturen. Man kan alltid hitta en kedja mellan två certifikat genom att gå via toppnoden. Dess certifikat har inte certifierats genom något annat certifikat, vilket gör toppnoden känslig för attacker. Även s.k. korscertifiering av certifikat nära toppnoden eller av dess nycklar är mycket känsliga för attacker.

Domännamnssystemet (DNS) är en tillämpning där öppen-nyckelsystem kommer att användas. Någon svensk organisation kommer inte att kunna kontrollera toppnoden i nyckelhierarkin. Dock kan denna nyckelhierarki användas för att lagra den information som behövs för att starta andra öppen-nyckel-infrastrukturer. DNS kan således leda till att öppen-nyckel-infrastrukturer som använder annan teknologi startas.[9]

Andra system som måste beaktas är SET (Secure Electronic Transaction), som dock är utformad för fast nyckellängd och fast krypteringsalgoritm och som är ett system främst avsett för kreditkortsliknande betalningar. Systemet används redan i dag i liten skala i ett fåtal pilotprojekt.

Ett ytterligare system som måste beaktas är PGP[10]. Systemet är spritt, och använder inte (utom i den senaste kommersiella versionen från en av levarantörerna) en nyckelhierarki utan i stället en s.k. web of trust. Det innebär att vem som helst kan agera CA för någon annan och åtskillnad görs mellan att lita på att ett certifikat är korrekt och att lita på certifikatinnehavaren som CA.

[9] Frågan behandlas inom ramen för Statskontorets utredning om säkerhetsstrategier, som skall avrapporteras till Kommunikations - departementet i maj 1998.

[10] Pretty Good Privacy, se vidare lista med ordförklaringar. Se även http://www.pgp.com

6 Utvecklingen på marknaden

Rutiner baserade på digital signatur ägnas stort intresse men har inte ännu nått någon omfattande spridning. De används bl.a. då betalningsuppdrag överförs via magnetband och disketter eller via teletransmission till en bank eller ett giroinstitut. Sigill baserat på symmetrisk krypto används också när tulldeklarationer sänds i form av digitala dokument från en räkningsidkare till tullen.

6.1 FN-projekt

En internationell arbetsgrupp som ingår i det av FN administrerade organet UN/EDIFACT[11] bedriver ett arbete benämnt EDIFACT FINANS genom en samarbetsorganisation inom den finansiella sektorn med syfte att utveckla standarder och gemensamma rutiner för att underlätta utväxlingen av information inom världshandeln. Arbetsgruppen har tagit fram en modell för att beskriva hur t.ex. betalningsuppdrag skall skyddas under transport och hur dagens skriftliga avstämningsuppgifter skall kunna bytas ut mot digitala dokument. Modellen, som är generell beträffande framställning och kontroll av digitala dokument, upptar förutom funktioner för den beskrivna signeringen tekniska och administrativa rutiner, varigenom den som tar del av en handling kan verifiera att uppgiften om utställare är riktig och att innehållet inte har manipulerats. Inom gruppen diskuteras vidare frågan om att tillskapa en betrodd tredje part (Trusted Third Party, TTP) som kan anförtros att administrera hemliga nycklar och garantera deras äkthet och knytning till angiven person.

[11] Se http://www.unece.org/trade/untdid/Welcome.html

6.2 EU-projekt

Inom EU har många informationssystem skapats för att medlemsländernas förvaltningar skall kunna samverka och byta information i gemensamma ärenden. Detta arbete samordnas sedan november 1995 i det s.k. IDA-programmet (Interchange of Data between Administrations)[12]. IDA-programmet förväntas leda till rekommendationer och råd angående elektronisk dokumenthantering, rättsfrågor och IT-säkerhet.

Inom sjöfarten pågår ett EU-projekt benämnt ”Bolero”[13], som syftar till att ersätta dagens hantering av konossement vid marina transporter med användning av digitala dokument försedda med digitala signaturer enligt vad som beskrivits ovan med en betrodd tredje part som registrerar innehav av dessa dokument och i varje ögonblick har aktuell information om vem som innehar ett visst dokument. På så sätt kan det genom IT-rutiner visas inte bara att ett dokument är omanipulerat utan också vem som har rätten till visst gods.

Trusted Health Information Systems är ett projekt inom sjuk- och hälsovården med stöd från kommissionen inom ramen för DG XIII:s INFOSEC-program för informationssäkerhet. Projektet är ett av fyra delprogram inom olika områden som rör elektroniska signaturer och TTP-organisationer.

6.3 Sverige

Under 1995 slutfördes projektet Strategisk samverkan kring elektronisk ID inom bank- och finanssektorn. Syftet med projektet var att finna en gemensam teknisk lösning för ett elektroniskt ID-kort för att med hjälp av detta höja säkerhetsnivån i olika elektroniska tjänster. Specifikationerna för lösningen gjordes allmänt tillgängliga.

[12] Se http://www.ipso.sec.be/ida/text/english/about.html
[13] Se http://www.ipso.sec.be/ecommerse/invencom.html#bolero

Samarbetet mellan Rikspolisstyrelsen, Försvarsmakten, Statskontoret, Riksförsäkringsverket, Riksskatteverket och Datainspektionen kring den s.k. allterminalen kan sägas vara ett nästa steg i utvecklingen. I detta arbete togs specifikationer fram för en moduluppbyggd säkerhetsmiljö för persondatorskydd. Till lösningen hör särskilda säkerhetskort (s.k. AT-kort). Korten består av aktiva kort som konfigureras med nycklar för unik elektronisk identitet, nycklar för signering respektive stöd för kryptering.

Våren 1995 bildades den ideella föreningen Säkrad Elektronisk Information i Samhället (SEIS)[14]. I och med SEIS initierades ett fortsatt arbete med syfte att främja utvecklingen av ett ramverk för allmänt accepterade, enkla, praktiska och ekonomiska säkerhetslösningar. Alla samhällssektorer är representerade i föreningen.

I arbetet inom SEIS har de tekniska specifikationerna för de grundläggande säkerhetsfunktionerna elektronisk identifiering, digital signatur och stöd för kryptering på aktiva kort förfinats och kompletterats. SEIS överväger att överlämna relevanta delar av specifikationerna för omvandling till svensk standard under våren 1998, när de något reviderats och harmoniserats med avseende på bl.a. den internationella användningen i Internet. SEIS har också tagit fram regler (”policy”) för utfärdande och certifiering av elektroniska ID-kort (med chip) som till sitt utförande också överensstämmer med den relativt nyligen fastställda SIS-standarden för vanliga, visuella ID-kort. Arbete pågår också inom SEIS med att utarbeta policy för framställningen av ”SEIS-kort” för att kunna garantera att en viss person inte får samma elektroniska identitet etc. som någon annan. Vilka krav som skall ställas på kataloger för certifikat m.m. behandlas också, liksom övriga frågor kring säkerheten i en öppen-nyckel-infrastruktur.

I juni 1997 antog Toppledarforum[15] ett förslag om en gemensam IT-säkerhetslösning i stat, kommuner och landsting. Lösningen baseras på användning i tjänsten av aktiva kort med de tre grundläggande säkerhetsfunktionerna enligt SEIS specifikationer.

[14] Se http://www.seis.se
[15] Se http://saturn.nutek.se/index.html

Arbetet med upphandling av rutiner m.m. för utfärdande av sådana kort inleddes under hösten 1997 av Statskontoret.

Försvaret har ett säkerhetssystem i vilket bl.a. ingår användning av aktiva kort för identifiering, digital signering och kryptering vid överföring av meddelanden. Systemet upphandlades år 1994–95 enligt då gällande standarder och specifikationer. I övrigt framgår den aktuella användningen av AT- och SEIS-kort i det följande.

6.3.1 Användningen av s.k. AT-kort för digital signatur

Tullverket har sannolikt den längsta erfarenheten av digital signatur i form av sigill baserat på symmetrisk kryptering. Redan år 1991 började tullen ge företagen möjlighet att digitalt signera handlingar för import- och exportklarering. Erfarenheterna har varit goda. Sedan 1997 pågår en successiv övergång till allterminallösningen med tillhörande AT-kort. Tullverket utfärdar de erforderliga korten åt företagen. I dag finns ca 7 000 kort i daglig användning i 500 företag med Tullverkets tillstånd. Tre fjärdedelar av det totala antalet klareringshandlingar hanteras helt elektroniskt. Tullverket har valt att arbeta utan CA.

Även Riksskatteverket (RSV) har valt allterminallösningen. Antalet användare med AT-kort är i dag ca 13 000, varav ca 3 000 inom kronofogdemyndigheten. När lösningen är fullt införd under 1999 beräknas det totala antalet användare till ca 15 000. Omkring 250 lokala arbetsställen är kopplade till en för skatteförvaltningen gemensam, central databas för utfärdande och certifiering av AT-korten. I dag används kortens funktioner för lokalt PC-skydd, s.k. stark autenticering (äkthetsverifiering) och linjekryptering. I februari 1998 tillkommer användning av funktionen för digital signering av beslut i förvaltningens nya skatte- och avgiftssystem Magi.

Rikspolisstyrelsen (RPS) har emellertid också valt allterminallösningen. Den har införts på i storleksordningen 15 000 stationära och 2 000 mobila arbetsstationer med sammanlagt omkring 25 000 kortanvändare. I slutet av år 1996 och början av år 1997 genom-

fördes ett i olika avseenden välkontrollerat och framgångsrikt försök med digital signering (med hjälp av AT-korten) och överföring av krypterade analyssvar från Statens kriminaltekniska laboratorium till länskriminalpolisen vid Polismyndigheten i Stockholms län. För åklagarmyndighetens handläggning av elektroniskt signerade dokument krävs emellertid att deras innehåll skrivs ut på papper. Beroende på åklagarmyndighetens krav på utskrift av elektroniskt överförd information använder RPS tills vidare inte AT-kortens funktion för digital signering i den löpande verksamheten.

På socialförsäkringsområdet har Riksförsäkringsverket (RFV) under 1997 ansvarat för införande av allterminallösningen. Totalt omfattas ca 15 000 arbetsstationer. Behovet av digital signering förväntas öka för att underlätta och effektivisera verksamheten i framtiden. Ännu så länge används AT-korten dock endast för identifiering etc. mot datasystemen. Behörighetsadministrationen sköts av försäkringskassorna och certifieringen av AT-kort av RFV:s centrala dataavdelning. Någon tidpunkt för införande av digital signatur i verksamheten är ännu inte fastställd.

Danderyds sjukhus i Stockholms län har nyligen infört en säkerhetslösning motsvarande allterminalen för reglering och administrering av behörigheterna till bl.a. journalsystemen. Liksom hos de ovan beskrivna myndigheterna så utfärdas de erforderliga aktiva korten i sjukhusets egen regi på säkerhetsavdelningen. Verksamheten har utfallit väl. På sikt kan digital signatur integreras med journalsystemet för läkarnas i lag föreskrivna signering av journaluppgifter. Detta kräver dock vidareutveckling av tillämpningarna.

6.3.2 Användningen av s.k. SEIS-kort för digital signatur

För hälso- och sjukvården i övrigt gäller att samarbete inletts mellan landstingen i Skåne, Väst-Sverige och Östergötland samt Huddinge sjukhus i Stockholms läns landsting för utveckling av en testmodell för digital signering med hjälp av aktiva kort konfigurerade enligt SEIS specifikationer och levererade av Posten. Hälso- och

sjukvårdens utvecklingsinstitut (Spri) medverkar i arbetet och modellen avses börja prövas för signering av reseräkningar bland ett femtiotal användare under senare delen av 1998. Även i detta sammanhang diskuteras digital signering av journalerna med aktiva kort för tjänstebruk. Skånelandstinget verkar i det här avseendet ligga längst framme i planerna med planerad start tidigast i början av 1999. I sammanhanget kan noteras att en standard för algoritm för digital signering inom hälso- och sjukvården finns fastställd av det europeiska standardiseringsorganet CEN (ENV 12388).

I mars 1997 gav Centrala studiestödsnämnden (CSN) de studerande på Kungliga Tekniska Högskolan i Stockholm (KTH) möjlighet att digitalt signera vårterminens obligatoriska mitterminsförfrågan eller -försäkran med hjälp av signeringsfunktionen på de studerandes s.k. IDOL-kort (ID-orienterade lösningar)[16]. Experimentet var möjligt tack vare att studerande på KTH under hösten 1996 utrustats med aktiva kort innehållande de tre grundläggande säkerhetsfunktionerna enligt SEIS specifikationer som ett led i en brett upplagd försöksverksamhet i samarbete mellan KTH, Posten, Telia och Tryggbanken m.fl. Användning av digital signatur för försäkran till CSN om pågående studier fungerade tekniskt och praktiskt till stor belåtenhet. Styrkt av bl.a. denna erfarenhet vill CSN gå vidare för att ta vara på motsvarande möjligheter för ansökan, komplettering av ansökan och annan hantering med avseende på studiemedlen. Någon utveckling i stor skala bedöms dock inte vara möjlig förrän de legala aspekterna på digital signatur och därmed sammanhängande frågor helt klarlagts. CSN ser också fördelar med möjligheter att använda digital signatur både inom nämnden och i samarbetet mellan nämnden och andra myndigheter.

I många landsting och kommuner finns omfattande planer på elektronisk handel. Landstinget Dalarna ligger exempelvis mycket långt framme beroende på att landstinget redan för mer än tio år sedan började konkretisera tankarna på att med hjälp av digital teknik radikalt förändra inköpsrutinerna för förbrukningsmaterial inom sjukvården. I dag samlas beställningar i landstingets system för materialförsörjning och går sedan vidare till landstingets egna

[16] Se http://idol.promotor.telia.se/

lager eller aktuella leverantörer. Arbetet med att utveckla elektronisk handel är för övrigt Toppledarforums mest omfattande projekt och ett intensivt arbete med den fortsatta utvecklingen pågår på många håll. Även inom den statliga delsektorn börjar arbetet komma igång. De öppna och generella gränssnitt för säkerhetslösningarna som projektets säkerhetsgrupp tagit fram bygger på användning av aktiva kort med de tre grundläggande säkerhetsfunktionerna elektronisk identifiering, digital signatur och stöd för kryptering enligt de av SEIS framtagna specifikationerna. Möjlighet till juridiskt hållbar digital signering tros vara en mycket viktig framgångsfaktor för elektronisk handel.

Finansinspektionen testar regelmässig elektronisk överföring av uppgifter från ett tiotal banker och försäkringsbolag. Personer på de aktuella bankerna och bolagen har utrustats med aktiva kort levererade av Posten. Två av kortens funktioner används i försöksverksamheten – elektronisk identifiering och stöd för kryptering. Med säker identifiering av uppgiftslämnarna och säker överföring av uppgifterna från bank och bolag till finansinspektionen har krav på digital signering i detta fall inte bedömts nödvändiga. Försöket kommer att utvärderas. Också internt inom Finansinspektionen förutses i framtiden behov finnas av digital signatur.

Nordbanken har sedan senhösten 1997 utfärdat personliga, aktiva kort enligt SEIS specifikationer till ca 10 000 kunder, med eller utan foto beroende på kundernas önskemål. Alla tre grundfunktioner i korten används för bankens Internet-tjänster för ansökan om lån, öppnande av konto och anslutning till fondsparande. Lösningen är i full drift. Lån har exempelvis redan beviljats – helt och hållet utan ”papper”.

I samarbete med flera banker utvecklar Bankgirocentralen en lösning för säkra elektroniska betalningar att användas mellan företagens ekonomisystem och bankgirosystemet. Säkerhetsfunktionerna består av säker elektronisk identifiering, digital signatur och stöd för kryptering med hjälp av aktiva kort enligt SEIS specifikationer. Pilotverksamhet inleds under första kvartalet 1998.

Företaget SignOn utvecklar i samarbete med Stadsbyggnadskontoret i Stockholm, Stockholmshem och Posten en Internetap-

plikation som möjliggör att de regelbundna och obligatoriska ventilationsprotokollen från Stockholmshem kan överföras elektroniskt signerade till Stadsbyggnadskontoret. Försöksverksamhet planeras att påbörjas i mars 1998. I verksamheten kommer aktiva kort enligt SEIS specifikationer att användas. Korten levereras av Posten som också står för säkerhetsplattformen (s.k. CA-funktioner m.m.). I praktiken omvandlar företaget SignOn de ordinarie blanketterna till elektroniska dokument som därefter görs tillgängliga via Internet. Den elektroniska blanketten fylls i av personal på Stockholmshems berörda enheter och signeras digitalt av behörig person med hjälp av det personliga kortets signeringsfunktion, varefter den signerade elektroniska blanketten returneras och därmed blir tillgänglig för Stadsbyggnadskontoret via Internet. Verksamheten är enligt uppgift den första av sitt slag i världen.

6.3.3 Användning av digital signering och verifiering vid Handelsbanken

Också Handelsbanken har en lösning för digital signering i privata bankaffärer över Internet. Handelsbanken har emellertid valt en annan lösning för funktionen än användning av fysiska, aktiva kort. Genom uppkoppling via Internet till Handelsbankens system hämtar bankens kunder helt enkelt en särskild programvara med vars hjälp de på egen hand kan skapa sitt certifikat innehållande den hemliga nyckeln och samtidigt generera motsvarande öppna nyckel. När detta är gjort sänds de elektroniskt (över Internet) till bankens säkerhetssystem, så att certifikatet kan signeras med digital signatur i banken. När det av bankkunden skapade certifikatet signerats av behörig tjänsteman på banken returneras det till kundens system (PC) där certifikatet sedan förvaras. Genom att banken har tillgång till kundens öppna nyckel kan kunden därefter, när så behövs, använda den digitala signaturen i de fortsatta kontakterna med banken.

6.3.4 Secure electronic transaction – SET

SET (Secure Electronic Transaction) är en teknisk specifikation som har utarbetats i syfte att skapa förutsättningar för betalning med kredit/betalkort över Internet och samtidigt utnyttjande av befintlig kontokortsinfrastruktur. Arbetet som påbörjades 1995 görs av VISA och Mastercard tillsammans med ledande programvaruleverantörer. I specifikationen regleras transaktioner, transaktionsformat, certifiering av involverade parter och regler för hur information sekretesskyddas, integritetsskyddas och ursprungskontrolleras. I systemet signeras transaktionerna digitalt med särskild programvara av dels konto-betalkortsinnehavaren och dels butiksinnehavaren. När transaktionen nått banken verifieras signaturerna.

Inom SET upprättas avtal mellan kortutgivande bank och kontokortsinnehavare och avtal mellan inlösande bank och försäljningsställe. Systemet är därmed slutet i betydelsen att det bygger på avtal mellan inblandade parter.

Försöksverksamhet har initierats och bedrivs gemensamt för flera länder i Europa. Även en svensk försöksverksamhet skall inledas i samarbete mellan VISA, FöreningsSparbanken, Handelsbanken, Postgirot Bank och SE-Banken. Försöksverksamheten beräknas omfatta ca 8 000 privatkunder och ett fyrtiotal försäljningsställen. Försöken i Sverige har försenats flera gånger.

7 Rättsliga aspekter

Den nya informationstekniken (IT) har tagits i bruk på nära nog alla samhällsområden.

Det har inom bl.a. rättsväsende, förvaltning och näringsliv blivit allt vanligare att lagring och behandling av data inom en verksamhet fysiskt sker på en annan plats än i de egna lokalerna och att kommunikationen såväl inom som mellan verksamheter sker elektroniskt. Användandet av digitala signaturer kan möjliggöra en övergång från begränsade tillämpningar i främst slutna användningskretsar till användning av *öppna* system för bl.a. förmedling av signerade dokument och digitala ersättningar för traditionella betalningsmedel. Digitala signaturer och motsvarande rutiner för accesskontroll, insynsskydd m.m. är en metod för att uppnå sådan säkerhet och kontrollerbarhet att digitala dokument m.m. godtas på samma sätt som traditionella sådana och detta även i juridiska sammanhang.

Frågor som uppkommer är hur befintliga regler skall tillämpas på digitala handlingar och om den nya tekniken gör det nödvändigt att ändra reglerna. Frågor kring detta har utretts i många sammanhang under de senaste åren. Detta avsnitt avser att utifrån frågeställningar kring användningen av digitala signaturer kort sammanfatta de problem som har ansetts förknippade med att ersätta pappershandlingar med digitalt representerade handlingar. Avsnittet avser att lägga en grund för ställningstagande till vilka rättsliga frågor som måste lösas i fortsatt arbete för att genom bruk av digitala signaturer möjliggöra att allmänt tillgängliga telenät skall kunna användas för säker elektronisk förmedling av handlingar.

En utgångspunkt bör vara att om reglering erfordras så bör denna vara så teknikoberoende som möjligt.

7.1 Rättsområden av intresse – översikt

7.1.1 Regler om formkrav

I vissa rättsregler ställs krav på att en rättshandling skall uppfylla vissa formkrav för att den skall tillerkännas rättsverkan. Några av de vanligaste formkraven är kravet på *skriftlighet*, *egenhändig namnteckning* och att en handling skall vara upprättad i ett fysiskt *originalexemplar*. I kravet på skriftlighet kan i många fall även ligga ett underförstått krav på såväl egenhändig namnteckning som att handlingen upprättas i ett originalexemplar.[17]

Effekterna av att formkrav inte uppfylls varierar. I vissa fall är kravet absolut för rättshandlingens giltighet[18]. I andra fall kan avsteg från skriftlighetskravet medföra marknadsrättsliga sanktioner. Ibland knyts rättsverkningarna till dokumentet som sådant; den som har dokumentet i sin besittning är också innehavare av den rättighet som dokumentet är bärare av. Detta gäller främst s.k. omsättningpapper, t.ex. skuldebrev, växel och check.

[17] IT-utredningen har i sitt betänkande konstaterat att ett stort antal författ - ningar på förvaltningsområdet som re glerar förfarandet vid handläggningen av ärenden innehåller begrepp såsom ”handling” och ”skriftlig”, SOU 1996:40 s. 92. Datastraffrättsutredningen har bl.a. behandlat användningen av begreppen ”handling” i anknytning till rättegångsbalken, SOU 1992:110 s. 106 ff. Handlingsbegreppet i anknytning till tryckfrihetsförordningen är senast behandlat av Datalagskommittén. Se särskilt SOU 1997:39 s. 471 ff. samt 493 ff. Utredning kring begrepp som ”skriftlig” och ”handling” har även företagits i samband med tulldatoriseringen, dvs. i samband med införande av Tulldatasystemet (TDS). Se särskilt SOU 1989:20, Tullregisterlag m.m. Delbetänkande av utredningen om lagstiftningsbehovet vid tulldatoriseringen (TDL-utredningen). Vidare har dessa begrepp och därtill hörande frågor behandlats avseende skatteförvaltningens ärendehantering i samband med utredning om författningsän dringar nödvändiga för att möjliggöra ett utökat användande av automatisk databehandling i skatteförvaltningens ärendehantering, Ds 1994:80 Elektronisk dokumenthantering inom skatteförvaltningen. Se även Seipel, *Electronic Documents related to the Swedish EDI-system for Customs Authorities*.

[18] Se t.ex. 4 kap. 1 § tredje stycket jordabalken

Formkravet har främst sin grund i rättssäkerhets- och effektivitetssträvanden vid ekonomiskt, eller av andra skäl, betydelsefulla aktiviteter. Häri ligger bl.a. att säkra bevisning om att en åtgärd faktiskt vidtagits, vem som vidtagit den och om dess innehåll. En annan aspekt är att statsmakten, genom att ställa vissa formkrav, kan underlätta olika förfaranden kring en aktivitet, t.ex. beskattning. Formkravet kan dessutom tjäna som varning och därmed säkerställa att en part uppmärksammas på konsekvenserna av en rättshandling.

Formkraven varierar mellan olika länder. Vid internationella transaktioner uppkommer därför frågan vilket lands formkrav som skall tillämpas. Frågan om avtalets form intar en särställning i internationell privaträtt. En rättshandling anses normalt vara giltig till formen antingen om den uppfyller formkraven i det land vars lag skall tillämpas på avtalet, eller om den uppfyller formkraven enligt lagen på den ort där rättshandlingen företogs. Vissa undantag följer dock av Romkonventionens art. 9 (se *bilaga 7*). Vid elektronisk kommunikation kan problem uppkomma att bestämma var en rättshandling företagits.

Elektroniskt överförd information (elektroniska dokument) särskiljer sig från traditionella pappersdokument i flera avseenden som har direkt betydelse för dess rättsliga status. För det fall att lagstiftaren ställer upp krav på *underskrift* torde detta inte kunna uppfyllas med hjälp av elektroniska dokument.[19]

För att säkerställa att digitala signaturer tillerkänns samma rättsverkan som den traditionella namnteckningen torde det krävas att regler som innehåller formkrav ändras så att digitala signaturer – som tillkommit med erforderlig grad av säkerhet – tillskrivs samma verkan som egenhändiga namnteckningar.[20] Med hänsyn till att motiven bakom uppställda formkrav i olika författningar kan variera, är en generell regel som likställer digitala signaturer med namnteckning inte möjlig. Sannolikt måste i stället en prövning ske från författning till författning. För att få en överblick över de

[19] SOU 1996:40 s. 95. Betänkandet anger på annat ställe (s. 93f) att *skriftlig handling* även kan innefatta elektroniska dokument.
[20] SOU 1996:40 s. 95. Jfr dock Christina Hultmark, Elektronisk handel och avtalsrätt, 1998, s. 66 f.

lagregler som innehåller krav på skriftlig form och undertecknande fordras att det sker en inventering av samtliga rättsregler i den svenska rättsordningen, överenskommelser med främmande makt och EU-bestämmelser. Detta leder dock till träffmängder som är alltför stora för att medge en detaljerad analys över vilka rättsregler som kan aktualiseras i samband med bruket av digitala signaturer, åtminstone inom ramen för denna promemoria. Den s.k. IT-utredningen fann för sin del vid en databaserad sökning att orden ”underskriv-” och ”underteckna-” förekom i 100 respektive 462 författningar, medan ”skriftlig-” förekom i 1 095 författningar. Som jämförelse kan nämnas att man i den danska rapporten till Folketinget om säker digital kommunikation[21] funnit 1 400 lagkrav på underskrift samt omkring 4000 lagkrav om skriftlighet[22].

I den svenska lagstiftningen förekommer det en rad författningar med krav på att handlingar skall vara skriftliga eller undertecknade. Nedan återges endast några exempel på lagrum som uppställer krav på underskrift. För en mer fullständig redovisning av författningar som innehåller krav på underskrift hänvisas till *bilaga 3*.

- Köpehandlingen skall undertecknas av såväl säljare som köpare vid överlåtelse av fast egendom (4 kap. 1§ jordabalken).

- En rättegångsfullmakt skall vara egenhändigt undertecknad av part (12 kap. 8 § rättegångsbalken).

- Årsbokslut skall skrivas under av bokföringsskyldig med angivande av dagen för underskriften (11 § bokföringslagen).

- Firmateckning skall enligt firmalagen ske genom tydlig angivelse av den fullständiga firman och underskrift med namn av firmatecknare (26 § firmalagen).
- Testamente skall underskrivas av testator i två vittnens samtidiga närvaro (10 kap. 1 § ärvdabalken).

[21] Rapporten lades gemensamt fram av fem departement den 16 december 1997.
[22] http://www.fsk.dk/fsk/div/digkomrd.html

IT-utredningen tillsattes i maj 1994 med uppgift bl.a. att utreda användningen av elektroniska dokument inom förvaltningen och näringslivet (Dir. 1994:42). Den lade i mars 1996 fram förslag till författningsändringar som f.n. är föremål för överväganden inom Justitiedepartementet[23]. De lagförslag som är av direkt betydelse för digitala signaturer bifogas i *bilaga 4*.

7.1.2 Bevisfrågor

7.1.2.1 Allmänt

Även i de fall skriftlig form eller egenhändig underskrift inte utgör ett formellt krav tillmäts sådan form eller underskrift stor betydelse i bevishänseende. Skillnaden mellan underskrift på papper och digital signatur torde emellertid här vara mindre än i fråga om formkravet.

Svensk rättsskipning bygger på principen om *fri bevisprövning*[24]. Det finns inte någon begränsning av vilka kunskapskällor som får användas – bevisföringen är fri. Domaren är vid sin värdering av bevisningen obunden av lagregler – bevisvärderingen är fri. Det finns således ingen särskild begränsning enligt svensk rätt i fråga om möjligheten att åberopa eller beakta IT-material som bevisning.

Normalt sett torde det spela mindre roll om en som bevis åberopad handling företes i huvudskrift (original), kopieform eller som ett protokollsutdrag i en process. Problemen är närmast av praktisk art.

– Hur klarläggs fakta i IT-miljön? Osäkerhet kan föreligga om uppgifternas tillkomsthistoria och tillförlitlighet.

[23] SOU 1996:40 Elektronisk dokumenthantering. Utredningen – som är till mycket god hjälp för förståelsen av integreringen av IT i svensk förvaltning – finns tillgänglig på http://www.dtek.chalmers.se/Datafrihet/Sou/1996/40/
[24] 35 kap 1 § rättegångsbalken

- Värderingen av IT-material i en process kan vara tekniskt komplicerad. Hur bör den som bedriver handel via t.ex. Internet gå tillväga för att underlätta en riktig bevisvärdering? Vem bör ses som utställare till en potentiell handling? Vem skall därvid anses ”ha lämnat” de för bevistemat relevanta uppgifterna, när nya uppgiftssammanställningar genereras med andra sökbegrepp än de som varit avsedda.

- Hur skall behovet av medverkan från t.ex. experter på berörda informationssystem säkerställas?

Dessa frågor behandlas närmare av Datastraffrättsutredningen (SOU 1992:110) och i Europarådets rekommendation No. R (95) 13 Concerning Problems of Criminal Procedure Law Connected with Information Technology.

7.1.2.2 Bevisbördan vid förfalskningsinvändning

I rättspraxis har ansetts att, om en föregiven gäldenär bestrider en handlings äkthet, det åligger borgenären att visa att handlingen är äkta (jfr NJA 1976 s. 667). Om en gäldenär gör gällande att en handling visserligen är äkta men att handlingens text ändrats, s.k. innehållsförfalskning, har däremot gäldenären enligt uttalanden i doktrinen i princip bevisbördan för sitt påstående.

Frågan om dessa bevisbörderegler bör tillämpas även när det gäller förfalskningar av inköpsnotor i samband med användandet av ett kontokort som inte är en värdehandling och inte heller ett legitimations- eller presentationspapper har prövats i rättsfallet NJA 1992 s. 263. Högsta domstolen (HD) ansåg det åvila kontokorthavaren att göra åtminstone antagligt att det förelåg en förfalskning. Om detta krav uppfyllts fordras, enligt HD, för bifall till kontokortsföretagets talan att företaget visar att inköpsnotan är äkta. Denna regel gäller enligt rättsfallet såväl vid innehållsförfalskning som vid underskriftsförfalskning.

7.1.3 Civilrättsliga frågor

Detta avsnitt behandlar kortfattat standarder, standardavtal och patentfrågor. Vad gäller ansvarsfrågor i olika partsrelationer behandlas detta i avsnitt 7.4.6.

7.1.3.1 Standarder

För att möjliggöra globalt fungerande kommunikationer pågår arbeten inom standardiseringsorganen.

På internationell nivå arbetar Internet Engineering Task Force (IETF), ISO/ITU och World Wide Web Consortium (W^3C) med standarder som avser öppna nycklar, certifikat och digitala signaturer.[25]

ISO och IEC har en gemensam kommitté för IT-standardisering, JTC 1. En kommitté[26] inom JTC 1 har utvecklat en standard för digitala signaturer, benämnd ”ISO/IEC 9796 Digital signature schemes giving message recovery”. Denna standard består av fyra delar, ”Mechanisms using redundancy”, ”Mechanisms using a hashfunction”, ”Mechanisms using a check-function” samt ”Discrete-logarithm based mechanisms”.

Den första delen är från år 1991 och därmed den äldsta signaturstandarden. Den beskriver användningen av RSA i en innehållsrik bilaga. Arbete pågår med att ta fram en ny standard, ISO/IEC 14888 ”Digital signatures with appendix”, som bl.a. innefattar användning av DSA, Schorr, ElGamal och elliptiska kurvor.

Datastraffrättsutredningen nämner som en fotnot i avsnittet ”Begrepp och teknisk bakgrund”, s. 78, ISO 7498 Part 2 angående en definition av digital signatur. Denna fastställdes som Svensk Standard år 1989.

[25] Om säkerhet och pålitlighet vid elektronisk kommunikation – Mot en europeisk ram för kryptering och digitala signaturer, KOM(97)503 slutlig, s. 24

[26] SC 27, se http://www.iso.ch:8080/jtc1/se27/

Det vanligaste formatet för certifikat är X.509 v3[27].

SET (Secure Electronic Transactions) är en protokollstandard som används av industrin och som har konstruerats för att man på ett säkert sätt skall kunna överföra känslig information via öppna nätverk.

För den finansiella sektorn i USA har den federala standarden DSS antagits av ANSI X9; X9.30, som innefattar DSA och SHA-1. Arbete pågår med X9.31 som använder ”reversible DSA” och X9.62 som använder elliptiska kurvor.

Statskontoret har i sin rapport 1997:18, Svenska delen av Internet, gjort en sammanställning över befintliga säkerhetsstandarder för användning på Internet. Sammanställningen bifogas, se *bilaga 3.*

I SIS katalog över Svensk Standard, 1997:2, återfinns under ämnesområde 35.040.00, ”Kodning av teckenmängder och annan information”, en rad standarder rörande dataskydd.

I det internationella standardiseringsarbetet prövas regelmässigt om en tilltänkt standard berörs av något patentanspråk. Om så är fallet krävs, för att ett förslag till standard skall bli antaget, att berörda patenträttsinnehavare tillkännager att licenser kommer att utfärdas på rättvisa och lika villkor.

Avslutningsvis kan nämnas att standardiseringsarbete kan visa sig vara alltför tidskrävande och att även s.k. de facto-standarder kan uppkomma på marknaden.

[27] Om säkerhet och pålitlighet vid elektronisk kommunikation – Mot en europeisk ram för kryptering och digitala signaturer, KOM (97)503 slutlig, s. 24

7.1.3.2 Standardavtal

Den typ av standardavtal som förekommer i dag inom IT-miljön (s.k. EDI-standardavtal) omfattar normalt ingen reglering av digitala signaturer. Man kan dock anta att den traditionella EDI-kommunikationen, som i dag sker i slutna system, i viss utsträckning kommer att ersättas med kommunikation i öppna nät. Tekniken med digitala signaturer möjliggör att många av nackdelarna med kommunikation i öppna nät kan undvikas. Om utvecklingen går dithän, kommer sannolikt parter som har kontinuerliga avtalsrelationer att reglera hanteringen av digitala signaturer genom avtal. För andra aktörer är detta mer tveksamt. Man kan dock tänka sig situationer där även dessa grupper kommer att omfattas av standardavtal som reglerar digitala signaturer. Detta kan t.ex. gälla i ett elektroniskt köpcentrum, där alla aktörer anslutit sig till köpcentrumets allmänna avtalsvillkor i frågan.

Inom ramen för CA-verksamhet förekommer standardregleringar – s.k. Certification Practice Statement, CPS – vari vanligen framgår vilken teknik CA använder sig av, CA:s handläggningsrutiner samt omfattningen av CA:s ansvar.

7.1.3.3 Patentfrågor

Som framgår i avsnitt 2.1, utnyttjas signatur- och hash-algoritmer vid signering med digitala signaturer. Dessa algoritmer kan vara föremål för patentskydd. Vissa komponenter eller funktioner som är viktiga för den tekniska implementeringen kan också vara patenterade, t.ex. inom området smarta kort. Om lagstiftning rörande vilken teknik som skall användas för framställning av digitala signaturer bedöms nödvändig, måste förekomsten av patentskydd beaktas.

Implementeringspatent för IC-kort

Patent på en teknik för att göra det möjligt att exempelvis utföra endast *en* digital signatur per aktiveringstillfälle finns. För att ånyo göra en signatur krävs sålunda att kortet aktiveras på nytt av innehavaren. De mest aktuella algoritmerna är följande.

Signaturalgoritmer: Dessa finns i två former.

- RSA, som även är användbar för s.k. öppen nyckelkryptering, är den mest kända och mest använda algoritmen för digitala signaturer. Den förekommer i internationell standard[28]. Den är patenterad i USA[29], men fri för användning i Europa.

- DSA, som ingår i den amerikanska signaturstandarden DSS. Även den är patenterad[30]. NIST, som står bakom lanseringen av DSS, har dock deklarerat att den skall erbjudas avgiftsfri på världsmarknaden. DSA är emellertid föremål för en patenttvist och det är skrivande stund oklart om tvisten är löst[31].

Elliptiska kurvor: Denna matematiska bakgrund för att skapa nya och effektivare signaturalgoritmer är i sig inte patenterad för signaturbruk. Dock har många effektiva implementeringar, där elliptiska kurvor utnyttjas, patenterats.

Hash-algoritmer: De vanligaste hash-algoritmerna, som förekommer i samband med digitala signaturer, är inte patenterade.

[28] ISO, ISO/IEC
[29] Patentet går ut den 20 september 2000.
[30] Patentet är från den 27 juli 1993.
[31] Patentintrång har hävdats av Diffie-Hellman, Merkle-Hellman och Schnorr.

7.1.4 Straffrättsliga och straffprocessuella frågor

Den straffrättsliga anpassningen till IT-miljön

Frågor om straffrättsligt skydd i IT-miljö har tidigt behandlats inom bl.a. OECD[32] och Europarådet. I Europarådet har en rekommendation[33] utarbetats angående vilka förfaranden som bör vara kriminaliserade.

Vissa lagändringar har genomförts i Sverige för att bereda straffrättsligt skydd på IT-området; dels i samband med datalagens[34] införande, dels med anledning av ett betänkande av Förmögenhetsbrottsutredningen[35]. Sverige har härigenom fått ett straffrättsligt skydd som omfattar förfaranden i IT-miljön i huvudsak.

På ett område, som är av särskilt intresse i anknytning till digitala signaturer, har det dock inte gjorts några författningsändringar, nämligen i fråga om brotten mot urkund[36].

Enligt svensk rätt är brotten mot urkunder i huvudsak inriktade på att skydda intresset av att kunna lita på bevismedlen. Från principiell synpunkt torde det vara självklart att sådana digitala dokument som är avsedda som bevismedel, är lika skyddsvärda som pappersurkunder. Detta synsätt har också kommit till uttryck i den tidigare omnämnda Europarådsrapporten. I rapporten rekommenderas att manipulationer med elektroniska dokument bör vara kriminaliserade i samma utsträckning som beträffande traditionella pappershandlingar.

Datastraffrättsutredningen

[32] OECD Report No. 10, Computor-related Crime: Analysis of Legal Policy, 1986
[33] Recommendation No. R(89)9 on Computor-related Crime and final report of the European Committee on Crime Problems, 1990
[34] Prop. 1973:33
[35] SOU 1983:50 och prop. 1985/86:65
[36] 14 och 15 kap. brottsbalken

För att belysa diskussionen kring de straffrättsliga aspekterna på digitala signaturer återges nedan i korthet synpunkter från Data-straffrättsutredningen (SOU 1992:110). Utredningens arbete är för närvarande under övervägande inom Regeringskansliet.

Det straffrättsliga förfalskningsskyddet tar i gällande rätt främst sikte på traditionella pappersurkunder och den information som dessa är bärare av. I rättspraxis har man dock, under trycket av den tekniska utvecklingen, godtagit vissa elektroniska dokument som urkunder. Detta trots att den ofrånkomliga prövningen av det berörda objektets äkthet endast varit möjlig genom resonemang som inte är förenliga med brottsbalkens synsätt och systematik. Ibland har man därmed tangerat gränsen för vad som kan anses vara straffrättsligt godtagbar analogibildning[37]. Det får därför anses i vart fall oklart om och i vilken utsträckning digitala dokument åtnjuter ett straffrättsligt skydd. För det fall ett regleringsbehov föreligger finns det anledning att överväga i vilken utsträckning detta kan tillgodoses genom en anpassning av befintliga bestämmelser i brottsbalken och/eller i vad mån behov föreligger att åtstadkomma en särlagstiftning. Med hänsyn till de digitala dokumentens obundenhet till nationella gränser, finns det även anledning att överväga behovet av att harmonisera strafflagstiftningen internationellt.

LAGRUM I BRB	BROTTSRUBRICERING
14:1	Urkundsförfalskning
14:2	*Förvanskning av urkund*
14:3	*Grov urkundsförfalskning*
14:4	Undertryckande av urkund
14:9	Brukande av falsk urkund
14:12	*Försök och förberedelse till urkundsförfalskning, grov urkundsförfalskning, undertryckande av urkund och brukande av*

[37] SOU 1992:110 s. 249

	falsk urkund
15:10 första stycket	Osann försäkran
15:10 andra stycket	*Vårdslös försäkran*
15:11 första stycket	Osant intygande
15:11 andra stycket	Brukande av osann urkund
15:12	Missbruk av urkund
15:13	Förnekande av underskrift
23:2 första stycket	Förberedelse till brott
36:5–6	Tvångsmedel

Tabell: De lagrum som varit föremål för mer principiella överväganden återges med fet, icke kursiverad, stil.

För att kunna straffrättsligt skydda ett dokument – oavsett om det är digitalt eller av traditionellt snitt – krävs dels att dokumentet innehåller någon form av utställareangivelse som kan straffrättsligt knytas till den som uppger sig vara utställaren eller den som falskeligen uppger att någon annan än han själv är det, dels att dokumentet kan äkthetsprövas. Det som i detta sammanhang särskiljer de digitala dokumenten från de traditionella pappersurkunderna är just svårigheten att kontrollera om och i vilken utsträckning dokumentet varit föremål för förvanskning i något avseende. Till skillnad från pappersurkunden är innehållet i ett digitalt dokument inte låst till något fysiskt medium utan kan i normalfallet lagras, transporteras, mångfaldigas och ändras utan att dessa förfaranden låter sig kontrolleras. Att bereda möjligheter till sådan kontroll är ett av de huvudsakliga syftena med en digital signatur.

För att kunna erbjuda digitala dokument ett straffrättsligt skydd mot t.ex. förfalskningar krävs därför rutiner för att kunna ”låsa” *innehållet* i dokumentet så att ändringar i dokumentet inte kan göras med mindre än att de kan upptäckas vid en kontroll. Liksom i fråga om vanliga lås torde det inte finnas något digitalt lås, varken nu eller inom överskådlig framtid, som kan erbjuda ett hundraprocentigt skydd mot forcering. Detta i sig torde inte utgöra något hinder mot att straffrättsligt skydda digitala dokument. Fråga är

dock vilka krav på säkerhet som skall ställas på ett digitalt lås för att det digitala dokumentet skall kunna åtnjuta ett straffrättsligt skydd. En annan fråga av betydelse i sammanhanget är i vilken utsträckning en manipulation av ett dokument skall kunna verifieras vid en kontroll för att ett straffrättsligt skydd skall kunna åtnjutas. Ytterligare en fråga som bör belysas är i vad mån det finns anledning att differentiera det straffrättsliga skyddet så att digitala dokument som inte uppfyller kraven på godtagbara digitala lås inte helt ställs utan skydd[38].

En lagteknisk lösning bör under alla förhållanden ges en sådan utformning att de kontroller som är möjliga inom IT-miljön kan användas samtidigt som den framtida utvecklingen av dessa system inte motverkas.

Digitala signaturer

Digitala signaturer syftar till att säkerställa *vem* som har ställt ut ett digitalt dokument och att *innehållet* i handlingen inte är manipulerat.

För att med framgång kunna realisera ett system med digitala signaturer krävs att verksamheten redan från början åtnjuter allmän tillit. Detta förutsätter inte enbart ett val av teknik som kan erbjuda hög säkerhet, utan även ett fullgott straffrättsligt skydd mot missbruk av tekniken.

Det pågående arbetet inom SEIS bygger på att skapa digitala signaturer med s.k. aktiva kort, vars funktioner ”öppnas” med hjälp av PIN-koder. De aktiva korten avses till det yttre att utformas som vanliga ID-kort. Innehavaren till kortet förutsätts memorera och hemlighålla PIN-koden.

[38] Datastraffrättsutredningen har föreslagit att digitala meddelanden som inte uppfyller kraven på kontrollbarhet bör ges ett begränsat straffrättsligt skydd. Detta kan enligt utredningen tillgodoses genom att en ny bestämmelse om ansvar för *missbruk av handling* införs. Utredningen föreslår därvid att ansvar bör inträda först vid br ukande av objektet.

Så länge korten endast används för traditionell hantering[39], bör nuvarande rutiner för utgivning och användning av ID-kort tillämpas. För sådana objekt finns såväl ett fungerande straffrättsligt skydd som fungerande överenskommelser mellan aktörerna.

Frågan är emellertid hur man bör se på skyddet för PIN-koden respektive de digitala data som finns lagrade på t.ex. ett chip som ett aktivt kort försetts med. Enligt gällande svensk rätt utgör det inte något brott i sig att lista ut och att skriva någon annans lösenord. Datastraffrättsutredningen har därför i sitt betänkande föreslagit en ny regel om missbruk av lösenord[40]. En fråga är i vilka fall ett chip med lagrade data omfattas av urkundsbegreppet.

Fråga är vidare hur man bör betrakta förfaranden där annan än den för vilken en digital signatur är utställd, begagnar sig av det aktiva kortet och PIN-koden. Lika litet som det går att tekniskt kontrollera vem som gjort ett uttag från en bankomat, går det att kontrollera vem som begagnat sig av en viss digital signatur. Det går naturligtvis att fastställa för vem signaturen är utställd men inte av vem den brukats, än mindre om detta skett inom ramen för innehavarens samtycke. Denna begränsning i förening med den potential av områden där signaturen kan användas, ger upphov till frågan om inte varje bruk av en digital signatur av annan än den för vilken signaturen är utställd bör kriminaliseras.

En annan typ av missbruk mot vilket straffrättsligt skydd kan övervägas är om någon, som har försett en handling med sin digitala signatur, förnekar att han signerat handlingen. Hur säkra rutinerna än görs vållar ett förnekande av signatur alltid osäkerhet och

[39] Kortinnehavaren åberopar sitt kort inför en person som gör en ”manuell” kontroll av om kortinnehavaren är den han utger sig för att vara, t.ex. vid begäran om tillträde till en lokal.

[40] ”Den som *olovligen brukar lösenord* eller annan hemlig identitetsinformation, som kan ge åtkomst till data för automatisk informationsbehandling, i avsikt att ge sig eller annan ut för att vara viss person eller lämnar ut sådan identitetsinformation för att missbrukas på det sättet, döms, om åtgärden innebär fara i bevishänseende ...”

merarbete. Sådana förfaranden borde måhända därför kriminaliseras på motsvarande sätt som i traditionell miljö[41].

Straffprocessuella tvångsmedel

De straffprocessuella frågorna har ett nära samband med straffrätten. De brottsutredande myndigheterna kan nämligen i vissa fall – genom beslut av domstol, åklagare eller polis inom ramen för s.k. straffprocessuella tvångsmedel – ges befogenhet att vidta åtgärder som normalt inte är tillåtna för myndigheter. Den straffrättsliga och den straffprocessuella regleringen kännetecknas härvid av känsliga gränsdragningar mellan å ena sidan skyddet för den enskildes fri- och rättigheter[42] och å andra sidan det allmännas intresse av att bereda skydd mot vissa typer av angrepp. Härvid berörs såväl Sveriges internationella åtaganden som bestämmelser i grundlag och vanlig lag. Motsvarande frågor måste lösas för digitalt förvarande handlingar.

Frågan om en anpassning av det straffprocessuella regelsystemet till IT-miljön har behandlats av Datastraffrättsutredningen. Även Polisrättsutredningen har i sitt slutbetänkande (SOU 1995:47 Tvångsmedel enligt 27 och 28 kap. RB samt polislagen) berört sådana frågor. Förslagen från dessa utredningar bereds för närvarande inom Justitiedepartementet. Andra frågor om straffprocessuella tvångsmedel som kan ha beröringspunkter med IT-miljön behandlas av Buggningsutredningen (JU 1996:07, dir. 1996:64).

Även internationellt är straffprocessuella frågor med anknytning till informationsteknik behandlade. Europarådet har antagit en

[41] Jfr bestämmelsen i 15 kap. 13 § brottsbalken om förnekande av underskrift och Datastraffutredningens förslag till IT-anpassning av 14 kap. 9 §.

[42] Även inom ramen för den enskildes fri- och rättigheter kan motstående intressen uppstå. Som exempel kan nämnas en situation där ett intrång i den personliga integriteten, i form av hemlig telefonavlyssning, kan möjliggöra att ett planerat brott mot den kroppsliga integriteten (t.ex. mord) avvärjs.

rekommendation[43] i ämnet och för närvarande pågår ett arbete som har till syfte att skapa en konvention som berör bl.a. internationellt samarbete i sådana frågor[44].

7.1.5 Förvaltningsrättsliga frågor

Förvaltningslagen (1986:223) innehåller inte något krav på att ett meddelande som inkommer till en myndighet skall vara underskrivet av avsändaren. Enligt 10 § 3 st. förvaltningslagen får en myndighet dock begära att ett meddelande som inte är underskrivet skall bekräftas av avsändaren genom en egenhändigt undertecknad handling. Krav på att handlingar skall vara undertecknade finns däremot i specialförfattningarv vilka äger företräde före förvaltningslagen (3 § förvaltningslagen)

7.1.5.1 Elektroniska dokument i svensk lagstiftning

I nuläget har elektroniska dokument vunnit insteg i knappt trettio svenska författningar, se *bilaga 6*. Ett elektroniskt dokument definieras härvid som en upptagning vars innehåll och utställare kan verifieras genom ett visst tekniskt förfarande[45]. Användande av elektroniska dokument har reglerats främst inom tull- och skatteområdet, inom exekutionsväsendet samt i fråga om pantbrevsregister. Riksdagen har vid tre tillfällen uttalat att frågan om elektroniska dokument i förvaltningsförfarandet måste få en generell lösning[46].

På såväl på tull- som skatteområdet krävs ett särskilt medgivande från den mottagande myndigheten för att få ge in lagstadgade

[43] Recommendation No. R (95) 13 Problems of criminal procedural law connected with information technology.
[44] Committee of Experts on crime in cyberspace, PC-CY.
[45] T.ex. i 12 § tullagen (1994:1550), 2 kap. 2 § lag (1990:325) om självdeklaration och kontrolluppgifter, 2 a § indrivningsförordningen (1993:1229).
[46] Betänkande 1989/90:KU2, 1990/91:KU11 samt 1993/94:LU33.

uppgifter i elektroniskt format. Generaltullstyrelsen har lämnat utförliga anvisningar om elektronisk uppgiftslämning i föreskrifter (TFS 1994:45) för tillämpning av tullagen och tullförordningen.

Bakgrunden till lagändringarna om elektroniska dokument på skatteområdet återfinns i Finansdepartementets Ds 1994:80 Elektronisk dokumenthantering inom skatteförvaltningen samt i prop. 1994/95:93 med samma namn. En elektronisk akt föreslogs kunna innehålla alla handlingar i ett ärende, såväl handlingar som upprättats i elektronisk form som elektroniska avbildningar av pappersburna handlingar. Elektroniska handlingar upprättade inom skatteförvaltningen föreslogs bli rättsligt likställda med pappersdokument. Från och med år 1998 kan RSV eller skattemyndighet medge skattskyldig att ge in sin deklaration i form av ett elektroniskt dokument[47]. Hittills har endast deklarationsbilagor, som inte behöver undertecknas, kunnat lämnas på av RSV anvisat elektroniskt format. Detta format har utgjorts av ett system baserat på en smart diskett, benämnd ELDA. I ELDA-systemet erhåller användaren en diskett med certifikat samt privata och öppna nycklar. Disketten innehåller även de program användaren begagnar i kommunikationen med skatteförvaltningen. RSV arbetar på en vidareutveckling av webb-baserad teknologi för uppgiftslämnande, vilken ingår i den s.k. IN/UT-dataplattformen. RSV avser att möjliggöra säker kommunikation med utnyttjande av standardprogram för Internet och med SSL-protokollet eller starkare kryptering.[48]

7.1.5.2 Arkivfrågor

Arkiv, här använt som benämning på en funktion snarare än som en lokal eller ett bestånd av handlingar, har under århundraden varit en garant för att handlingar som dokumenterar rättigheter och

[47] Jfr 26 § skattebetalningslagen (1997:483) och 2 kap 2 § lag (1990:325) om självdeklaration och kontrolluppgifter.

[48] Riksskatteverkets program för elektroniska dokument och digitala signaturer finns angivna i en preliminär rapport med förslag för 1998, RSV dnr 2847-97/920.

skyldigheter skall kunna bevaras. Under denna tid har funktionen också undergått förändringar, från att vara inriktad på legala frågor till att främst förknippas med vetenskapliga och kulturella aspekter på de bevarade handlingarna. Detta har lett till att betydelsen av arkiv och de bestämmelser som rör arkiv kommit att underskattas som ett inslag i bevarandet av rättssäkerheten. Under senare år har dock de offentligrättsliga aspekterna uppmärksammats i lagstiftningen.

Den nu gällande arkivlagen (1990:782) trädde i kraft den 1 juli 1991. I samband därmed utfärdade Riksarkivet ett helt nytt regelverk (RA-FS 1991:1 m.fl.), som innehåller dels reviderade bestämmelser, dels en kodifiering av praxis gällande arkivområdet. Författningarna behandlar alla moment i arkivbildningen, från framställning av handlingar till krav på arkivlokalens utformning. De grundläggande kraven i författningarna är mediaoberoende och gäller alla typer av handlingar; papper, ADB-upptagningar, mikrofilm etc. De är vidare utformade på ett sådant sätt att de inte innehåller onödig detaljstyrning utan i stället möjliggör för den arkivbildande myndigheten att utnytta framställningssätt m.m. som är lämpliga för ändamålet. Begränsande är i stort sett endast de inskränkningar som följer av att de framställda handlingarna skall kunna läsas och överföras till nya databärare över tiden utan att vissa viktiga egenskaper förändras.

Om framställning av ADB-upptagningar

I arkivlagen fastställs följande syften för arkivbildningen.

- Myndigheternas arkiv är en del av det nationella kulturarvet.

- Myndigheternas arkiv skall bevaras, hållas ordnade och vårdas så att de tillgodoser rätten att ta del av allmänna handlingar, behovet av information för rättskipningen och förvaltningen, och forskningens behov (3 §).

För att dessa syften skall kunna uppnås, och det bör särskilt noteras att det inte finns någon inskränkning i tiden för ovanstående, krävs bl.a. att myndigheten vid framställningen av handlingar använder materiel och metoder som är lämpliga med hänsyn till behovet av arkivbeständighet (5 §).

Användning av ADB för arkivbildningen och framställningen av handlingar kan innebära en hel del problem. Till förekommande av manipulation, oavsiktliga ändringar m.m. ställs krav på system för behörighetskontroll, säkerhetskopiering, förvaring av dubbla exemplar på skilda platser m.m. När det gäller den fysiska databärarens bristande beständighet har detta hanterats genom regelbunden överföring till nya databärare. Med denna strategi har det även varit möjligt att möta problemet med att den tekniska utrustningen, p.g.a. den snabba utvecklingen, snabbt blir föråldrad.

Den tekniska utvecklingen för med sig även ett annat problem, nämligen det stora antalet format för data i form av teckenuppsättningar, filformat, kompressionsmetoder etc. De åtgärder som vidtagits för att i berört hänseende säkerställa ett bevarande är byggt på en strategi som avviker något från den som rör fysiska databärare, t.ex. pergament och papper. Säkerställandet av den logiska beständigheten, dvs. att innehållet i ADB-upptagningar kan bevaras, har hanterats genom att Riksarkivet föreskrivit att ADB-upptagningar, som skall bevaras, måste framställas i enlighet med internationella, europeiska eller nationella standarder eller åtminstone kunna konverteras till sådan standard för att man skall kunna garantera att de kan bevaras på lång sikt. Föreskrifterna är endast tvingande när ADB-upptagningar överlämnas till arkivmyndigheten. I annat fall skall dessa ses som en (stark) rekommendation vid avställning av ADB-upptagningar för långtidslagring hos myndigheten (dvs. när uppgifter inte längre behövs för myndighetens verksamhet). Då de flesta typer av ADB-upptagningar (t.ex. register, ordbehandlingsdokument, e-postmeddelanden etc.) normalt inte har sådana egenskaper som kan gå förlorade vid en konvertering, har det hittills varit möjligt att lösa de flesta problem med bevarande.

Om handlingars egenskaper och gallring

De egenskaper som är avgörande för om en handling skall anses autentisk och tillförlitlig behandlas bl.a. inom den arkivvetenskapliga disciplinen diplomatik, som har sitt ursprung i det medeltida Europa. I dag är det kanske vanligare att man ägnar sig åt dessa frågor inom kriminaltekniska laboratorier och i domstolar än inom arkivsektorn. Men spåren av diplomatiken kan återfinnas såväl i de regler som summariskt behandlades i det föregående avsnittet, som i den gallringsdefinition som används i Riksarkivets författningssamling.

Gallra – förstöra allmänna handlingar eller uppgifter i allmänna handlingar; förstöra sådana handlingar/uppgifter i samband med överföring till annan databärare räknas som gallring om överföringen medför informationsförlust, förlust av möjliga informationssammanställningar, förlust av sökmöjligheter eller förlust av möjligheter att fastställa informationens autenticitet.

I detta sammanhang är det främst förlusten av möjligheten att fastställa informationens (dvs. handlingens) autenticitet som är intressant och som bör vägas mot de syften i arkivlagen som återgivits ovan. När det gäller överföring mellan myndigheter skulle det teoretiskt sett vara möjligt att garantera att digitalt signerade ADB-upptagningar kan bevaras i det upprättade formatet. Myndigheterna skulle kunna fatta överenskommelser om långsiktigt läsbara format. Alternativt skulle Riksarkivet kunna föreskriva om sådana. Det torde vara svårt, om än inte omöjligt, att i förvaltningslagen (1986:223) – som komplettering till den regel (10 § 3 stycket) som rör myndighetens rätt att begära egenhändigt undertecknad handling – införa tvingande regler om de tekniska format som får användas när allmänheten lämnar uppgifter eller inger handlingar i form av ADB-upptagningar till en myndighet. För digitala handlingar som upprättas av enskilda kommer sannolikt huvudregeln att vara ”gallring för att bevara” i de fall inte särskilda formkrav kan ställas av myndigheten. Ökade kostnader för ett bevarande (p.g.a. ökat

behov av konvertering samt minskade möjligheter att säkert fastställa vem som är utställaren av en digital handling) kan till följd härav uppkomma.

Olika roller vid framställning av konventionella handlingar

För behandlingen av relationerna mellan myndigheterna, Riksarkivet och CA, kan det vara av visst intresse att känna till något om relationerna i den mer konventionella miljön. Riksarkivet fungerar här som kravställare, gentemot myndigheterna. Myndigheterna har att följa de tekniska krav som ställs på papperskvaliteter, metoder för framställning av reprografiska kopior m.m. Härigenom ställs även indirekta krav på leverantörerna. Det är Statens provningsanstalt (SP) eller annat ackrediterat certifieringsorgan inom arkivområdet som kontrollerar att de produkter och tjänster som används uppfyller Riksarkivets krav. Ackrediteringsorganet SWEDAC kontrollerar i sin tur att SP uppfyller de krav som kan ställas på ett certifieringsorgan (t.ex. i fråga om lokaler, dokumentation, personalens utbildning). Riksarkivet och landsarkiven kontrollerar slutligen att myndigheterna använder sådana produkter som uppfyller Riksarkivets tekniska krav vid framställning[49]. Som alternativ till certifiering kan en s.k. leverantörsförsäkran användas. Ett sådant förfarande förutsätter emellertid att krav ställs på producenters och leverantörers interna kontroll- och kvalitetssystem.

7.1.6 Internationell privat- och processrätt

Digitala signaturer kommer i stor utsträckning att användas vid elektronisk kommunikation över nationsgränserna. Oavsett kommunikationens syfte (handels- eller annan affärstransaktion, informationsöverföring, penningöverföring etc.) kan problem av

[49] Jfr även Elektronisk dokumenthantering (SOU 1996:40), bil. 3 ”Arkiv – bevarande och gallring”, s. 241 ff och bil. 4 ”Rättsliga standarder”, s. 249 ff

rättslig natur uppstå. När sådana problem uppstår vid gränsöverskridande kommunikation uppkommer också frågor om vilket lands lag som gäller och vilkets lands domstolar som är behöriga att slita en tvist.

De regler som ger svar på sådana frågor utgör den internationella privat- och processrätten. En genomgång av rättsregler som kan få betydelse för användning av digitala signaturer skulle vara ofullständig om inte även dessa regler omnämndes.

Det problem av internationellt privaträttslig karaktär som här är av störst intresse rör frågan om vilket lands lag som skall avgöra om ett avtal med internationell anknytning är formenligt upprättat.

I takt med den ökade internationaliseringen av handeln aktualiseras internationellt privaträttsliga problem allt oftare. Detta torde vara anledningen till att internationella organisationer och mellanstatliga organ som UNCITRAL och EU inte bara ser som en viktig uppgift att samordna regleringen av infrastrukturen för digitala signaturer, utan finner det också viktigt att utröna i vad mån ländernas nationella lagstiftningar om digitala signaturer och elektroniska dokument kan samordnas.

En genomgång av vissa principer inom den internationella privat- och processrätten återfinns i *bilaga 7.*

7.1.7 Specialreglering

Vissa problem kan tänkas uppkomma på grund av att de krypteringsalgoritmer som används för framställning av digitala signaturer kan vara att anse som s.k. strategiska produkter och därmed vara föremål för exportförbud. Det regelverk som finns på området finns redovisat i delbetänkandet E-pengar – näringsrättsliga frågor (SOU 1998:14), i avsnittet 4.10.1. De slutsatser som utredningen därvid kommer till torde i viss utsträckning bli tillämpbara också beträffande digitala signaturer eftersom i båda fallen autenticitet och inte konfidentialitet är syftet med användningen av tekniken. Skillnader torde dock finnas i förhållande till vad utredningen haft att ta ställning till.

7.2 En internationell utblick

7.2.1 UNCITRAL

Inom ramen för FN:s handelsrättskommission (UNCITRAL)[50] pågår f.n. ett arbete med att utarbeta modellregler för digitala signaturer. Arbetet är en vidareutveckling av den modellag om elektronisk handel som UNCITRAL antog vid sin 29:e session år 1996. Regleringen av digitala signaturer skall framför allt behandla ansvarsfördelningen mellan nyckelinnehavare, CA och den som förlitar sig på en digital signatur. Inför de förhandlingar som hölls i januari 1998 hade ett underlag utarbetats med i huvudsak följande innehåll.

Regleringen skall vara teknikneutral på så sätt att även andra tekniker än digitala signaturer enligt öppen-nyckel-konceptet omfattas. En definition föreslås av vad som utgör en ”säker elektronisk signatur”. En typ av säker elektronisk signatur är en digital signatur enligt öppen-nyckel-konceptet. Även andra tekniska tillvägagångssätt kan uppfylla de krav som ställs för att en elektronisk signatur skall kvalificeras som säker.

UNCITRAL förhåller sig neutral till frågan om CA-verksamhet skall bedrivas under tillståndkrav. Anledningen är främst att detta anses vara en offentligrättslig fråga (Public law), som inte lämpar sig för internationell harmonisering via UNCITRAL.

När det gäller ansvarsfördelningen mellan de parter som är inblandade vid upprättandet av digitala signaturer föreligger förslag på tre centrala artiklar.

– Artiklarna 2 och 3 reglerar i vilken utsträckning en nyckelinnehavare är ansvarig för meddelanden som signerats med dennes nyckel. Nyckelinnehavaren presumeras vara bunden, men kan undgå bundenhet om han förmår visa att han inte själv signerat meddelandet. Om anledningen till att nyckeln blivit utsatt för missbruk går att hänföra till nyckelinnehavaren själv (t.ex. genom att han lämnat ut sin PIN-kod eller inte spärrat nyckeln

[50] Se http://www.un.or.at/uncitral

inom rimlig tid från det han blivit medveten om risken för missbruk) kan han bli skadeståndsskyldig mot förlitande part.

– Artikel 11 reglerar ansvaret mellan CA och CA:s kontraktsparter, vilket kan vara såväl nyckelinnehavare som förlitande part. Utgångspunkten är att parterna är fria att själva reglera ansvarets omfattning, så länge som detta inte är oskäligt.

– Artikel 12 reglerar CA:s ansvar i förhållande till förlitande parter som inte står i avtalsförhållande med CA. Utgångspunkten är att CA bär ett ansvar för all förlust som förorsakas förlitande part om denne lider skada på grund av att han felaktigt förlitat sig på en verifierad digital signatur. Om CA emellertid förmår visa att CA inte agerat vårdslöst, undgår CA ansvar. CA kan begränsa sitt ansvar i förhållande till förlitande part genom att ange för vilket ändamål den digitala signaturen är avsedd eller genom att ange ett maximaltransaktionsvärde.

Det som här omtalats om arbetet i UNCITRAL utgör endast underlag för förhandlingarna. Den slutliga regleringen kan komma att i betydande utsträckning avvika från underlaget.

7.2.2 ICC

ICC, den internationella handelskammaren, bedriver ett omfattande projekt inom området elektronisk handel, ECP-projektet (Electronic Commerce Project). I projektet deltar ett stort antal företag och organisationer från näringslivet (banker, fraktbolag, teleoperatörer m.fl.). Projektet är uppdelat i tre arbetsgrupper, ”Electronic Trade Practices”, ”Information Security” samt ”E-Terms”.

Arbetet inom Information Security har resulterat i att ICC givit ut publikationen General Usage for International Digitally Ensured

Commerce (GUIDEC)[51]. Arbetet med GUIDEC startade i samband med arbete inom ICC med de legala aspekterna av elektronisk handel och användning av digitala signaturer samt med att etablera en internationell kedja för registrerings- och certifieringsorgan.

Syftet med GUIDEC är att etablera ett regelverk för att skapa tillförlitlighet till digitala meddelanden och till certifieringsprocessen. GUIDEC är utarbetat på grundval av det amerikanska advokatsamfundets regelverk ”Digital Signature Guidelines” (se därom under avsnittet 7.2.9 USA) och UNCITRAL:s modellag för elektronisk handel. Dokumentet är enbart avsett för transaktioner mellan näringsidkare och sålunda inte för transaktioner där konsumenter är delaktiga. Regelverket är inte avsett att påverka nationella regler som ställer krav på att en handling skall vara bestyrkt av t.ex. Notarius Publicus. Dokumentet är avsett att kunna tillämpas oavsett vilken jurisdiktion som är tillämplig. Hänsyn till att särregleringar förekommer i olika lagstiftningar tas uttryckligen i vissa regler.

GUIDEC innehåller en omfattande begreppsapparat. Den engelska termen ”Ensure” spelar en central roll i terminologin i dokumentet. Begreppet används i stället för ”digitally signing” eftersom det ansågs finnas betydande skillnader mellan en ordinär underskrift och en signatur framställd med elektroniskt medium. Även om GUIDEC i första hand tar sikte på s.k. öppen-nyckelsystem, är innehållet tillämpligt även på andra metoder och så tillvida inte avsett att vara låst till viss teknologisk lösning.

Själva regelverket – ”Best Practices” – innehåller regler om signering, ”ensuring”, av meddelanden och om certifiering. Regelverket är förhållandevis detaljrikt och innehåller kommentarer.

Dokumentet är avsett att revideras i takt med utvecklingen på området för elektronisk handel.

[51] International Chamber of Commerce, nov. 1997, Paris, Frankrike, Internet www.iccwbo.org. GUIDEC finns tillgänglig på http://www.iccwbo.org/guidec2.htm

7.2.3 OECD

Organisation for Economic Co-operation and Development (OECD) ser frågan om digitala signaturer som skärningspunkten i avvägningen mellan å ena sidan nationernas intresse av att främja elektronisk handel och å andra sidan deras legitima säkerhetsmässiga och polisiära betänksamhet inför allmänt spridd kryptering av kommunikation och information[52]. Organisationen antog i mars 1997 ett antal rekommendationer till medlemsländerna om riktlinjer för krypteringspolicies. Dessa rekommenderar bl.a. medlemsstaterna att ta bort, och att undvika att i form av krypteringspolicies skapa, omotiverade hinder för internationell handel och utveckling av informations- och kommunikationsnätverk.

Samtidigt utfärdade OECD riktlinjer för krypteringspolicies med det uttalade syftet att främja användningen av kryptografi[53]. Riktlinjerna bygger på följande i dokumentet uttalade principer.

- Tillit till kryptografiska system bör främjas genom marknadens utveckling av pålitlig teknologi. Tillit kan vidare skapas genom statliga regelverk och tillståndsgivning, samt statlig användning av tekniken.

- Användning av valfri kryptografisk metod skall vara tillåten. Myndigheternas kontroll får inte gå utöver vad som krävs för att fullgöra statens uppgifter.
- Krypteringstekniken skall utvecklas på den öppna, konkurrensutsatta marknaden.

- Utvecklingen av internationella tekniska standarder, kriterier och protokoll för krypterad kommunikation bör främjas.

[52] OECD, Paris den 12 juni 1997, ”Electronic Commerce – Opportunities and Challenges for Government”. Rapporten finns tillgänglig på http://www.oecd.org/dsti/sti/it/ec/prod/

[53] OECD, Paris den 27 mars 1997 ”Cryptography Policy: The Guidelines and the Issues”. Rapporten finns tillgänglig på http://www.oecd.org/dsti/sti/it/secur/prod/e-crypto.htm

- Individernas grundläggande rättigheter om skyddad kommunikation och skydd för personliga uppgifter skall respekteras.

- Nationella regler om tillgång till kryptografiska nycklar skall så långt som möjligt respektera individernas integritet.

- Regler om ansvar för tillhandahållare och användare av kryptografiska tjänster bör utformas.

- Staterna bör söka internationellt samarbete i utvecklingen av krypteringspolicies, bl.a. för att undvika att skapa handelshinder.

7.2.4 EU

Inom EU har kommissionen riktat uppmärksamheten mot den elektroniska handeln[54], som man anser vara en av de viktigaste pådrivande krafterna för att det globala informationssamhället skall kunna utvecklas. Kommissionen har ansett den elektroniska handeln kräva ett samordnat regelverk på gemenskapsnivå. Utöver direktivet om rättsligt skydd för databaser förutser man ytterligare behov av gemenskapslagstiftning med sikte på bl.a. datasäkerhet och integritetsskydd.

För att underlätta den kommersiella användningen av elektronisk kommunikation genom öppna nät har kommissionen konstaterat att det krävs säkrare rutiner och har därvid pekat på behovet av en reglering av digitala signaturer. Man befarar emellertid att olika regler i medlemsstaterna kan hindra eller störa den fria rörligheten av varor och tjänster inom gemenskapen, vilket i sin tur hindrar utvecklingen av den elektroniska handeln. Kommissionen överväger därför att föreslå en gemenskapslagstiftning för digitala signaturer,

[54] Några av kommissionens viktigare initiativ på området är: ”Om säkerhet och pålitlighet vid elektronisk kommunikation – Mot en europeisk ram för kryptering och digitala signaturer”, KOM(97)503 slutlig, ”Ett europeiskt initiativ inom elektronisk handel”, KOM(97)157 slutlig, samt direktiv 96/9/EG om legala skyddet för databaser (EGT L 77, 27.3.96, s. 20)

som man anser bör vara genomförd före år 2000. Man har därvid pekat på följande regleringsbehov.

- Vissa gemensamma regler för certifieringsorganen (CA) krävs för tillförsäkra att certifikat som utfärdats i ett medlemsland skall erkännas av övriga medlemsländer. Vissa gemensamma typer av certifikat kan även behövas, så att graden av försäkran och tillit blir densamma inom EU. Regler om bl.a. tillstånd och självcertifiering bör dock bestämmas på medlemsstatsnivå.

- För att bidra till ett ömsesidigt erkännande av digitala signaturer internationellt kommer kommissionen att identifiera behovet av gemensamma tekniska krav och verksamhetskrav, liksom gemensamma värderingskriterier och -procedurer, inklusive standarder, avseende varor.

- För att digitala signaturer skall erkännas som likvärdiga med traditionella signaturer, ur bl.a. bevishänseende, kan det komma att krävas nationella bestämmelser. Kommissionen avser att utreda behovet av gemenskapsregler på området.

- Ett internationellt ramverk för digitala signaturer kommer att kräva såväl att gemenskapen som medlemsstaterna deltar i det internationella arbetet på området.

I sammanhanget skall även nämnas en rapport[55], som bl.a. beskriver digitala signaturer och dess problemställningar som beställts av Infosec-sekretariatet vid kommissionens DG XIII. Rapporten innehåller vidare förslag på hur ett direktiv om digitala signaturer på gemenskapsnivå *kan* utformas, se *bilaga 8*. Man har därvid stannat vid två alternativ.

[55] Legal and Regulatory Issues for the European Trusted Services Infrastructure; Final Report, juni 1997. Rapporten är framtagen av Mr. Luca Remotti, Istituto per lo Studio della Vulnerabilitá delle Societá Tecnologicamente Evolute – IST, Rom, Italien.

I det ena alternativet föreslås direktivet – utöver definitioner av elektroniska dokument, digitala signaturer och betrodda tredjepartsorgan (TTP) – endast omfatta regler om deras egenskaper, uppgifter och användning.

I det andra alternativet föreslås direktivet därutöver även innehålla regler om vilka handlingar systemet kan tillämpas på, var och när ett avtal har kommit till stånd, vad som är ”virtuell hemvist” etc.

I rapporten finns vidare en sammanställning över rättsläget i medlemsstaterna vad avser digitala signaturer, se *bilaga 9*.

Under 1998 avser kommissionen att föreslå vidare åtgärder på området, bl.a. ett direktiv om digitala signaturer. Kommissionen avser vidare att bl.a. uppmuntra industrin och internationella standardiseringsorgan att utveckla standarder som kan samverka med varandra, för digitala signaturer och kryptering.

7.2.5 Italien

Italiens parlament har den 15 mars 1997 antagit en lag som syftar till att reformera den offentliga förvaltningen och åstadkomma administrativa förenklingar. Bestämmelserna innebär att arbetsuppgifter och befogenheter flyttas över till regionerna och till lokala myndigheter.

Enligt artikel 15.1 i denna lag får IT-myndigheten (l´Autorità per l´informatica) i uppdrag att förverkliga ett enhetligt kommunikationsnät för myndigheterna inom den offentliga förvaltningen för att därigenom tillgodose behovet av samordning, hög kompetens och självständiga bedömningar. IT-myndigheten skall utarbeta ramavtal inför upphandling av tjänster och utrustning för elektronisk överföring.

Artikel 15.2 stadgar att handlingar, data och dokument, som hanteras med hjälp av automatisk databehandling (ADB) eller via telekommunikation av den offentliga förvaltningen och av enskilda, liksom avtal som sluts på detta sätt, har rättsverkan. Reglerna omfattar även arkivering och överföring. Vidare skall de närmare

bestämmelserna läggas fast i särskilda förordningar som skall utfärdas 180 dagar efter lagens ikraftträdande.

Ett förslag till förordning, som innehåller bedömningsgrunderna och tillvägagångssättet för tillämpningen av lagen beträffande framställning, arkivering och överföring av dokument med hjälp av ADB eller via telekommunikation, har lagts fram och godkänts av det italienska Ministerrådet den 5 augusti 1997. Förslaget innehåller tre kapitel.

Allmänna bestämmelser

Kapitel I innehåller definitioner bl.a. av begreppen elektroniskt dokument (documento informatico), digital signatur, asymmetriskt nyckelpar, privat nyckel, öppen nyckel, biometrisk nyckel, tidsstämpel och elektronisk adress (art. 1). Vidare stadgas följande. Ett elektroniskt dokument som framställs eller arkiveras med hjälp av ADB eller överförs via telekommunikation har rättsverkan om det överensstämmer med bestämmelserna i denna förordning (art. 2). IT-myndigheten skall lägga fast tekniska regler för hanteringen av elektroniska dokument. Reglerna skall med hänsyn till den vetenskapliga och tekniska utvecklingen ses över vartannat år. Även regler av bl.a. organisatorisk natur som syftar till att garantera säkerhet, integritet och sekretess skall införas (art. 3). Ett elektroniskt dokument enligt denna förordning uppfyller det legala kravet på skriftlighet (art. 4). Kopior, avskrifter och utdrag m.m. som hanteras enligt bestämmelserna i förordningen har rättsverkan om äktheten intygas av en tillförlitlig person (art. 6). Ett elektroniskt dokument som undertecknas med en digital signatur enligt artikel 10 har rättsverkan som urkund (art. 5). För deponering av den privata nyckeln finns särskilda bestämmelser (art. 7). Beträffande certifieringsförfarandet stadgas bl.a. att de öppna krypteringsnycklarna skall förvaras hos ett certifieringsorgan under minst tio år. Certifieringsorganet skall registreras i en förteckning som skall finnas tillgänglig hos IT-myndigheten (art. 8). Användare och certifieringsorgan skall förhindra att skada uppstår för någon

annan. Certifieringsorganet skall därutöver uppfylla vissa skyldigheter som syftar till att säkert identifiera den som ansöker om certifikat och att säkra nyckelhanteringen. Det finns även bestämmelser om hur certifieringsorgan skall förfara när dess verksamhet upphör (art. 9).

Digital signatur

I kapitel II framgår att elektroniska dokument kan förses med en digital signatur antingen i själva dokumentet eller i ett separat dokument. En sådan digital signatur är jämförbar med en underskrift. Om den digitala signaturen är återkallad eller förfallen anses inte någon underskrift föreligga (art. 10). Avtal som hanteras med hjälp av ADB och via telekommunikation med användande av digital signatur har full rättsverkan (art. 11). Ett elektroniskt dokument som överförs via telekommunikation anses avsänt och mottaget om det har sänts till den uppgivna elektroniska adressen. Tidpunkten för framställandet, avsändandet eller mottagandet av ett elektroniskt dokument har bevisvärde vid invändningar från tredje man. Ett elektroniskt dokument som överförs via telekommunikation på ett säkert sätt är jämförbart med en underrättelse[56] per post i de fall som lagen medger det (art. 12). Anställda som sköter överföringen av dokument via telekommunikation är ålagda tystnadsplikt och får inte mångfaldiga sådana dokument. Avsändaren har ansvaret för informationsöverföringen intill dess överlämnande har skett till mottagaren (art. 13). Elektroniska betalningar skall ske enligt fastlagda tekniska regler (art. 14). En digital signatur vars äkthet intygas av en notarie eller annan auktoriserad tjänsteman ersätter rättsligen sigill, stämplar, kontrasignering och märken av allehanda slag. Ett dokument som lämnas eller sänds via telekommunikation eller med hjälp av ADB till en offentlig förvaltning har full rättsverkan om dokumentet försetts med en digital signatur

[56] I den italienska texten används ordet *notificazione.* I detta arbete har det inte gått att klargöra om det är underrättelse, av mer allmän karaktär, som avses, eller om det gäller delgivning.

(art. 16). Den offentliga förvaltningen hanterar själv sina krypteringsnycklar, vilka certifieras och offentliggörs av justitieministern eller den som han delegerat uppgiften till (art. 17). Elektroniska dokument som upprättas hos offentliga förvaltningar utgör originalinformation. Tekniska regler för upprättande och bevarande av elektroniska dokument beslutas av IT-myndigheten i samråd med arkivmyndigheterna (art. 18). I alla elektroniska dokument från offentliga förvaltningar skall den egenhändiga namnteckningen ersättas med en digital signatur (art. 19).

Verkställighetsbestämmelser

Enligt bestämmelserna i kapitel III skall de statliga förvaltningarna före den 31 december 1997 lägga fast en utvecklingsplan för ADB-systemen. Förvaltningarna skall genomföra eller revidera dessa planer, inom fem år räknat från den 1 januari 1998. En utvärdering skall göras och presenteras i en rapport senast den 31 december 1998 inför ställningstagandet om pappersarkiven skall ersättas med arkiv i elektronisk form (art. 20). Den praktiska hanteringen av dataflödet skall de offentliga förvaltningarna ha förberett till den 31 december 1998 (art. 21). Vid denna tidpunkt skall förvaltningarna också kunna tillhandahålla elektroniska formulär och blanketter, som skall vara åtkomliga via telekommunikation (art. 22).

7.2.6 Tyskland

Tyskland har relativt nyligen antagit en lag om reglering och ramvillkor för informations- och kommunikationstjänster. Lagen antogs av Förbundsdagen den 13 juni 1997 och trädde i kraft den 1 augusti 1997 med undantag för ändringar i upphovsrättslagen, vilka trädde i kraft den 1 januari 1998. Lagen omfattar 11 artiklar, som innefattar en lag om teletjänster (art. 1), en lag om skydd för persondatauppgifter i teletjänster (art. 2), en lag om digitala signaturer (art. 3), ändring i strafflagen (art. 4), ändring i lagen om brott mot ordningsföreskrifter (art. 5), ändring i lagen om spridande

av skrifter farliga för ungdomar (art. 6), ändring i upphovsrättslagen (art. 7), ändring i lagen om prisangivelser (art. 8), och vissa ytterligare regleringar.[57]

Med stöd av 16 § lagen om digitala signaturer utfärdade Förbundsregeringen en förordning om digitala signaturer, som trädde i kraft den 1 november 1997. Nedan följer inledningsvis en kort beskrivning av lagen och förordningen om digitala signaturer. Därefter följer en grundligare genomgång av lagens innehåll.

7.2.6.1 Sammanfattning av lagen och förordningen om digitala signaturer

I lagen och förordningen om digitala signaturer regleras infrastrukturen för uppbyggnaden av säkerheten kring digitala signaturer. I lagen anges

- de krav som de tekniska komponenterna måste uppfylla. Hänvisningar finns även till vissa standardspecifikationer på området som också måste vara uppfyllda, samt

- en ram för den administrativa uppbyggnaden av digitala signaturer. Bland annat anges hur tilldelning av signaturnycklar skall gå till och hur de tekniska komponenterna skall vara beskaffade. Det finns vidare instruktioner för innehavaren av en signaturnyckel och regler för nyckelns användning.

Lagen bygger på att såväl uppbyggnaden som driften av infrastrukturen skall ske i privat regi och i fri konkurrens. Såvida inte annat är särskilt föreskrivet reser inte lagen något hinder mot att tillverkning och användning av digitala signaturer sker på annat sätt än det i lagen föreskrivna. En digital signatur som framställs genom alla led i enlighet med lagen, anses dock alltid vara garanterad en särskild grad av säkerhet.

[57] BT-Drs. 13/7934 den 11 juni 1997.

I lagen godtas tekniska komponenter och intyg (certifikat) från stater inom EU och EES, under förutsättning att dessa uppfyller lagens krav. Motsvarande gäller även intyg m.m. från andra stater om det finns överstatliga eller mellanstatliga avtal därom.

I förordningen om digitala signaturer beskrivs dels säkerhetskraven för de tekniska komponenterna, dels de närmare bestämmelserna om CA-verksamhet. I 4 § p. 1 förordningen föreskrivs bl.a. att bäraren av den privata signaturnyckeln skall finnas i personligt förvar.

7.2.6.2 Lagen om digitala signaturer

Nedan återges paragrafvis de centrala delarna i den tyska lagstiftningen om digitala signaturer.

1 § Syfte och tillämpningsområde

Syftet med lagen är att ange de allmänna villkor som måste vara uppfyllda för att digitala signaturer skall anses som säkra i den mening att förfalskningar av digitala signaturer eller förfalskningar av signerade data på ett tillförlitligt sätt kan konstateras. Lagen tillåter även andra förfaringssätt med digitala signaturer än det i lagen föreskrivna, såvida annat inte är särskilt föreskrivet.

2 § Begreppsapparaten

Digital signatur: Sigill för digitala data som tillverkats med en privat signaturnyckel och som med hjälp av en tillhörande öppen nyckel – försedd med nyckelcertifikat från ett certifieringsorgan eller behörig myndighet – gör det möjligt att bekräfta identiteten hos signaturnyckelns innehavare och datas äkthet.

Certifieringsorgan: Fysisk eller juridisk person som innehar tillstånd enligt 4 § och vars uppgift är att intyga tilldelningen av öppna signaturnycklar till fysiska personer.

Certifikat: Ett med digital signatur försett digitalt intyg som avser tilldelning av en öppen signaturnyckel till en fysisk person (signaturnyckelcertifikat) eller ett särskilt digitalt intyg (attributcertifikat) som, med en entydig hänvisning till ett signaturnyckelcertifikat, innehåller ytterligare uppgifter.

Tidsstämpel: Ett med digital signatur försett digitalt intyg från ett certifieringsorgan, som anger att vissa data inlämnats dit vid en viss tidpunkt.

3 § Behörig myndighet

Det är tänkt att en nyinrättad federal myndighet under det tyska ekonomidepartementet för tillsyn av telekommunikationer och post – ungefärligen motsvarande den svenska Post- och telestyrelsen – skall vara behörig myndighet. Till dess en sådan myndighet är inrättad kommer departementet för post- och telekommunikationer att vara behörig myndighet.

4 § Licensiering av certifieringsorgan

Ett certifieringsorgan måste ha tillstånd för att få bedriva verksamhet.[58] För att erhålla tillstånd krävs att sökanden kan visa prov på tillförlitlighet och sakkunskap och i övrigt uppfyller lagens och förordningens krav på säkerhet. Sökanden måste därvid inom viss angiven tid presentera ett säkerhetskoncept och ett intyg om att säkerhetsåtgärderna genomförts för den behöriga myndigheten. Det omtalade intyget utfärdas av ett av den behöriga myndigheten godkänt organ.

[58] I detta arbete har denna bestämmelse tolkats så att det är certifieringsorgan som avser att uppfylla lagens krav som behöver tillstånd.

Den behöriga myndigheten utfärdar certifikat för signaturnycklar som används för att underteckna certifikat. Certifikaten skall vid varje tidpunkt vara tillgängliga för var och en via allmänt tillgängliga teleförbindelser. Detsamma gäller även för uppgifter om adresser och telefonnummer till certifieringsorganen, spärrade certifikat, upphörande av och förbud mot utövande av tillståndspliktig verksamhet och återkallade tillstånd.

Avgifter tas ut för det allmännas åligganden enligt lagen och förordningen.

5 § Tilldelning av certifikat

Den som ansöker om ett certifikat måste identifieras. Tilldelningen av en öppen signaturnyckel skall vara intygad i ett nyckelcertifikat. Certifikatet skall vid varje tidpunkt kunna kontrolleras av var och en via allmänt tillgängliga teleförbindelser. Med samtycke från nyckelinnehavaren skall certifikatet kunna återkallas[59] på samma sätt.

På begäran skall uppgifter om tillstånd av olika slag och behörighet att företräda tredje person tas in i nyckelcertifikatet.

På begäran får, i stället för namn, en pseudonym föras in i certifikatet.

Det ankommer på certifieringsorganet att ombesörja att åtgärder vidtas så att i certifikatet intagna uppgifter inte obemärkt kan förfalskas. Certifieringsorganet måste också vidta åtgärder för att säkerställa att den privata nyckeln hålls hemlig. Förvaring av privata nycklar hos certifieringsorganet är otillåtet.

Certifieringsorganets personal som arbetar i certifieringsverksamheten skall vara tillförlitlig.

Vid tillverkning av signaturnycklar och när certifikat utfärdas skall sådana tekniska komponenter användas som anges i 14 §. Detta gäller även tekniska komponenter som möjliggör kontroll av certifikat.

[59] Den tyska originaltexten talar om ”abrufbar zu halten”.

6 § Informationsskyldighet

Certifieringsorganet skall informera sökanden om de åtgärder som krävs för att bidra till säkra digitala signaturer och för att kunna kontrollera dessa på ett tillförlitligt sätt m.m.

7 § Signaturnyckelcertifikats innehåll

Signaturnyckelcertifikatet *måste* innehålla följande uppgifter. Innehavarens namn (pseudonym), öppen signaturnyckel, algoritmer för användning av signaturnyckelinnehavarens öppna nyckel och certifieringsorganets öppna nyckel, certifikatets löpnummer, certifikatets giltighetstid, certifieringsorganets namn samt uppgift om signaturnyckelns användning är begränsad till viss användning. Därutöver *får* uppgifter om behörighet att företräda tredje person samt vissa andra uppgifter tas in i certifikatet. Ytterligare uppgifter får tas in i certifikatet endast med den berördes samtycke.

8 § Spärrning av certifikat

Certifieringsorganet skall spärra ett certifikat *om* nyckelinnehavaren begär det, *om* certifikatet förverkats, *om* giltighetstiden löpt ut *eller om* den behöriga myndigheten spärrat certifikatet. I ett beslut om spärrning, som inte får göras retroaktivt, skall anges den tidpunkt då beslutet träder i kraft.

Tredje person är behörig att begära att ett certifikat spärras om det innehåller uppgifter om denne.

Om ett certifieringsorgan får sin licens återkallad eller eljest upphör med sin verksamhet är det den behöriga myndigheten som förordnar om spärrning av certifikat.

9 § Tidsstämpel

På begäran skall certifieringsorganet förse digitala data med en tidsstämpel.

10 § Dokumentation

Här regleras certifieringsorganets skyldighet att dokumentera de säkerhetsåtgärder som vidtas. Även de utställda certifikaten skall dokumenteras. Detta sker för att data skall kunna kontrolleras till sitt innehåll och för att förhindra att de förfalskas.

11 § Verksamhetens upphörande

Den behöriga myndigheten skall omgående underättas om ett certifieringsorgan upphör med sin verksamhet. Ännu giltiga certifikat skall antingen övertas av annat certifieringsorgan eller spärras. Dokumentationen skall överlämnas till det övertagande certifieringsorganet eller i annat fall till den behöriga myndigheten.

Den behöriga myndigheten skall även omgående underrättas om ett certifieringsorgan blir föremål för en ansökan om konkurs- eller ackordsförfarande.

12 § Dataskydd

Införskaffande av personuppgifter kräver samtycke från berörd person. Uppgifter om den som använder sig av pseudonym, får lämnas ut till myndigheter endast för vissa särskilt angivna syften. Har så skett skall nyckelinnehavaren underrättas.

13 § Kontroll

För att säkerställa lagens och förordningens efterlevnad har den behöriga myndigheten utrustats med vissa maktbefogenheter gentemot certifieringsorganen. Den får förbjuda att olämpliga tekniska komponenter används. Den kan också, helt eller delvis, interimistiskt förbjuda att ett certifieringsorgan bedriver tillståndspliktig verksamhet.

Myndigheten ges rätt att inspektera certifieringsorganets lokaler. Certifieringsorganet är också skyldig att på begäran lämna ut uppgifter i viss utsträckning till myndigheten.

Licens skall återkallas *om* certifieringsorganet eftersätter sina skyldigheter enligt lagen eller förordningen, *om* det framkommer sådana omständigheter som skulle ha utgjort grund för att vägra licenstilldelning *eller om* certifieringsorganet inte rättar sig efter sådana beslut som avses i första stycket ovan.

Om en licens återkallas eller om ett certifieringsorgan eljest upphör med sin verksamhet, skall myndigheten se till att verksamheten antingen övertas av ett annat certifieringsorgan eller att avtalen med nyckelinnehavarna sägs upp. Detsamma gäller vid en konkursansökan eller vid ett ackord om verksamheten därmed upphör.

Giltigheten av utfärdade certifikat berörs inte av att en licens återkallas. När det pga. omständigheterna finns skäl anta *att* ett certifikat är förfalskat, *att* ett certifikat inte är tillräckligt säkert mot förfalskningar eller *att* de tekniska komponenterna som ingår i certifikatet är bristfälliga ur säkerhetssynpunkt, kan den behöriga myndigheten spärra certifikatet.

14 § Tekniska komponenter

Vid tillverkning och lagring av signaturnycklar samt vid tillverkning och kontroll av digitala signaturer skall sådana tekniska komponenter och säkerhetsåtgärder användas, som på ett tillförlitligt sätt kan påvisa förfalskningar av digitala signaturer och signerade

data. De tekniska komponenterna skall vara så beskaffade att de skyddar mot obehörig användning av privata nycklar.

För framställning av data som skall signeras, krävs tekniska komponenter och säkerhetsåtgärder som på förhand klart anger att en digital signatur tillverkas samt gör det möjligt att fastslå till vilken datamängd den digitala signaturen hänför sig. För granskning av signerade data krävs tekniska komponenter och säkerhetsåtgärder, som gör det möjligt att konstatera huruvida signerade data är oförändrade, till vilken datamängd den digitala signaturen hänför sig och till vilken nyckelinnehavare den digitala signaturen hör.

För tekniska komponenter, med vars hjälp nyckelcertifikat skall kunna kontrolleras eller återkallas, krävs åtgärder som skyddar certifikatförteckningarna från obehörig ändring eller återkallelse.[60]

De tekniska komponenterna skall vara kontrollerade i erforderlig omfattning. Ett av den behöriga myndigheten godkänt organ skall intyga att de tekniska komponenterna uppfyller kraven.

Tekniska komponenter, som har framställts eller placerats på marknaden i enlighet med de regler eller krav som gäller i en annan medlemsstat inom EU (eller i ett EES-land) och som uppfyller motsvarande säkerhet som stipuleras i lagen, skall anses uppfylla kraven på säkerhetsmässiga egenskaper. När skäl därtill föreligger kan den behöriga myndigheten i enskilda fall kräva att bevisning företes till styrkande av att överensstämmelse med kraven föreligger. Intyg från godkända organ i andra medlemsstater (även EES-stater) äger värde som bevis om att kraven är uppfyllda, förutsatt att organet befinns likvärdigt med inhemska organ som är godkända.

15 § Utländska certifikat

Digitala signaturer som kan kontrolleras med en öppen signaturnyckel för vilken det finns ett utländskt certifikat, som utfärdats i någon annan medlemsstat inom EU (eller i ett EES-land), jämställs med digitala signaturer enligt lagen under förutsättning att

[60] Den tyska originaltexten talar om ”Abruf”.

de uppvisar likvärdig säkerhet. Motsvarande gäller även för digitala signaturer utfärdade i andra stater, om överstatliga eller mellanstatliga avtal om ömsesidigt erkännande av certifikat har träffats.

7.2.7 Danmark

Danmarks IT-säkerhetspolitik

Under år 1995 tillsatte regeringen i Danmark ett IT-säkerhetsråd med uppgift att lämna regeringen råd i IT-säkerhetsfrågor och formulera ett upplägg för en dansk politik för IT-säkerhet. IT-säkerhetsrådet har formulerat sina förslag m.m. i publikationen ”Danmarks IT-sikkerhedspolitik – et oplæg”[61].

Redan år 1991 tillsatte danska Telestyrelsen en arbetsgrupp för att utreda ett eventuellt myndighetsinitiativ på krypteringsområdet. Avsikten var att belysa vilka konsekvenser en reglering av nyckelcentraler kunde få med avseende på en rad juridiska problemställningar. Arbetsgruppen utarbetade en rapport, i vilken de funktioner angavs som kunde ingå i en krypteringstjänst. Vidare redovisades på vilket sätt funktionerna kunde dokumenteras vara uppfyllda, bl.a. med hänsyn till kvalitetssäkring. Arbetsgruppen fann det bäst att branschen själv utformar dessa kvalitetskrav, varför gruppen inte föreslog någon lagstiftning på området.

IT-säkerhetsrådet fann emellertid i sitt arbete att det förekom anledning att på nytt ta upp frågan om behovet av en reglering. Man bedömde en möjlig handlingsväg vara att ta ett lagstiftningsinitiativ på krypteringsområdet. Detta för att säkra ett rättsligt erkännande av dokumentation som överförs genom kryptering. Rådet ansåg emellertid att det förelåg skäl att i stället föreslå regler om hur rättighetsgrundande TTP-verksamheter skall vara inrättade för att uppnå högsta möjliga säkerhet, vilket skulle kräva en belysning av de skiftande säkerhetskraven inom varje särskilt tillämpningsområde. Rådet konstaterade vidare att särskilda förhållanden

[61] Forskningsministeriet, nov 1996, http://www.fsk.dk

gör sig gällande i EDI-förhållanden, som sker *inter partes*. Särskilda förhållanden ansågs också föreligga beträffande s.k. innehavarpapper, dvs. originaldokument som är bärare av en rättighet.

Rådet fann att det beträffande digitala signaturer föreligger ett behov av klara regler som talar om när en framtagning av hashvärden eller kryptering av ett dokument skall anses vara ett uttryck för avsändarens vilja att bli bunden av innehållet i dokumentet. Det borde enligt rådets uppfattning finnas generella regler som anger när en digital signatur kan jämställas med en vanlig underskrift. Däremot kunde det enligt rådet diskuteras om staten bör vara den som driver, understödjer eller kontrollerar TTP-verksamhet med avseende på säkerhetslösningar baserade på öppen-nyckel-kryptering. Regler om digitala signaturer borde kunna införas oavsett om det offentliga står bakom nyckelcentralerna. Det fordras endast att rättsreglerna anger hur en nyckelcentral eller en CA skall uppträda för att signaturen skall ges vissa rättsverkningar. Telestyrelsen, som tidigare haft frågan uppe, hade hänvisat till de regler om teknisk kontroll och kontroll av laboratorier m.m. som finns i Danmark. De nämnda bestämmelserna tog enligt rådet emellertid inte särskilt sikte på de uppgifter som en CA skall utföra. Rådet ansåg att uppgifter som sammanhänger med att identifiera en person borde skötas av samhället. Detta skulle minska risken för att felaktiga certifikat utfärdas. Ett ytterligare argument för att ha en offentlig myndighet som central CA för personidentifiering ansågs vara en lägre skadeståndsrisk. I de fall säkerhetssystemet skulle komma att användas för dispositioner av mycket stor ekonomisk omfattning skulle det kunna tänkas att många privata verksamheter avskräcktes från att ta på sig rollen som nyckelcentraler.

I förslaget om införandet av ett ”borgerkort” var tanken att det centrala personregistret i Danmark skulle föra ett register över kortinnehavare och agera som central CA för identifiering av enskilda personer. Tanken med förslaget var aldrig att utesluta andra intressenter från att bedriva motsvarande verksamhet. För att andra än det centrala personregistret skall kunna bedriva verksamhet med identifiering av enskilda personer med motsvarande rättsverkan som

”borgerkortet”, ansåg rådet detta dock kräva någon form av kontroll.

Beträffande nyckelcentralerna vore det enligt rådet tillräckligt om det offentliga utövade tillsyn över sådana privata verksamheter som handhar nyckelhanteringen i ”borgerkort-projektet”. Samma sak ansågs gälla för CA-funktioner utöver den CA-funktion som var avsedd att finnas i projektet.

Beträffande den offentliga kontrollen av nyckelcentralernas verksamhet anförde rådet att fråga uppkommit om inte det allmänna borde stödja utvecklingen av en öppen-nyckel-infrastruktur. Detta genom att som villkor för att vissa rättsverkningar skall uppkomma, ställa bestämda krav på den använda teknologin. Rådet konstaterade att en rad myndigheter av praktiska skäl redan börjat att godta användningen av digitala meddelanden och detta även i fall där det finns uttryckliga krav på skriftlighet. Rådet menade dock att det kan vara förbundet med en viss osäkerhet om rättsutvecklingen på detta sätt styrs av praxis.

Rådet kom till slutsaten att Danmark, med beaktande av det internationella arbetet på området inom EU och FN, så fort som möjligt borde förbereda en lagstiftning som, med undantag för innehavarpapper, fastställer vilka procedurer en nyckelcentral eller en CA bör följa för att åstadkomma samma giltighet för elektroniska dokument som hittills har kunnat erhållas genom bruk av pappersdokument och underskrift.

Rapport till Folketinget om säker digital kommunikation

Ministrarna från fem departement inom regeringskansliet avlämnade i december 1997 en rapport ”Sikker digital kommunikation”[62] till Folketinget med en rad initiativ som regeringen avser att ta för att främja digital kommunikation. Rapporten kan ses som ett danskt svar på EU-kommissionens meddelande ”Om säkerhet och pålitlighet vid elektronisk kommunikation – Mot en europeisk ram för kryptering och digitala signaturer”. Rapporten är avsedd att

[62] http://www.fsk.dk/fsk/div/digkomrd.html

åtföljas av flera lagstiftningsintitiativ. Ett lagförslag om digitala signaturer kommer att presenteras under första halvåret 1998.

I rapporten anges regeringens målsättning vara att realisera ett principiellt jämställande av digital och pappersbaserad kommunikation. Man vill göra det möjligt att kunna använda digital kommunikation på alla områden där denna kommunikationsform kan uppfylla samma funktioner som pappersdokumentet.

Användningen av elektronisk kommunikation för bindande juridiska transaktioner förutsätter enligt rapporten säkra tekniska lösningar och en säker nyckelhantering. Regeringen avser därför att ta initiativ till en lagstiftning av nyckelcentralernas verksamhet. Detta vill man realisera genom att införa ett auktoriseringsförfarande och en rad minimikrav för den digitala signaturens utformning, säkerhetsnivå m.m. för att på så sätt främja utbudet av lösningar med tillräcklig kvalitet.

I rapporten konstateras vidare att det kan uppstå en rättslig osäkerhet vid införande av ny teknik. Detta med hänsyn till möjligheten att använda digital kommunikation och digitala signaturer för juridiskt bindande dispositioner. På en rad områden i dansk rätt föreligger inte några formkrav, t.ex. vid ingående av avtal. Avgörandet för en digital signaturs bevisverkan ligger i sista hand hos domstolarna. Domstolarna har att tillämpa fri bevisprövning. Med en ramlagstiftning om digitala signaturer kan det emellertid förväntas att en digital signatur – som framställs i överensstämmelse med lagens krav – tillerkänns ett högre bevisvärde än den annars skulle få.

I rapporten ifrågasätts vidare om domstolarna utan vidare skulle acceptera digitala signaturer på områden där det finns uttryckliga krav i lagstiftningen på underskrift och skriftlighet m.m. Denna osäkerhet anser man inte vara tillfredsställande med hänsyn till de samhällsekonomiska fördelarna som följer av att främja elektronisk kommunikation. Det bör därför genom lagstiftning fastslås på vilka områden, i vilken omfattning och på vilket sätt digital kommunikation med digital signatur kan användas när det föreligger formkrav om underskrift och skriftlighet.

En reglering kan enligt rapporten ske på två sätt.

- I ”frameldingsmodellen” är utgångspunkten att det i den kommande lagstiftningen om digital signatur ingår en bestämmelse om att krav på skriftlighet och underskrift i lagstiftningen inte utgör hinder för att använda digitala meddelanden med digital signatur. Detta bör kombineras med en bestämmelse om att kunna undanta särskilda lagar eller förordningar från huvudregeln.

- Vid ”tilmeldingsmodellen” är utgångspunkten den motsatta, dvs. det införs inte någon generell reglering av möjligheterna att använda digital signatur på områden där det finns formkrav. Det får i stället regleras inom de särskilda rättsområdena om digital signatur kan användas när formkrav föreligger.

Forskningsministeriets initiativ till en lagstiftning om digitala signaturer är fogad som bilaga till rapporten. Förslagets huvuddrag beskrivs i det följande.

- Genom lagstiftning inrättas ett auktoriseringsförfarande för nyckelcentralernas organisation och verksamhet. Auktorisationen är frivillig och erhålls efter ansökan. En offentlig tillsynsfunktion inrättas för att övervaka efterlevnaden av de krav som fastställs för erhållande av auktorisation.

- Rättsverkningarna av digitala signaturer skall regleras enligt ”frameldingsmodellen” eller ”tilmeldingsmodellen”.

- Nyckelcentralen är i förhållande till såväl signaturinnehavaren som signaturmottagaren ansvarig för förluster som följer av fel som förorsakats av att nyckelcentralen inte har efterkommit föreskrifter om hur digitala signaturer skall åstadkommas eller utformas. Detsamma gäller om nyckelcentralen har brustit i sin skyldighet att upplysa signaturmottagaren om giltigheten av en digital signatur m.m. Ett objektivt ansvar föreslås för nyckelcentralerna. Om användaren själv har varit försumlig bör nyck-

elcentralen ges möjlighet att föra bevisning om att det uppkomna felet är förorsakat av användarens försumlighet.

- Där särskilda ansvarsregler saknas skall allmänna skadeståndsrättsliga regler gälla.

- Om någon förlorar sin privata signaturnyckel måste möjligheten att få signaturen bekräftad hos nyckelcentralen spärras så fort som möjligt. Det ankommer därför på signaturinnehavaren vid förlust av nyckel att kontakta nyckelcentralen som sätter in en spärrningsnotering i telefonkatalogen. På så vis kan mottagaren, vid försök att få signaturen bekräftad, se att signaturen är spärrad. När en signatur är spärrad presumeras mottagaren vara i ond tro. För att häva denna presumtion måste mottagaren visa att han kontrollerat att nyckeln inte varit spärrad. Nyckelcentralen övertar ansvaret för förluster som förorsakas mottagaren om nyckelcentralen inte spärrar certifikatet på användarens uppmaning.
- Ansvars- och straffrågor vid förfalskning och liknande, får avgöras enligt reglerna om straff- och skadeståndsansvar för sådana brott.

- Nyckelcentralen är skyldig att ange när en digital signatur upphör att gälla. Uppgiften måste även finnas tillgänglig i samband med att signaturmottagaren bekräftar en mottagen signatur. Effekten blir att digitala meddelanden som åsatts en digital signatur inte har samma bevisvärde när tiden för signaturnyckelns giltighet väl har överskridits.

- Användningsområdet för en digital signatur skall kunna begränsas. Sådana begränsningar kan tas in i certifikatet som finns i nyckelcentralernas telefonkatalog. Om ett meddelande faller utanför användningsområdet kommer det i praxis att vara en presumtion för att signaturen obehörigen har använts av tredje man. För att inte dessa begränsningar skall bli alltför svåra att hantera, överväger man att begränsa antalet möjliga kategorier

av inskränkningar som användaren och nyckelcentralen kan välja. Några exempel på sådana kategorier kan vara: kommunikation med det offentliga, familjerättsliga dispositioner, elektronisk handel samt handel med fast egendom.

– Slutligen ankommer det på myndigheter i allmänhet att inrätta sin verksamhet så att medborgare som så önskar skall kunna kommunicera digitalt med myndigheten. Detta gäller även för sådana fall där det fordras bindande rättshandlingar i någon form från medborgarens sida.

7.2.8 Finland

I skrivande stund föreligger förslag enligt vilket den finländska regeringen i början av februari 1998 skall fatta ett principbeslut att vidta förberedelser för användande av elektroniska dokument och elektroniska signaturer i den offentliga förvaltningen[63]. Ministerierna och ämbetsverken skall se till att uppgifter om de viktigaste tjänsterna avsedda för medborgarna, företag och sammanslutningar samt nödvändiga blanketter finns tillgängliga på datanät så att en stor del av ansökningar och framställanden kan meddelas också via sådana nät före år 2001. Myndigheterna skall utveckla de elektroniska dokument och tjänster för att uträtta ärenden som behövs samt ett gemensamt serviceutbud.

Ärenden i den offentliga förvaltningen skall kunna uträttas elektroniskt. Justitieministeriet och de övriga ministerierna skall bereda den lagstiftning som krävs för uträttande av ärenden, elektroniska dokument och elektronisk signatur samt identitetskort och certifieringsmyndighetstjänster före den 30 juni 1999. Befolkningsregistercentralen utses till statlig certifieringsmyndighet med ansvar för utfärdande och upprätthållande av elektroniskt identitetskort samt för att annan behövlig certifieringsorganisation och certifieringstjänster skapas.

[63] Källa: Matti Pulkkinen, Finansministeriet, Finland.

Ett avgiftsbelagt identitetskort avsett för alla medborgare skall tillverkas och tas i bruk under år 1999. Kortet är ett medel för elektronisk autenticering av person och signatur. Före utgången av 1998 skall en registertjänst skapas för den offentliga förvaltningen, med e-postadresser och annan kontaktinformation som behövs för samarbetet mellan EU-länderna och för nationella behov.

Finansministeriet och Inrikesministeriet skall ansvara för verkställandet och uppföljningen av beslutet. Tillsammans med andra myndigheter skall de meddela anvisningar och rekommendationer i dessa frågor.

7.2.9 USA

Elektroniska och digitala signaturer

I den amerikanska lagstiftningen används – mer eller mindre konsekvent – begreppen elektroniska signaturer och digitala signaturer. Den mer generella termen elektronisk signatur definieras vanligen som alla enheter såsom bokstäver, tecken och symboler som kommit till uttryck på elektroniskt eller liknande vis och som utförts eller antagits av en part i en transaktion med syftet att autenticera ett meddelande. Ett meddelande är elektroniskt signerat om en elektronisk signatur är logiskt associerad med meddelandet[64]. I princip alla delstater som använder begreppet elektronisk signatur kräver att vald teknisk lösning skall generera en signatur som (A) är unik för den person som begagnar den, (B) kan verifieras, (C) är under användarens enskilda kontroll, (D) är knuten till en datamängd på ett sådant sätt att signaturen ogiltigförklaras om

[64] Jfr Floridas ”Electronic Signature Act”; 1996 Florida Senate Bill 942: ”'Electronic signature' means any letters, characters, or symbols, manifested by electronic or similar means, executed or adopted by a party with an intent to authenticate a writing. A writing is electronically signed if an electronic signature is logically associated with such writing.”, http://www.scri.fsu.edu/fla-leg/bills/senate-1996/sb0942.html

datamängden förändrats och (E) uppfyller de föreskrifter en tillsynsmyndighet kan komma att uppställa[65].

En digital signatur är en delmängd inom de elektroniska signaturerna. Den definieras genom att den begagnar en informationssäkerhetsåtgärd (”information security measure”), vanligen kryptografi, som avser att säkerställa att ett meddelande är oförvanskat och att det verkligen härrör från angiven utgivare[66]. Det teknikneutrala uttrycket ”elektronisk autenticering” används ofta i sammanhanget.

Federal lagstiftning

Det primära ansvaret för civilrättslig lagstiftning i USA vilar på delstaterna. Den federala myndigheten har dock ett betydande handlingsutrymme på det civilrättsliga området. Ingen federal lagstiftning om generell giltighet av digitala signaturer har i dagsläget antagits[67]. I en av Representanthuset anordnad ”hearing”[68] den 28 oktober 1997 om digitala signaturer uppmanades Kongressen av

[65]Thomas J. Smedinghoff, ”Analyzing State Digital Signature Legislation”, augusti 1997, http://www.mbc.com/ds_rev.html

[66] En skolbildande definition av digitala signaturer återfinns i Utah Digital Signature Act,Utah Code § 45-3-103(10):
”Digital signature” means a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine whether:
(a) the transformation was created using the private key that corresponds to the signer's public key; and
the message has been altered since the transformation was made.

[67] Det amerikanska livs- och läkemedelsverket (Food and Drug Administration) har antagit föreskrifter som, under vissa förutsättningar, jämställer digitala signaturer och elektroniska papperbundna dok ument. http://www.fda.gov/cder/esig/part11.htm

[68] United States House of Representatives Committee on Science, Subcommittee on Technology hearing entitled ”Do You Know Who You Are Doing Business With? Signatures In A Digital Age”, 97-10-28, http://www.house.gov/science/pressrel/105-142.htm

Clintonadministrationens representant att avvakta med lagstiftningsåtgärder till dess frågeställningarna hunnit bli bättre utredda[69].

Två lagstiftningsärenden har emellertid initierats av enskilda representantshusledamöter; H.R. 2937 ”Electronic Financial Services Efficiency Act” (EFSA) och H.R. 2991 ”Electronic Commerce Enhancement Act” (ECEA), båda väckta under november 1997.[70]

I det förra lagförslaget (EFSA) föreslås att elektronisk autenticering eller digitala signaturer, under vissa förutsättningar, skall ha samma rättsverkan som pappersbundna handtecknade underskrifter. Förslaget förhåller sig teknikneutralt till vilka typer av elektronisk autenticering som skall accepteras. Varje metod är godkänd som möjliggör att man *dels* på ett tillförlitligt och verifierbart sätt kan identifiera upphovsmannen eller avsändaren av ett dokument eller annat meddelande, *dels* på ett tillförlitligt sätt kan fastställa att dokumentet eller meddelandet inte har förvanskats. I EFSA föreslås vidare att ett ”National Association of Certification Authorities” inrättas, som skall stå under tillsyn av det federala finansdepartementet. Envar som tillhandahåller elektroniska autenticeringstjänster i USA skall registreras/licensieras av detta organ. Licensieringsmyndigheten skall vidare förordna en kommitté för tillsyn av standarder för elektronisk autenticering. Kommittén har till uppgift att uppställa, formulera och vidareutveckla kriterier som skall appliceras på den framväxande elektroniska autenticeringsbranschen. Lagförslaget, som har remitterats till ett flertal utskott, har mött kritik bl.a. för att det inte adresserar frågan om de ofta kontradiktoriska delstatsregleringarna[71].

I det senare lagförslaget (ECEA) föreslås åtgärder för att möjliggöra en säker digital kommunikation med och betalning till de federala myndigheterna och deras organ. Alla federala blanketter och formulär föreslås kunna tillhandahållas och tas emot i elektro-

[69] http://www.news.com/News/Item/0,4,15788,00.html

[70] Lagförslagen finns tillgängliga bl.a. på det amerikanska Kongressbibliotekets databas http://thomas.loc.gov

[71] Stewart Baker och Michael D. Hintze, ”H.R. 2937: The Electronic Financial Services Efficiency Act of 1997”, http://www.steptoe.com/hr2937.htm

nisk form med begagnande av digitala signaturer. Officiella underrättelser skall på begäran kunna sändas ut elektroniskt. Närmare riktlinjer för hur certifikatet för en digital signatur skall vara beskaffat för att accepteras av myndigheterna föreslås utfärdas av Kongressens organ ”Office of Management and Budget”. Härvid uppställs kravet att certifikatet måste vara utställt av en offentlig myndighet eller licensierad TTP. Lagförslaget har remitterats till ett flertal utskott.

Delstatlig lagstiftning [72]

Cirka 40 delstater har antagit eller lagt fram förslag till lagstiftning om elektronisk autenticering. Vanligast är lagstiftning av begränsad räckvidd, som godkänner elektronisk autenticering endast i kommunikation med offentligrättsliga organ eller vårdinstitutioner. I september 1997 hade 28 delstater lagt fram 48 lagförslag med begränsad räckvidd. Av dessa hade 23 delstater antagit 36 sådana lagar. Nära samtliga av dessa hade valt modellen elektronisk signatur.

21 delstater hade vid samma tid lagt fram 31 lagförslag av mer generell räckvidd beträffande kommunikation inom såväl den privata som offentliga sektorn. Av dessa hade 10 delstater antagit 13 sådana lagar. De flesta delstater som antagit lagstiftning av generell räckvidd har valt modellen digital signatur, men bilden förvirras av att vissa delstater använder sig av begreppet digital signatur trots att det framgår av lagtexten att vad som avses motsvarar elektronisk signatur medan andra helt undviker att definiera innehållet i det begrepp man valt att använda[73]. Vidare har flera delstater lagstiftat om såväl elektroniska som digitala signaturer.

[72] Primärkälla till detta avsnitt är ”Survey of Electronic and Digital Signature Legislative Initiatives in the United States”, utgiven av The Internet Law & Policy Forum. Rapporten kan hämtas från http://www.ilpf.org/digsig/digrep.htm. För ytterligare information http://www.mbc.com/ds_sum.html

[73] Smedinghoff, a.a.

De delstatliga initiativen kan i de flesta fall föras in under en av följande tre regleringskategorier: föreskriftsinriktad, kriteriebaserad eller minimalistisk reglering.[74]

Föreskriftsinriktad reglering

Modeller inom den *föreskriftsinriktade* regleringskategorin bygger på att underlätta elektronisk handel genom ett detaljerat regelverk av lagar och föreskrifter. I korthet innefattar kategorin ett (frivilligt) licensieringsförfarande inom ramen för en öppen-nyckel-infrastruktur, en fördelning av skyldigheter mellan kontraktsslutande parter, en reglerad ansvarsfördelning, bevispresumtioner samt standarder för signatur och dokumentautenticering.

Den mest kända – om än inte den mest spridda – modellen inom denna kategori är *Utah/Guidelines-modellen*. Delstaten Utah antog först i världen en lag som syftar till att främja elektronisk handel med hjälp av digitala signaturer. Lagen arbetades fram i samarbete med en kommitté inom det amerikanska advokatsamfundet (ABA) som, parallellt med utredningen, sammanställde och publicerade en slags modellag med kommentarer för digitala signaturer, ”Digital Signature Guidelines”.[75]

Utah/Guidelines har kommit att utöva ett stort inflytande på annan delstatlig lagstiftning om elektronisk autenticering. Modellen bygger på att särskilda organ (CA) utfärdar certifikat som knyter viss person till en öppen nyckel. CA kan erhålla licens från en delstatsmyndighet. Licensiering är frivillig, men nödvändig för att en digital signatur med certifikat från CA skall omfattas av lagen. Några utmärkande drag för *Utah/Guidelines-modellen* är följande.

[74] I den amerikanska terminologin används begreppen: prescriptive, criteria-based och signature-enabling approaches.

[75] American Bar Association, Section of Science and Technology, Electronic Commerce Division, Information Security Committee, ”Digital Signature Guidelines”, Chicago 1996, http://www.abanet.org/scitech/ec/isc/dsgfree.html

- Delstaten utser en myndighet som utfärdar föreskrifter till lagen, licensierar CA och utövar tillsyn över dessa.

- Tillsynsmyndigheten kan godkänna CA som licensierats utanför delstaten, förutsatt att licensieringen skett mot kriterier som är likvärdiga med den inhemska regleringen.

- Licensierad CA åtnjuter lagstadgade ansvarsbegränsningar; beloppsbegränsningen framgår av det utställda certifikatet.

- CA måste ställa säkerhet för sin verksamhet och kan bli föremål för revision.

- Digitala signaturer, som utfärdats av licensierad CA, uppfyller formkraven för undertecknande *om* den kan verifieras med en öppen nyckel från CA:ns katalog, *om* signaturen har tillfogats meddelandet i avsikt att underteckna det *samt om* mottagaren saknar vetskap om eventuell missbruk av signeringsnyckeln.

- I en rättstvist rörande digitala signaturer skall domstolen presumera *att* användaren av signaturen är den person som utpekas som innehavare i certifikatet, *att* denne anbringat signaturen på ett meddelande i avsikt att underteckna det *samt att* mottagaren av det signerade meddelandet varit i god tro om avsändarens rätt att inneha signeringsnyckeln.

- Innehavaren av en signeringsnyckel åläggs aktsamhetskrav vad avser kontroll över nyckeln.

Av de 14 delstater som lagt fram lagförslag enligt Utah/Guidelines-modellen har endast 3 genomfört förslagen. Skälet till detta uppges vara att modellen upplevs som alltför teknikbunden till öppen-nyckel-infrastrukturen och verkar därigenom begränsande för alternativa lösningar.

Kriteriebaserad reglering

Inom den *kriteriebaserade* kategorin är den s.k. *California-modellen* ledande. Lagtexten hålls typiskt sett mycket kort. Föreskrifter och rättspraxis skall fylla ut resten. För att elektronisk autenticering skall anses uppfylla lagstadgade krav på undertecknande, förutsätts enligt modellen att vissa kriterier är uppfyllda. Kraven motsvarar dem som angivits i inledning till detta avsnitt (A)–(E)[76]. Syftet med denna modell är att vinna största möjliga flexibilitet i en tid av snabb teknologisk utveckling. I t.ex. Kalifornien uppfyller, enligt de föreslagna föreskrifterna till lagen, två olika teknologier säkerhetskraven; digitala signaturer enligt öppennyckel-infrastruktur samt ett system betecknat ”Signature Dynamics”. Det senare bygger på en biometrisk teknik där de rörelser som genereras vid en namnteckning med en penna eller motsvarande digitaliseras och knyts till ett dokument med hjälp av kryptografi. Signaturen kan sedan verifieras genom jämförelse med ett deponerat skriftprov. Systemet avses fungera utan CA.[77] I Kalifornien har lagstiftningen begränsats till att endast omfatta kommunikationer med offentligrättsliga organ. Av de 14 delstater som antagit eller behandlar lagförslag enligt California-modellen, har åtta begränsat räckvidden på liknande sätt, medan sex ansett modellen förenlig med en generell räckvidd.

[76] Jfr California Government Code Section 16.5
http://www.ss.ca.gov/digsig/code165.htm
[77] Jfr ”Final Draft of California Digital Signature Regulations”, California Administrative Code, Title 2. Administration, Division 7. Secretary of State, Chapter 10. Digital Signatures. (http://www.ss.ca.gov/digsig/finalregs.htm)

Minimalistisk reglering

Med en *minimalistisk* inriktning anses i princip *varje* elektroniskt märke eller tecken, som åsatts ett meddelande i avsikt att autenticera det, uppfylla formkraven på skriftlighet och undertecknande. Meddelandet anses undertecknat om den elektroniska signaturen är knuten till det.[78] Modellen är minimalistisk i sin omfattning; lagarna ställer inte upp standarder för CA eller regler om ansvarsbegränsningar, bevispresumtioner eller godkännande av signaturer från andra delstater. Valet av tillvägagångssätt har valts i syfte att snabbt undanröja osäkerhet om formkrav. Lagstiftningen följs i många fall upp senare med kompletterande föreskrifter m.m.

22 delstater har och ytterligare fem delstater överväger lagstiftning som faller inom denna kategori. Av de delstater som redan infört lagstiftningen, har alla utom fem begränsat signaturlagarnas räckvidd.[79]

Hybridmodeller

Delstaten Illinois har utfärdat ett nytt lagförslag[80], som lånat drag från såväl *Utah/Guidelines* som *California-modellen*. Förslaget är vidare influerat av modellagarna från *NCCUSL* (se nedan) samt *UNCITRAL*. I lagförslaget föreslås elektroniska dokument och signaturer, med vissa undantag, uppfylla formkraven på skriftlighet och undertecknande. Detta gäller dock inte när det är uppenbart att huvudregeln är oförenlig med annan lagstiftning. Undantag från

[78] Jfr Floridas ”Electronic Signature Act” Section 4 (4).
[79] Delstater som har en minimaltistisk reglering av generell räckvidd är Florida, New Hampshire, Oregon, Texas och Virginia.
[80] Illinois Electronic Commerce Security Act, Illinois Attorney General’s Commission on Electronic Commerce and Crime, draft December 15, 1997. Förslaget med utförlig kommentar kan hämtas från http://www.mbc.com/ceccmsg.html

huvudregeln görs även för lagar om testamente och stiftelser, för vissa fullmakter av privat karaktär samt värdepapper.[81]

I det aktuella lagförslaget föreslås vidare en kvalificerad form av signaturer, s.k. säkra elektroniska signaturer. Elektroniska signaturer klassas som säkra om de skapats med en i lagen eller tillhörande föreskrift godkänd säkerhetsteknologi, eller med en mellan parterna överenskommen teknologi. En ”säker” signatur presumeras härröra från utpekat utställare och ha anbringats i syfte att underteckna dokumentet.

NCCUSL

Det amerikanska institutet ”National Conference of Commissioners on Uniform State Laws” (NCCUSL), verkar sedan 1800-talets slut för att främja en enhetlighet mellan delstaternas olika lagstiftningar. Organisationen bedriver sitt arbete bl.a. genom att utarbeta modellagar. Man har även lagt fram ett utkast till lagstiftning om elektronisk autenticering[82], ”Uniform Electronic Transactions Act”. Detta utkast är alltjämt under uppdatering. Det anger i sina kommentarer att delar av förslaget har påverkats av Illinois-förslaget samt UNCITRAL:s modellag.

7.3 Behov av regler för digitala signaturer och deras rättsverkan

För att möjliggöra regelmässigt bruk av det allmänt tillgängliga telenätet för transport av telemeddelanden under säkra former med användning av digitala signaturer krävs normer som medför säkerhet. Sådana normer kan åstadkommas på flera sätt. Ett är lagstift-

[81] ECSA Sec. 202 och 203
[82] Uniform Electronic Transactions Act. Senaste utkastet publicerat 25 november 1997, Förslaget finns tillgängligt på http://www.law.upenn.edu/library/ulc/uecicta/eta1197.htm

ning med åtföljande statlig regelgivning genom sekundär författningsgivning eller tillståndskrav. Ett annat är marknadsbestämda regler, som med utgångspunkt från gängse lagstiftning om avtal, skadestånd och annat ansvar, bildas genom olika former av avtal mellan parterna. Den förra metoden torde snabbare ge tydliga spelregler men kan samtidigt innebära ett hinder för teknisk utveckling och upplevas som mer byråkratisk. Den senare är sannolikt mer flexibel men viktiga tolkningsfrågor får överlämnas till praxis och torde komma att vara olösta under en längre tid. En lämplig blandning av de båda metoderna kan vara att föredra för att ge rättsområdet erforderlig stadga, samtidigt som utvecklingen inte onödigtvis hämmas.

7.3.1 Pappersdokument – elektroniska dokument

Datastraffrättsutredningen (SOU 1992:110) har ingående beskrivit skillnaden mellan traditionell och elektronisk hantering av handlingar. Nedan återges utredningens redovisning av de grundläggande skillnaderna mellan det elektroniska och det pappersbaserade dokumentet.

Materiell sak – kvasimateriellt objekt: Pappersurkunderna är materiella objekt (saker), medan digitalt representerade uppgifter inte med vanligt språkbruk kan beskrivas som materiella **o**bjekt.

Självständig existens: Pappersurkunden bevarar text och utställarangivelse skilda från andra saker, medan relationerna mellan text, utställare och bärare inte är lika entydiga och låsta i IT-miljön.

Varaktig existens: Pappersurkunden låser fysiskt och varaktigt föreställningsinnehållet på ett enda sätt, medan IT-rutinerna är utformade så att lagrade uppgifter kan representeras av data i bearbetnings- och överföringsfaser av så tillfällig karaktär att objektet knappast kan anses varaktigt i vanlig mening.

Unik existens: Pappersurkunden upprättas så att det föreligger ett i princip unikt fysiskt exemplar, originalet, medan informationsteknik bygger på lagringar och överföringar av ett originalinnehåll.

Individuell karaktär: Pappersurkunden har en större eller mindre grad av fysisk särprägel, t.ex. i form av en underskrift, medan det vid IT-lagring inte finns andra unika egenskaper än sådana som knyts till mönstren av ettor och nollor, t.ex. genom kryptering.

Tillgänglighet: Pappersurkunderna är direkt läsbara medan en digital materialisering måste överföras från maskinspråk till läsbar form.

Representationsform: Pappersurkunden har skriften som enhetlig representationsform, medan de digitala materialiseringarna har ett flertal representationsformer, dels olika tekniska lösningar för representationen i lagrad form (elektroniskt, optiskt etc.), dels för läsbar form (t.ex. bildskärmsvisning, utskrift och röstsimulering).

Intern och extern manipulerbarhet, sårbarhet och spårlöshet: Manipulationer med pappersurkunder förutsätter ett materiellt angrepp som är möjligt att spåra på urkunden, medan en ändring av en digital materialisering innebär en spårlös förändring av ett bitmönster på en databärare, som det är möjligt att manipulera vid överföringen mellan olika medier.

Fysisk och logisk kontext: Pappersurkunden innehåller en fix och efter utställandet oåterkallelig konstellation av ett ändligt antal uppgifter som är sammanställda i ett bestämt informationssyfte, medan denna fixa och låsta form i IT-miljön ersätts av en möjlighet att med hjälp av datorprogrammen kombinera och bearbeta uppgifterna till ett nära nog oändligt antal variationer.

Äkthet: Pappersurkunden ger, genom den fysiska låsningen av texten till bäraren, en möjlighet att genom t.ex. en kriminalteknisk undersökning undersöka om den har manipulerats, medan den digitala lagringen av uppgifter inte utan särskilda åtgärder ger någon motsvarande möjlighet till äkthetskontroll.

Finalitet: När en urkund upprättas, föreligger oftast en klar slutlåsning av urkunden genom att dess upprättande avslutas med en namnteckning eller någon annan utställarangivelse i anslutning till texten. Digitalt lagrade uppgifter kan spårlöst ändras, även om materialiseringen förses med något digitalt lås. Några allmänt accepterade rutiner för bekräftelse finns inte.

Besittning och tradition – symbolfunktioner: En pappersurkund innehas (besitts) av någon, som i sin tur kan överlämna den (tradera) till någon annan. Papperet kan därmed vara fysisk bärare av en rättighet. Denna s.k. symbolfunktion återskapas normalt inte i IT-miljön, där t.ex. en överföring av data inte sällan innebär ett mångfaldigande av ursprungsmaterialet och inte en fysisk tradering av detta IT-material. Motsvarande rättsverkan ges i stället genom att t.ex. en rätt till viss egendom registreras som en uppgift i IT-systemet.

Uppkomsthistoria: Texten i en pappersurkund kan hänföras till en direkt mänsklig tanke, medan uppgifterna i en digital materialisering ibland kan vara resultatet av automatiska processer.

7.3.2 Namnteckning – Digital signatur

För det stora flertalet människor torde företeelsen att skriva sitt namn på ett papper betraktas som okomplicerat. Det är ofta redan av sammanhanget eller av tradition uppenbart i vilka situationer en namnteckning förväntas och vilka följdverkningar detta får. Det är inte heller ovanligt att det uttryckligen anges när en namnteckning förväntas och vilka effekter som följer av undertecknandet. Trots detta är det inte helt enkelt att entydigt beskriva och definiera vilka funktioner aktiviteten ”att underteckna” har. En rad beskrivningar finns på området såväl i offentliga utredningar som i annan litteratur.[83] Nedan följer en kortfattad beskrivning av de mer centrala funktionerna[84] samt en kortare redogörelse för i vad mån aktiviteten ”att påföra en digital signatur” förmår att uppfylla dessa funktioner.

Viljefunktionen: Aktiviteten ”att underteckna” kan anses ge uttryck för en vilja att handla på ett visst sätt. Närmast avser

[83] Se bl.a. SOU 1992:110, SOU 1996:40, Hultmark, Elektronisk handel och avtalsrätt, 1998, Hiselius, Lindberg 1989 samt Einersen.

[84] Här koncentreras framställningen till faktorer av främst rättslig betydelse. Alltså bortses från exempelvis psykologiska och sociala och traditionella faktorer.

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[85]. På motsvarande sätt kan en signatur genom bruket av en hemlig nyckel, t.ex. en digital signatur, anses ge uttryck för en vilja. I vilken utsträckning en varningsfunktion kan uppnås vid användning av en digital signatur torde främst vara avhängig den allmänna uppfattningen om en bindande förpliktelse därigenom får anses uppkommen.

Identifieringsfunktionen: Namnteckningen kan användas för att identifiera en person. Detta kan t.ex. ske genom att en namnteckning som en person nedtecknar i närvaro av en kontrollant jämförs med en underskrift som med viss grad av säkerhet härrör från personen i fråga. Även den digitala signaturen kan användas för att identifiera en person. Detta möjliggörs av att en digital signatur kan verifieras med den öppna nyckeln. Anknytningen mellan nyckelparet och en viss person måste dock vara fastställt, något som skall utföras av en CA.

Äkthetsfunktionen: 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. Kopplingen till en person följer av att namnteckningen är personlig. Kopplingen är dock inte absolut i den mening att namnteckningen är unik för en person. Namnteckningar kan förfalskas eller två personer kan ha så gott som identiska underskrifter. För att kunna fastställa en viss namnteckning anknytning till en person krävs normalt en jämförelse med en annan namnteckning som med säkerhet härrör från personen i fråga. Möjligheten att på detta sätt avslöja t.ex. förfalskningar varierar. En med namnteckning närliggande företeelse är sigillet. Den kan sägas

[85] Viljefunktionen har också en tillitssida. En person kan, utifrån den undertecknade handlingen, anta att han kan agera på ett visst sätt.

fylla liknande funktioner som en namnteckning. Ur kontrollsynpunkt föreligger dock en väsentlig skillnad mellan att anbringa en namnteckning eller ett sigill på ett papper. Under det att en namnteckning normalt låter sig kontrolleras i efterhand [86], går det inte att enbart utifrån sigillet sluta sig till huruvida den anbringats av behörig person eller ej. Liksom ett avtryck av sigillet kan en digital signatur åstadkommas av den som har tillgång till den privata nyckeln[87]. Om flera personer har kännedom om en hemlig nyckel saknas möjlighet att avgöra vem av dem som signerat. Signaturen är följaktligen inte personlig utan bygger på att personen i fråga får en unik signatur, som han måste behålla för sig själv[88]. Givet detta förhållande kan den digitala signaturen användas för att identifiera den som nyttjat den hemliga nyckeln. Den möjliggör också att manipulationer av meddelandet kan upptäckas vid kontroll. Den digitala signaturen är nämligen knuten till det signerade meddelandet på ett sådant sätt att eventuella förändringar av meddelandet efter signeringen är möjliga att konstatera.

Bevisfunktionen: 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. Även digitala signaturer kan tillhandahålla identifierings- och äkthetsfunktioner, varför dessa – på samma sätt som namnteckningen – kan användas i situationer där behov av säkring av framtida bevisning förekommer.

[86] Det anses att namnteckningar endast med svårighet kan förfalskas på ett sådant sätt att förfalskning inte kan upptäckas i efterhand vid närmare analys.

[87] Möjligheten för obehöriga att få tillgång till en privat nyckel kan förstås försvåras genom bl.a. att lagra denna på endast en bärare, t.ex. ett kort eller att göra nyttjandet beroende av kunskap om en PIN-kod.

[88] Här kan det vara nära till hands att jämföra med en stämpel med vilket ett unikt sigill kan fra mbringas.

7.4 Reglering av CA-verksamhet

Även när det gäller CA-verksamheten kan erforderliga normer skapas på olika sätt. Samma synpunkter kan här anläggas som i fråga om den digitala signaturens rättsverkningar.

7.4.1 Nyckelcertifikatets innehåll och verkan

De flesta förslag som syftar till ett utbrett bruk av asymmetrisk kryptering för signeringsfunktioner, dvs. i allmänt tillgängliga telenät, bygger på att en betrodd tredje part garanterar kopplingen mellan nyckel och en viss person, s.k. certifieringsfunktion. Detta ankommer på certifieringsinstansen och sker genom att denna utfärdar ett s.k. nyckelcertifikat.

Certifikatet är ett intyg. Vad som därmed intygas är främst beroende av ceritfikatets innehåll och utformning.

Nyckelcertifikaten innehåller ett flertal olika uppgifter, däribland hänvisningar till andra källor. Uppgifternas karaktär och omfattning torde inte vara i rättsligt hänseende underkastade någon annan begränsning än vad som följer av t.ex. datalagen (1973:289) om skydd för uppgifter om enskilda. För att certifikatet skall kunna fylla sin grundfunktion måste den emellertid vara försedd med ett visst minimum av uppgifter, som måste vara signerade av certifieringsorganet. Som exempel kan nämnas uppgifter om[89]

- innehavarens identitet,
- den öppna nyckel som skall knytas till identiteten,
- certifikatets giltighetstid,
- CA,

[89] Standarder finns redan framtagna för certifikatets innehåll. Denna uppräkning avspeglar dock inte någon speciell standard.

- hur certifikatet kan kontrolleras[90] ,
- serienummer eller annan uppgift varigenom certifikatet kan identifieras,
- under vilka förutsättningar CA tillhandahåller certifikatet, samt
- policy (regelverk) för certifikatutgivning.

För att osäkerhet inte skall råda i samband med ansvarsdiskussioner kring innehållet i ett nyckelcertifikat är det av stor vikt att det skapas klarhet kring *vem* som skall anses vara utställare av *vad*. Eventuella ansvarsövergångar måste även klargöras.

Särskilda problem kan tänkas uppstå i de fall där ett certifikat innehåller uppgifter om fullmaktsförhållanden. Två typer av fall kan särskiljas.

I det första fallet råder *inte* identitet mellan CA och fullmaktsgivare. Uppgiften tjänar som upplysning *om* fullmaktsförhållandet och grundar i sig inget fullmaktsförhållande. Det är alltjämt de bakomliggande rättsförhållandena som avgör huruvida det verkligen föreligger fullmakt eller inte. Är uppgiften i certifikatet felaktig aktualiseras i stället frågan vem som bär ansvaret gentemot den som förlitat sig på uppgiften.

I det andra fallet råder det identitet mellan CA och fullmaktsgivaren. Detta kan t.ex. vara fallet när en juridisk person, som utövar CA-funktion inom sin egen verksamhet, certifierar sin egen personal. Om företaget utfärdar ett certifikat till en anställd, i vilket det upplyses att den anställde ges behörighet att utföra rättshandlingar i bolagets namn genom att teckna dess digitala signatur, kan det hävdas att certifikatet i sig skall betraktas som en fullmakt. Det torde bero på utformningen av certifikatet om så är fallet eller det endast är fråga om en uppgift om ett fullmaktsförhållande i enlighet med det första fallet. För att det skall vara fråga om en fullmakt torde det dock krävas att den som signerar certifikatet är behörig att

[90] Dvs. uppgift om CA:s öppna nyckel och andra kontrollmekanismer.

företräda den juridiska personen (CA). Samma resonemang torde kunna föras vid annat ställföreträdarskap.

För den som överväger att införa behörighetsuppgifter i certifikat finns det – oberoende av ovannämnda fall – anledning att närmare studera allmänt förekommande problem inom fullmaktsläran, exempelvis hur fullmakter skall kunna återkallas med bindande verkan gentemot tredje man.

Av intresse kan vara att överväga om det vore ändamålsenligt att inrätta ett offentligt register över certifikat med uppgifter om behörigheter. Ett syfte med en sådan registrering kan vara att uppnå särskild rättsverkan genom registreringen.

Det är inte alldeles självklart vem som skall kunna knytas till en nyckel. Skall möjligheten att erhålla en digital signatur vara begränsad till fysiska personer eller skall även juridiska personer ha samma möjlighet? För det fall även juridiska personer skall ges denna möjlighet uppkommer frågor om hur det tillförlitligen skall visas vem som är behörig att företräda juridiska personer genom att använda dess nyckel. Vidare uppstår frågor kring identitetsuppgiftens utformning.

En annan typ av fråga hänför sig till certifikatinnehållets rättsverkan gentemot den som accepterar en digital signatur utan att kontrollera certifikatet. Ett exempel är frågan i vilken utsträckning ett certifikat kan ge upphov till ond tro hos den som förlitar sig på en digital signatur, om denne inte kontrollerar innehållet i certifikatet.

Certifikatets rättsliga betydelse kommer huvudsakligen att vara koncentrerad till dess funktion som bevis. Av betydelse är därför att certifikatet åtnjuter hög tillit. Några förhållanden som därvid kan vara av betydelse är

- det straffrättsliga skyddet mot förvanskning av certifkat,

- möjligheterna att erhålla ekonomisk ersättning från CA om uppgifterna i certifikatet är felaktiga, samt

– möjligheterna att skapa en metod för hur certifikatets innehåll skall kunna verifieras i en rättegång.

7.4.2 Infrastruktur

Behov av regler och kontroll

Det förtroende som en ID-handling, t.ex. körkort, åtnjuter kan sägas vara resultatet av två faktorer. Handlingen är tillräckligt tekniskt säker, dvs. svår att förfalska, och den organisation som ger ut den åtnjuter ett allmänt förtroende. Utgivningen av körkort, som sker genom Vägverkets försorg, är bunden till regler för hur detta skall gå till. Ett körkort måste t.ex. vara inplastat och försett med ett fotografi, vilket tillsammans med övriga tekniska krav gör det svårt att förfalska. Härigenom knyts en tillit till kortet, som gör det möjligt att använda det i olika sammanhang, trots att förlitande part – t.ex. en bank – inte själv har något med identitetshandlingens framställning att göra.

Liksom beträffande traditionella identitetshandlingar måste det finnas regler för hur elektroniska identitetshandlingar skall ges ut. En elektronisk identitetshandling måste ges ut i enlighet med en viss definierad och allmänt känd policy för att kunna godtas även av andra än den organisation som givit ut den.

För att en digital signatur skall få något rättsligt värde krävs för det första att den som skapat signaturen kan identifieras tillförlitligt, för det andra att nyckelcertifikatet är skapat på korrekt sätt, och för det tredje att de verktyg och den teknik som används för att skapa signaturen är tillräckligt säkra. Detta innebär dels att den funktion (CA) som identifierar användare och knyter en verklig identitet till en elektronisk identitet (CA) måste vara tillförlitlig, dels att de program/den utrustning som används för att skapa och verifiera signaturer måste vara tillförlitliga för att signaturen skall få något rättsligt värde.

I en framtid är det troligt att flera företag och organisationer kommer att vilja utöva CA-funktion. Frågan om vad som generellt sett måste krävas för att digitala signaturer allmänt skall kunna

accepteras måste därför besvaras – oberoende av vilken CA som ligger bakom certifieringen.

Behov av regler för tekniken

För att digitala signaturer verkligen skall kunna fungera erfordras tekniska standarder och eventuellt andra former av regler för en rad olika funktioner. Det är kanske inte nödvändigt att samtliga nedanstående funktioner regleras i standard eller författning. I vissa fall kan det kanske räcka med att de kommunicerande parterna är överens om vad som skall gälla. Detta kommer dock att medföra en större osäkerhet när det gäller den rättsliga bedömningen vid en tvist som rör giltigheten hos en digital signatur.

Algoritmer: För att använda en digital signatur måste dels en hash-algoritm (eller annat unikt ”fingeravtryck”), dels en kryptografisk algoritm bestämmas. Liksom i många utländska system används vanligen RSA i Sverige. Förutom själva algoritmen måste vissa parametrar preciseras. Av betydelse är framförallt längden på den privata nyckeln, men också den öppna nyckeln. I någon mån kan system som verifierar digitala signaturer innehålla olika parametrar, men valet får konsekvenser för det förtroende man kan ha för en digital signatur.

Skydd av signeringsnycklar: Ett starkt skydd kan bestå i att man använder sig av smarta kort, som anses uppfylla höga krav på säkerhet även för mottagaren av den digitala signaturen. I Sverige har många förordat användning av smarta kort för skydd av signeringsnycklar. I USA däremot har man även beprövade system med rent mjukvarumässig hantering av nycklar och signeringsfunktion. Motivet bakom en standardisering av elektroniska ID-kort torde främst vara möjligheten att därigenom kunna säkerställa att innehavaren av ett elektroniskt ID-kort kan använda det i valfritt system med bibehållen säkerhet. Standardiseringen möjliggör billiga produkter.

Personlig kod: Ett annat exempel på områden som bör standardiseras gäller hantering av den personliga koden för kortets signa-

turfunktion. Man kan som SEIS rekommenderat ha separata koder för signerings- respektive identifieringsfunktionen för att säkerställa att användaren är medveten om när han endast identifierar sig respektive signerar ett dokument. Det har dock ifrågasatts om man kan kräva av användarna att de skall kunna hålla isär två koder. Om man skall tillåta att samma kod används för båda funktionerna måste den personliga kodens uppbyggnad preciseras. Den kan bestå av 4–5 siffror eller en längre sträng av alfanumeriska tecken. Det senare alternativet ökar i viss mån säkerheten, men utesluter möjligheten att använda koden i vissa typer av terminaler som bara har siffertangenter. I båda de beskrivna fallen krävs i vart fall standardisering i någon form.

Nyckelcertifikatets format: Certifikatformatet bygger ofta på *en* internationell standard (t.ex. ITU/X.509). Eftersom standarden finns i flera varianter måste ett val göras. Valet är beroende av säkerhetsmässiga överväganden men också praktiska frågor som vilket identitetsbegrepp den digitala signaturen primärt är kopplad till. Det finns bl.a. möjlighet att låta ett certifikat vara kopplat till en identitet (t.ex. ett nummer), som i sin tur är kopplad till en fysisk eller juridisk person.

Metoder för återkallande av och kontroll av återkallade certifikat: För att kontrollera om ett certifikat är återkallat brukar man använda allmänt tillgängliga katalogtjänster. Dessa kan emellertid ha olika gränssnitt och olika regler för tillgänglighet, varför ett behov av översyn och harmonisering för att underlätta användningen föreligger. Vidare måste metoder definieras för hur ett certifikat skall återkallas.

Format för koppling av signatur och eventuellt certifikat till den signerade informationen för att skapa ett digitalt dokument: På området finns ett flertal internationella standarder som inte är särskilt väl utvecklade. Det är inte heller säkerhetsmässigt viktigt. Flera olika format kan få förekomma. Det är emellertid praktiskt viktigt att mottagaren av ett signerat dokument har teknik som möjliggör att läsa text och verifiera signaturer på ett korrekt sätt.

Metoder för att kontrollera säkerheten i det system som används vid signeringen: Det finns ett antal hot som gör att man inte

kan vara helt säker på att det använda signeringssystemet verkligen garanterar att det innehåll som den signerande personen avsett att signera, överstämmer med det innehåll som signerats. En fullständig kontroll av detta problem är mycket svår att genomföra och kräver långt gången standardisering av applikationsprogram, hårdvara och troligen en oberoende kontroll av den tekniska realiseringen av systemet.

Regler för den administrativa infrastrukturen

För att parterna skall fästa tilltro till den digitala signaturen är det viktigt med ett regelverk för hur certifikat och elektroniska ID-kort skall utfärdas. Försök görs inom t.ex. ETSI[91] och IETF[92] att skapa tekniska standarder på området. Standardiseringarbetet går mera ut på att skapa en begreppsmodell för s.k. betrodda tredjepartstjänster än på att definiera innehållet i ett regelverk. Detta överlämnas i stället åt aktörerna själva. De internationella försök som gjorts för att skapa standarder på området beskriver i allmänna ordalag certifieringsprocessen och behovet av att skydda privata nycklar.

Möjligen är det så att man skall söka andra vägar än den formella standardiseringsprocessen för att fastställa ett regelverk. Det är dock inget som hindrar att även andra procedurer kan bli föremål för standardisering. Exempel på sådana är standarder om kvalitetssäkring av administrativ hantering som skett genom ISO 9000-serien.

Ett regelverk för den administrativa hanteringen förutsätts svara på ett antal frågor. Som exempel kan nämnas följande.

- På vilka grunder skall certifikat/ID-kort utfärdas?
- Hur skall man kunna kontrollera vilket identitetsbegrepp som används?

- Hur kontrolleras sökandens identitet?

[91] European Telecommunications Standards Institute
[92] Internet Engineering Task Force

- Hur skall CA organisera skyddet och kontrollen av det system och de nycklar som används vid utfärdande av nyckelcertifikat?

- Hur skall signeringsnycklar av tillräckligt god kryptografisk kvalitet och med tillfredsställande skydd mot missbruk genereras? Skall dessa enbart finnas registrerade på ID-kort för att därefter vara låsta för all extern åtkomst?

- Hur kan man förhindra att ”hackers” eller någon annan med särskild kunskap från tillverkarsidan missbrukar den fysiska kortprodukten?

- Hur skyddar man ID-kort under transport från central personalisering till utlämningspunkten?

- Vilka möjligheter skall finnas att byta PIN-kod?

- Hur skall man säkerställa att information om återkallade certifikat finns tillgänglig för dem som önskar göra en kontroll?

Det föregående är exempel på frågor som kan specificeras i en säkerhetspolicy för en betrodd tredjepartstjänst. En sådan policy skulle kunna finnas i form av en standard.

Om CA och arkiv

Om vi förutsätter att de problem med långsiktigt bevarande – som berörts i avsnitt 7.1.5.2 med sikte på svårigheterna att samtidigt bevara läsbarhet och autenticitet hos digitala meddelanden/handlingar – kan lösas, återstår frågan hur man långsiktigt skall hantera den information om nycklar m.m. som CA hanterar. I vilken utsträckning bör denna information överföras till statliga och kommunala arkivmyndigheter när affärsmässiga skäl saknas att upprätthålla inaktuell information? För att trovärdigheten till

digitala handlingar även på lång sikt skall kunna bibehållas, måste också de åtgärder som nyttjats för att skapa detta förtroende kunna dokumenteras och bevaras. Detta gäller även efter att en CA-verksamhet har avvecklats.

För en digital handlings tillförlitlighet är signaturen avgörande. Den säkerhet kring handlingens ursprung och innehåll som signaturen är avsedd att skapa kan emellertid vara bristfällig. Det krävs därför att ytterligare företroendeskapande funktioner bevaras. Utöver dokumentation av nycklar, krävs att dokumentation som utvisar vilka som faktiskt blivit certifierade bevaras. I annat fall löper man inte bara risken att meddelanden från individer som haft certifikat kan bli föremål för förfalskning eller förvanskning. Helt nya meddelanden kan skapas, där den föregivna utställaren varken haft nyckel eller certifikat.

Mot den beskrivna bakgrunden framstår det, beträffande arkivering, som nödvändigt att noga överväga vilka åtgärder som erfordras i samband med avveckling av en CA. Man bör i någon mån kunna jämföra de nu uppkomna frågeställningarna med dem inför millennieskiftet. Det som i dag kan förefalla orealistiskt och överdrivet, kan måhända på lite längre sikt uppfattas som ett betydligt allvarligare och mer påträngande problem.

7.4.3 Certifiering och kontroll av CA

I detta avsnitt skall i korthet belysas på vilket sätt kontrollen (tillsyn) av CA-verksamhet kan gå till. Med kontroll sammanhänger frågor om certifiering eller licensiering av CA-verksamhet.

Kontrollen kan utföras av det organ som certifierar en CA. I ett hierarkiskt system ställer t.ex. en överordnad CA villkor för att certifiera en underordnad CA. Vid korscertifiering torde saken förhålla sig något annorlunda. Av bl.a. konkurrensskäl framstår det inte som troligt att deltagande CA skulle utöva tillsyn över varandra.

Kontrollen kan alternativt utövas av ett fristående organ. Tillsynsfunktionen kan vara avtals- eller offentligrättsligt reglerad.

Licens för CA-verksamhet

Licensiering kan ske antingen efter en ansökan eller genom självlicensiering. Licensieringen kan vara obligatorisk, dvs. en förutsättning för att bedriva CA-verksamhet. Verksamheten måste då definieras på något sätt. Regler om licens kan också vara fakultativa (frivilliga). Endast licensierade CA träffas då av vissa lagreglerade krav. Vid en fakultativ licensregim är det troligt att digitala signaturer, som härrör från en licensierad CA, kommer att åtjnuta en högre tillit än signaturer från icke-licensierad verksamhet.

Ett koncept med licensierad CA-verksamhet förutsätter svar på en rad centrala frågeställningar. Nedan följer en översikt av några viktigare frågeställningar.

- Vem skall vara behörig att ansöka om licens? Skall det vara en stat, en mellanstatlig organisation, t.ex. EU, en internationell organisation eller ett enskilt subjekt?

- Skall all CA-verksamhet vara underkastad licensplikt? Internationella överenskommelser – t.ex. artikel 59 i Romfördraget och WTO-fördraget – om fri rörlighet för tjänster liksom konkurrensregler och regler mot kartellbildningar kan inverka på regler om förbud mot olicensierad CA-verksamhet.

- I vilken omfattning skall licensgivaren ansvara för innehållet i ett certifikat gentemot tredje man? Genom att förena licensen med villkor – licensieringsschema – kan licensgivaren åläggas ett ansvar att vidta erforderliga undersökningar av CA. Detta kan i sin tur ge upphov till frågor om ansvar för licensgivaren gentemot den som förlitar sig på ett certifikat. Å andra sidan kan tilliten till ett certifikat ökas av att licensgivaren har ett ansvar för dem.

- Skall endast vissa särskilt betrodda grupper få bedriva CA-verksamhet? Tilltron till ett certifikat skulle kunna ökas om CA-

verksamhet endast fick bedrivas av redan betrodda grupper, som står under tillsyn i någon form. Exempelvis Notarius Publicus, advokater eller banker. Sådana regler kan få inverkan på ansvarsfrågor.

– I vilken utsträckning skall CA ges behörighet att reglera sin verksamhet? För att en CA skall kunna fungera effektivt måste den kunna utforma bindande regler för dem vars certifikat den certifierar. Detta kan åstadkommas genom avtal. Frågor om effektivitet och möjligheten att genomdriva kontraktsrättsliga skyldigheter kan dock tänkas uppstå.

– Behöver CA-verksamhet regleras? En möjlighet är att lita på marknadskrafternas självreglerande förmåga. Den som missbrukar sitt förtroende kommer på sikt inte att kunna bedriva verksamhet. En annan möjlighet är att överlåta på marknaden – genom t.ex. branschorganisationer – att själv reglera verksamheten. Om man i stället väljer en nationell lagreglering torde det, med hänsyn till CA:s internationella karaktär, krävas en avstämning med andra länder i syfte att förebygga regelkollisioner.

Krav för att erhålla licens

För att tillgodose användarintressen och säkerheten i systemet m.m. kan krav ställas på den som önskar erhålla licens. Kraven bör vara så utformade att de utfärdade certifikaten även godtas i andra länder. För svensk del kan det vara värdefullt om man på gemenskapsnivå fastställer gemensamma kriterier för CA-verksamhet. Därigenom skulle certifikat utfärdade i en medlemsstat bli erkända i samtliga medlemsstater (ömsesidigt erkännande). Kommissionen har i meddelandet ”Om säkerhet och pålitlighet vid elektronisk kommunikation – Mot en europeisk ram för kryptering och digitala signaturer” givit följande exempel på sådana gemensamma krav,

– säkerhet vid CA och efterlevnaden av lagarna om datasäkerhet,

– tillförlitlig identifiering av personer (för att garantera att en viss nyckelinnehavare kan identifieras),

– lägsta nivå på försäkringsskydd (CA måste kunna betala eventuella skadestånd),

– tekniska komponenter,

– utbildning och säkerhetskontroll av personalen, samt

– förbud mot ”självcertifiering” av CA.

Kommissionen fann i samma meddelande att det kunde vara lämpligt att – för att nå upp till högsta säkerhetsnivå – göra en tydlig åtskillnad mellan olika uppgifter, t.ex. certifiering och nyckeldeponering, och mellan olika typer av certifikat. Kravkatalogerna bör därför kunna se olika ut med hänsyn till de tjänster som erbjuds av CA.

Utöver de krav som kommissionen pekat på i sitt meddelande, torde det även krävas någon form av reglering på följande områden.

Dokumentation: Erforderlig dokumentation om identifiering, datum för utfärdande av certifikat, datum för när certifikat upphör att gälla, upphävande eller återkallelse av certifikat, tekniska förfaranden för att åstadkomma certifikat, tidsstämplar m.m. eftersom dessa kan komma att behöva bevisas vid en rättegång där företrädare för CA kallas att vittna. En reglering kan behöva ange den tid under vilken dokumentationen måste finnas bevarad. Hänsyn måste tas till preskriptionsregler. Regler om hur förvaring av dokumentationen skall ske med back-up rutiner och liknande säkerhetsåtgärder kan behövas.

Revision: CA:s verksamhet bör regelbundet revideras. Fråga uppkommer huruvida befintlig lagstiftning om bokföringsskyldighet m.m. – med möjlighet till revision – är tillfyllest eller om särskilda regler om revision behövs. Skall särskilda regler införas uppstår

frågan om revision skall utföras av enskilda revisorer eller av licensgivaren.

Tillsyn och verkställighet: Om reglering utformas som självreglering eller genom licenstilldelning måste ändå rätten för en organisation eller myndighet att utöva tillsyn och vidta verkställighetsåtgärder vara behörigen grundad i lag.

Överklagande: Varje form av regelverk torde fordra att möjlighet att överklaga beslut med stöd av regelverket finns. Förfaranderegler behöver införas.

Avgifter: CA kommer av allt att döma att ta ut avgifter för att ställa ut certifikat. Prisregleringsfrågor kan uppkomma. Avgifter till staten kan i vissa fall utgöra förklädda handelshinder för tjänster.

Upphörande av CA-verksamhet: För det fall en CA upphör med sin verksamhet kan regler komma att behövas om skyldighet att överlämna dokumentation och certifikat till en annan CA eller skyldighet att bibehålla dokumentation och behålla bevis om certifiering under viss tid.

Kontroll av tekniska produkter

Tekniska produkter, som är avsedda att användas för att åstadkomma digitala signaturer, skall enligt föregående avsnitt uppfylla vissa krav. För att säkerställa att kraven uppfylls krävs en kontrollfunktion.

Den tyska lagen om digitala signaturer (14 §) åskådliggör i grova drag vad som behöver kontrolleras. Krav på sådan kontroll torde uppkomma oberoende av om verksamheten bedrivs med licens eller inte. Bedrivs verksamheten med licens kan den tekniska kontrollen behöva definieras närmare. I det tyska regelverket[93] anges att vissa tekniska komponenter måste vara kontrollerade mot vissa kravnivåer. De algoritmer med tillhörande parametrar som får användas, skall offentliggöras. Kontrollerna skall utföras av särskilda godkända provningsställen.

[93] Jfr 17 § förordningen om digitala signaturer, som hänvisar till vissa tekniska komponenter i 14 § lagen om digitala signaturer

I Sverige finns en lag (1992:1119) om teknisk kontroll. Bedömning av överensstämmelse och annan teknisk kontroll utförs enligt lagen av, eller under medverkan av organ som avses i 1 § 1 i lagen, eller av ackrediterade organ. Detta gäller under förutsättning att kontrollen är föreskriven i lag eller annan författning, har ålagts någon genom beslut av myndighet eller annars har särskilda rättsverkningar enligt föreskrift i lag eller annan författning (2 §). Därefter följer regler om vilka organ som skall anmälas till EU. Sådana organ skall pröva överensstämmelse med bestämmelser som gäller inom EES. Till lagen finns en förordning, i vilken anges att myndigheter som får föreskriva att produkter, anläggningar eller motsvarande skall ha eller sakna vissa egenskaper (föreskrivande myndigheter) skall samråda med Styrelsen för ackreditering och teknisk kontroll (SWEDAC) innan de meddelar föreskrifter om bedömning av överensstämmelse som omfattas av lagen om teknisk kontroll.

SWEDAC är nationellt organ för ackreditering enligt lagen om teknisk kontroll. Det finns en instruktion för SWEDAC[94]. Därtill finns en förordning (1989:527) om riksprovplatser och riksmätplatser, som numera enbart avser riksmätplatser.

Lagen om teknisk kontroll skulle kunna tillämpas på tekniska komponenter för framställning av digitala signaturer.

[94] SFS 1996:81

Kontroll av CA-verksamhet

CA-verksamheten innefattar såväl administrativa förfaranden som användningen av tekniska komponenter. I kontrollen av en CA-verksamhet kan dock ingå att kontrollera att de tekniska komponenter som används uppfyller vissa krav.

En marknadsreglerad kontroll av CA-verksamhet kan tänkas gestalta sig på två olika sätt. I det ena fallet enas CA-organen om ett gemensamt kontrollorgan. I det andra fallet utövas kontrollen av de CA-organ som korscertifierar varandra. En CA som uppvisar brister kan därvid komma att uteslutas från samarbetet. Med hänsyn till konkurrenssituationen, torde det vara svårt att åstadkomma en egentlig tillsynsfunktion i det senare fallet.

Om CA-verksamheten lagregleras kan en tillsynsfunktion behöva inrättas. En sådan funktion torde inbegripa kontrollen av att uppställda krav för verksamheten efterlevs. Kontroll kan ske vid start av verksamheten, i samband med licenstilldelning och genom regelbundna eller stickprovsvisa kontroller av verksamheten.

7.4.4 Erkännande av utländska CA

För att elektronisk handel skall kunna fungera internationellt, måste certifikat utfärdade av utländska CA erkännas i andra länder. För EU innebär detta att nationella strukturer kan kompletteras med en samordning i detta avseende på gemenskapsnivå. För medlemsstaterna erfordras därutöver överenskommelser med tredje land.

Ömsesidigt erkännande av utländska CA

En svårighet i samband med erkännande av utländska CA är att det kan vara svårt att upptäcka brister i den utländska tillsynsapparaten. En brist i den utländska kontrollfunktionen kan medföra att tilltron till hela systemet minskar.

Några frågor som kan uppkomma vid erkännande av utländska CA är följande.

- Hur kommer kulturella skillnader att påverka ett erkännande?
- Vilka krav måste uppställas för att utländska certifikat eller CA skall kunna erkännas?
- Hur skall man förfara när en rättsordning innehåller ett obligatoriskt krav på licensiering medan en annan inte gör det?

Ömsesidigt erkännande av licensieringsförfarande

En möjlig regleringsväg är att införa en standard för CA-verksamhet[95]. Detta kommer att möjliggöra att CA från olika jurisdiktionsområden kan förlita sig på certifikat, som har utgivits enligt samma standard. Det bör emellertid beaktas att certifieringsprocessen innefattar människors medverkan i olika avseenden, vilket kan medföra betydande variationer i det sätt på vilket sådana standarder *de facto* tillämpas. Kommer det sålunda att vara möjligt att godta ett utländskt certifikat, som i och för sig uppfyller samma standard som den inhemska men härrör från land som saknar en tillförlitlig organisation för personidentifiering?

Erkännande genom standarder betyder inte att alla CA måste ha licens. I vissa rättsordningar kommer licensiering av CA att vara obligatorisk, i andra frivillig eller helt saknas. Avgörande för om en utländsk CA skall erkännas är licensieringsschemats tillförlitlighet. För att kunna bedöma om alla, några eller inga CA i ett visst land skall erkännas, måste rättsordningen i det landet studeras.

Erkännande i praxis av utländska digitala signaturer

[95] ITU:s standard X.509v3 etablerar användning av en CA-policyförklaring (eng. Certification Policy Statement, CPS) där de följande CA-verksamheterna beskrivs. Likheterna mellan policyförklaringarna mellan två CA skulle kunna möjliggöra ett jämställande i fråga om trovärdighet för deras certifikat.

Domstolarna kommer med all sannolikhet att ställas inför frågan om en utländsk digital signaturs tillförlitlighet. Särskilt när signaturen härrör från ett land för vilket det saknas regler om erkännande kommer det sannolikt att bli en kostsam process att bevisa tillförlitligheten hos den digitala signaturen.

Ett europeiskt ramverk

Inom EU har kommissionen i meddelandet ”Om säkerhet och pålitlighet vid elektronisk kommunikation – Mot en europeisk ram för kryptering och digitala signaturer”, lämnat förslag till ett europeiskt ramverk för digitala signaturer och kryptering.

Det finns inom EU två möjliga sätt att på rättslig väg främja den mellanstatliga elektroniska handeln. Medlemsstaterna kan i sin nationella lagstiftning själva införa regler om ömsesidigt erkännande av utländska certifikat. En tillämpning av artiklarna 30, 52 och 59 i Romfördraget förhindrar i viss utsträckning att konkurrenshämmande specialregleringar införs i enskilda medlemsländer. En annan möjlighet är att på gemenskapsnivå vidta åtgärder för att harmonisera en europeisk CA-verksamhet, liksom gemensamma kriterier och rutiner för utvärdering av sådan verksamhet. Sådan harmonisering kan ske med stöd av direktiv. Ett direktiv är bindande för medlemsstaterna.

Att gå vägen över nationell lagstiftning kan dock ge upphov till problem. Ett inte helt otänkbart exempel kan vara om en medlemsstat inrättar ett lagreglerat licensieringssystem för CA, som inte lämnar utrymme för ett erkännande av certifikat från andra medlemsstater. För att underlätta ömsesidiga erkännanden kan en lösning på gemenskapsnivå vara av värde.

7.4.5 Kontrollorganens befogenheter

Om CA-verksamhet lagregleras, varvid krav uppställs på hur verksamheten skall bedrivas m.m., torde en tillsynsfunktion behöva inrättas. För att denna skall bli effektiv måste tillsynsorganet utrustas med befogenheter som ger det möjligt att utföra tillsynsfunktionen och vidta åtgärder mot en CA som inte följer de regler som gäller för verksamheten.

Exempel på sådana befogenheter kan vara rätten att

- fordra in handlingar och göra inspektioner,
- utfärda föreskrifter för verksamheten och tekniska produkter,
- utfärda förelägganden eventuellt förenade med vitesföljd,
- förbjuda viss verksamhet,
- återkalla licens,
- spärra certifikat, samt
- anmäla till åtal.

Därutöver bör övervägas om det behövs en möjlighet att kunna tvångsförvalta en CA-verksamhet under en övergångstid, eventuellt kombinerad med en befogenhet att kunna överlåta verksamheten eller avveckla den.

Vid utformning av regler för en tillsynsverksamhet, kan reglerna för tillsyn inom finanssektorn vara vägledande.

7.4.6 Ansvarsfrågor i olika partsrelationer

Problembeskrivning

Användningen av digitala signaturer aktualiserar en rad olika partskonstellationer där gällande rätt beträffande ansvarsförhållandena är osäker.

Förhållandet mellan *förlitande part och nyckelinnehavare* är oklart i det fallet då någon obehörig missbrukar den privata nyckeldelen. Missbruket kan t.ex. ha möjliggjorts på grund av att den underliggande tekniken varit enkel att manipulera eller på grund av att nyckelinnehavaren handskats vårdslöst med sin PIN-kod eller sitt smarta kort. Enligt svensk rätt torde som utgångspunkt gälla att nyckelinnehavaren inte blir bunden av rättshandlingar som inte företagits av honom.

Relationen mellan *CA och förlitande part* kan vara av olika slag. Den kan vara kontraktuell, utom-kontraktuell, kvasi-kontraktuell, indirekt kontraktuell eller förvaltningsrättslig – allt beroende på situationen. Är förhållandet mellan CA och den förlitande parten kontraktuellt råder avtalsfrihet. En redogörelse för vad som då gäller finns i avsnitt 7.4.7 I de allra flesta fall torde något avtalsrättsligt förhållande emellertid inte föreliga. I utomobligatoriska förhållanden är utgångspunkten att skadeståndsskyldighet för ren förmögenhetsskada föreligger endast i de fall skadan orsakats genom brott[96]. Rättsfallet NJA 1987 s. 692 visar dock att man i vissa situationer är beredd att skydda sådana personer som, utan att vara avtalsparter, har ett näraliggande och skyddsvärt intresse av att avtalet fullgörs på ett korrekt sätt[97].

Hur man än kategoriserar relationen är ansvarsfördelningen oviss. Fråga är t.ex. vilken typ av ansvar CA har för nyckelinnehavarens identitet och att meddelanden är oförändrade. Är det fråga om ett strikt ansvar, culpa-ansvar, exculpationsansvar eller ansvar endast om CA agerat brottsligt? Därutöver uppkommer problem

[96] Se 2 kap. 4 § skadeståndslagen.
[97] Se Ramberg, Allmän avtalsrätt, 4 uppl. s. 273 f. och Hultmark, Elektronisk handel och avtalsrätt, 1998, s. 38 f.

och osäkerhet beträffande i vilken omfattning, och i så fall hur, CA kan begränsa sitt ansvar. Härvid kan det eventuellt vara skillnad beroende på om den förlitande parten är konsument eller näringsidkare.

Relationen mellan *nyckelinnehavaren och CA* är den minst problematiska. Den är kontraktuell och vardera partens skyldigheter kan regleras i avtalet. Om CA inte uppfyller sina avtalsrättsliga förpliktelser föreligger ett kontraktsbrott. Följderna av det regleras i avtalet, ev. utfyllt med allmänna avtalsrättsliga principer. På det kommersiella området begränsas avtalsfriheten ytterst genom generalklausulen i 36 § avtalslagen. Om nyckelinnehavaren är konsument kan man tänka sig att avtalsfriheten har ytterligare begränsningar (jfr konsumentköplagen och konsumenttjänstlagen).

En annan fråga är i vilken omfattning CA skall kunna återkalla eller temporärt spärra ett certifikat utan nyckelinnehavarens uttryckliga begäran.

En situation kan uppstå då en obehörig person utger sig för att vara en viss person som aldrig har varit i kontakt med CA. Därvid uppkommer frågan om *CA:s ansvar i förhållande till den som utsatts för identitetsmissbruk*. Visserligen blir den som utsatts för sådant missbruk inte bunden eller ansvarig i förhållande till den förlitande parten, men han kan lida avsevärd skada t.ex. på grund av att hans kreditvärdighet blivit ifrågasatt. Det är osäkert hur CA:s ansvar gestaltar sig om CA t.ex. agerat vårdslöst i samband med identitetskontrollen.

Behovsbeskrivning

Så som framkommit råder viss osäkerhet i rättsläget beträffande ansvaret i de relationer som en digital signatur aktualiserar. Det föreligger ett behov av en närmare analys av rättsläget och av om det är nödvändigt med lagstiftning eller om frågorna kan överlämnas till praxis. Det skall därvid beaktas att behovet av civilrättslig reglering påverkas av hur CA-verksamheten regleras. Behovet av en analys accentueras särskilt då nyckelinnehavaren är

konsument. En utgångspunkt för en vidare analys av denna fråga bör vara upprätthållandet av ett starkt konsumenträttsligt skydd.

I detta sammanhang bör påpekas att den tyska lagen om digitala signaturer inte behandlar ansvarsfrågor och att detta var ett aktivt ställningstagande av den tyska lagstiftaren.

Det amerikanska advokatsamfundet

Det amerikanska advokatsamfundet har i en skrift[98], nedan kallad ”Guidelines”, föreslagit ett regelverk för CA-verksamhet. Guidelines innehåller de grundläggande reglerna för CA. En av reglerna innefattar en ansvarsbegränsning för CA.

Enligt advokatsamfundet kan en skiljelinje göras mellan ansvar för skadefall som är en följd av att CA brutit mot de regler som uppställts för verksamheten och sådana skador som inträffat trots att CA följt reglerna.

Enligt advokatsamfundet skall en CA, som följer tillämplig lagstiftning och i förekommande fall avtalsvillkor samt det regelverk som Guidelines innehåller, inte kunna göras ansvarig för skada som

1 innehavaren av ett certifikat eller en annan person ådragit sig, eller

2 är orsakad av att någon förlitat sig på

- ett certifikat som utställts av CA,
- en digital signatur som verifieras med hjälp av en öppen nyckel som finns angiven i ett certifikat, eller
- information som finns angiven i ett sådant certifikat eller hos en depositarie (eng. repository).

[98] Digital Signature Guidelines – Legal Infrastructure for Certification Authorities and Secure Commerce, 1996, American Bar Association, Chicago, USA

Möjligheten att på detta sätt begränsa CA:s ansvar är enligt advokatsamfundet nödvändigt för att stimulera etableringen av CA-verksamhet. Utan tillräcklig klarhet om de grundläggande reglerna med möjlighet att uppskatta de rättsliga riskerna, torde det enligt advokatsamfundet vara få som vågar satsa på en etablering.

7.4.7 Statens ansvar

En fråga som kan bli aktuell inom ramen för ett system med digitala signaturer är vilket ansvar staten har vid stora skadefall. Svaret på frågan är i hög grad beroende av vilken roll staten har i ett system och hur detta system rättsligt sett är strukturerat. Av intresse är också frågan vad som gäller beträffande statens ansvar vid CA:s konkurs. Nedan följer en kort beskrivning av det rådande rättsläget på angivna områden.

Stora skadefall – staten uppträder som CA

Om staten (en statlig myndighet) ikläder sig rollen som CA, kan staten – som vilken CA som helst – ha ett skadeståndsansvar. Karaktären av detta ansvar kan ha olika skepnader beroende på systemets rättsliga struktur m.m. Som framgått tidigare (se avsnitt 7.4.6) kan ett sådant ansvar *gentemot den signerande parten* vara rent avtalsrättsligt grundat. Ansvaret är i så fall reglerat i parternas avtal, eventuellt utfyllt med allmänna kontraktsrättsliga principer. Här råder avtalsfrihet, vilket innebär att parterna efter eget gottfinnande kan reglera alla relevanta frågor, såsom ansvarsgrunder, ansvarets omfattning, ansvarsbegränsningar m.m. Om parterna inte har reglerat dessa frågor – vilket i och för sig förefaller mindre realistiskt – kan man diskutera vilket ansvar CA bär. Svaret är inte givet. Det beror bl.a. på hur kontraktet i övrigt är utformat. Som en ”miniminivå” kan man dock säga att en CA åtminstone är ersättningsskyldig vid väsentliga kontraktsbrott.

På det kommersiella området begränsas avtalsfriheten ytterst av generalklausulen i 36 § avtalslagen, som möjliggör jämkning av oskäliga avtalsvillkor. I de fall den signerande parten är konsument kan man tänka sig att avtalsfriheten har ytterligare begränsningar (jfr konsumenttjänstlagen). Vad som nu sagts gäller oberoende av om staten ikläder sig rollen som CA.

Fråga är vidare om staten har något ansvar utöver vad som generellt gäller eller om statens ansvar är inskränkt på något särskilt sätt.

Så länge förhållandet mellan staten (i egenskap av CA) och signerande part är att betrakta som kontraktsrättsligt, går inte statens ansvar längre än vad som följer av allmänna skadeståndsrättsliga principer. Skadeståndslagen, som bl.a. reglerar det allmännas ansvar, gäller i princip inte i inomobligatoriska (kontraktsrättsliga) förhållanden (1 kap. 1 §).

Vidare inställer sig frågan om statens ansvar i förhållande till den *förlitande parten*. Relationen mellan förlitande part och CA kan i och för sig vara kontraktsrättsligt grundat. I så fall gäller i princip vad som sagts ovan. Vanligen torde det dock inte finnas något avtalsförhållande mellan CA och den förlitande parten. I sådana fall aktualiseras den generella bestämmelsen om statens (det allmännas) skadeståndsansvar i 3 kap. 2 § skadeståndslagen. I det aktuella lagrummet föreskrivs att staten eller kommun skall ersätta personskada, sakskada eller ren förmögenhetsskada, som vållas genom fel eller försummelse vid myndighetsutövning i verksamhet för vars fullgörande staten eller kommun svarar. Det innebär att det här finns en skillnad jämfört med om CA är ett privat subjekt. Statens ansvar för ren förmögenhetsskada förutsätter inte brott vilket är fallet om CA är ett privat subjekt (jfr 2 kap. 4 § skadeståndslagen). Statens ansvar går alltså i så måtto längre. Det krävs dock för ansvar att skada har uppkommit vid myndighetsutövning. Möjligen kan detta krav i något fall verka begränsande.

I övrigt kan nämnas att det på snarlika områden finns (eller kan förväntas) särskild reglering. I förslaget till ny personuppgiftslag (se prop. 1997/98:44) föreslås (se 48 §) en bestämmelse om att en personuppgiftsansvarig skall ersätta en registrerad person för skada

och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med lagen orsakat. Denna ersättningsskyldighet kan jämkas om den personuppgiftsansvarige kan visa att felet inte berodde på honom. Personuppgiftslagen torde inte vara tillämplig på digitala signaturer, eftersom dessa inte är att betrakta som personuppgifter (jfr 3 §). Skadeståndskonstruktionen kan dock förväntas bli kopierad i flera registersammanhang.

I SOU 1993:55 föreslås att stat eller kommun skall ersätta ren förmögenhetsskada som vållas genom fel eller försummelse när en myndighet lämnar upplysningar. Detta förslag är för närvarande under beredning inom Justitiedepartementet.

Stora skadefall – Statens ansvar i andra fall

Om staten inte har rollen som CA är läget annorlunda. Staten har inget särskilt skadeståndsansvar vid t.ex. stora skador. Om man vill åstadkomma ett sådant ansvar krävs särskild reglering. Från andra områden kan nämnas olika ”garantikonstruktioner”, t.ex. den insättningsgaranti kontohavare i bank har.

Slutligen kan nämnas att läget kan bli annorlunda om staten – utan att vara CA – på något annat sätt ingår i systemet. Om staten t.ex. utövar tillsyn eller liknande, kan staten vid brister i fullgörandet av sin tillsynsuppgift drabbas av ersättningsskyldighet. Det beror då på hur tillsynsfunktionen är uppbyggd och reglerad.

Statens ansvar i händelse av CA:s konkurs

Om en CA försätts i konkurs, får eventuella anspråk på ersättning bevakas i konkursen. Konkursboet svarar inte för sådant. Staten har – utöver de anställdas rätt till lönegaranti – inget särskilt ansvar i sådant fall.

7.4.8 Integritets- och säkerhetsfrågor

En CA kan tillhandahålla olika tjänster i samband med digitala signaturer. En central uppgift är att verifiera rätten till en öppen nyckel samt denna nyckels egenskaper. Detta kan bl.a. leda till att ett register över öppna nycklar skapas. Ett sådant register kommer att innehålla uppgifter om nyckelinnehavare. En person kan ha flera öppna nycklar beroende på i vilken roll han uppträder. Det är också möjligt att använda pseudonym och därmed vara anonym.

En CA i ett land kan också certifiera nyckelinnehavare i andra länder. Uppgifter kommer då att lämnas över nationsgränser. Dessa och andra omständigheter leder till att faktorer om uppgifternas art, vem som har ansvaret för uppgifterna, hur dessa används, säkerheten i hanteringen och utlämnandet av uppgifter måste beaktas.

Regler som i detta sammanhang bör beaktas återfinns i regeringsformen (RF), datalagen (1973:289), Europarådets dataskyddskonvention, den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna samt EG:s dataskydds- och ISDN-direktiv.

Sedan den 1 januari 1995 gäller den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna som lag i Sverige. Enligt artikel 8 i konventionen har alla rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens.

1 kap. 2 § RF stadgar att det allmänna skall värna den enskildes privatliv och familjeliv. Den övergripande regleringen till skydd för den personliga integriteten återfinns i 2 kap. 3 § andra stycket RF som stadgar att varje medborgare i den utsträckning som närmare anges i lag har ett skydd mot att hans personliga integritet kränks genom att uppgifter om honom registreras med hjälp av automatisk databehandling.

De närmare bestämmelserna om integritetsskyddet finns i datalagen (1973:289). Datalagen reglerar inrättandet och förandet av personregister, dvs. register som förs med automatisk databehandling och som omfattar personuppgifter. Juridiska personer omfattas inte av datalagens regler.

Europarådets dataskyddskonvention, som trädde i kraft i januari 1981, har till syfte att se till att grundläggande fri- och rättigheter, särskilt den enskildes rätt till personlig integritet i samband med automatisk databehandling av personuppgifter respekteras.

Inom integritetsskyddsområdet har EU utfärdat två direktiv, *dels* Europaparlamentets och rådets direktiv 95/46/EG om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (dataskyddsdirektivet), *dels* Europaparlamentets och rådets direktiv 97/66/EG om behandling av personuppgifter och skydd för privatlivet inom telekommunikationsområdet.

Dataskyddsdirektivet omfattar väsentligen skyddet av fysiska personers grundläggande fri- och rättigheter, särskilt rätten till privatliv, i samband med behandlingen av personuppgifter. Däremot omfattas inte sådan behandling av personuppgifter som faller utanför gemenskapsrättens område såsom allmän säkerhet och inte heller register för personligt bruk. Direktivet anger förutsättningarna för när personuppgifter får behandlas. I direktivet finns regler om säkerhet vid behandling. Särskilt skyddsvärd anses sådan behandling som innefattar överföring av uppgifter i ett nätverk vara.

En proposition (prop. 1997/98:44) om en ny personuppgiftslag har av regeringen överlämnats den 8 december 1997 till riksdagen. I den föreslagna lagen, som skall ersätta datalagen, genomförs dataskyddsdirektivet. Lagen följer i allt väsentligt direktivets disposition och innehåll. På samma sätt som i direktivet undantas privat behandling av personuppgifter. Ansvarig för behandlingen av personuppgifter är den personuppgiftsansvarige (jfr direktivets *registeransvarig*). Den personuppgiftsansvarige kan låta annan, personuppgiftsbiträdet (jfr direktivets *registerförare*), utföra behandlingen. Personuppgiftslagen reglerar den behandling av personuppgifter som är tillåten. I 30 § finns regler om säkerheten vid behandling av personuppgifter. Paragrafen omfattar såväl den personuppgiftsansvariges behandling som den som direkt eller indirekt har hans uppdrag att utföra behandlingen. Särskilda bestämmelser i annan lagstiftning om behandling av personuppgifter tar över. De övergripande reglerna om säkerhetsåtgärderna och

omfattningen av dessa återfinns i 31 §. Bestämmelserna motsvarar artikel 17 i dataskyddsdirektivet. Enligt 32 § kan tillsynsmyndigheten, dvs. Datainspektionen, besluta om vilka säkerhetsåtgärder som skall vidtas och förena beslutet med vite. Enligt huvudregeln i 33 § är det förbjudet att föra över personuppgifter till länder utanför EU eller länder som inte är anslutna till Europeiska ekonomiska samarbetsområdet. Vissa undantagssituationer såsom när den registrerade samtycker finns i 34 §. Enligt de föreslagna ikraftträdande- och övergångsbestämmelserna är lagen avsedd att träda i kraft den 24 oktober 1998. Vid samma tidpunkt skall också datalagen upphöra att gälla utom bl.a. i de fall då behandlingen av personuppgifter har påbörjats före ikraftträdandet. I sådana fall gäller datalagens regler t.o.m. den 30 september 2001.

8 Samhällets sårbarhet och digitala signaturer

En utbredd användning av digitala signaturer för olika ändamål innebär att samhället tillförs en ny infrastrukturell metod för förtroendeskapande mellan såväl fysiska personer som organisationer. I takt med att användningen ökar kommer olika verksamheters beroende av tillförlitliga digitala signaturer att öka.

De medel som i dag erbjuds för att skapa digitala signaturer innebär att en infrastrukturell teknisk plattform skapas, vars funktionsförmåga är avgörande för att digitala signaturer skall kunna bibehålla sin förtroendeskapande karaktär.

I takt med ett ökat teknikberoende i samhället får olika typer av störningar allt större konsekvenser. Störningar kan på sikt också komma att drabba fler sektorer i samhället. Noggranna analyser av de konsekvenser som kan förutses bör därför genomföras på ett tidigt stadium för att om möjligt förebygga eller mildra vissa av dem.

8.1 IT-systemens sårbarhet

Digitala signaturer hanteras per definition av och i IT-system. Redan kända brister i olika IT-system finns beskrivna i rapporter från Riksrevisionsverket, SAMS, Toppledarforum, Överstyrelsen för civil beredskap (ÖCB), Statskontoret m.fl., och kommer även att finnas i de system som utgör den infrastrukturella plattformen för digitala signaturer.[99]

[99] *Rapporter från Riksrevisionsverket:* Rätt data 1990-11-30, F 1991:21, IT/ADB-samverkan inom offentlig sektor, Fg 191:11, ADB i samverkan, F

Vissa verksamheter är av avgörande betydelse för samhällets förmåga att motstå påfrestningar. Om en verksamhet är beroende av IT-system för att utföra sin uppgift gäller detta även under störda förhållanden. Inom totalförsvarets civila delar skall de flesta uppgifter utföras även under störda förhållanden, även om kraven på kvalitet och produktionsvolym är lägre. Banktjänster och transfereringar i samhället är i dag helt baserade på informationsteknik. Systemens förmåga att fungera i kristid bygger helt på funktionsförmågan i dag under ostörda förhållanden. Den uppfattningen har även Hot- och riskutredningen, vars arbete ligger till grund för regeringens proposition 1996/97:11 Hot och risker i samhället.

Hot, risker samt störningar i systemen kan uppstå av många orsaker. Nedan följer några exempel på faktorer som kan påverka systemdriften.

- Obehöriga kan göra intrång i systemen, vilket kan få till följd att obehöriga får del av lagrad information, att information försvinner/förvanskas eller att systemet som sådant saboteras.

- Avbrott i försörjningen av el, vatten och luft.

- Avbrott i telekommunikationer.

1992:2, Fel data kostar! 1992-02-07, F 1993:34, Myndigheterna och informationsteknologi – IT, RRV 1994:31 Bättre ADB-projekt.
Rapporter från SAMS (Samrådsgruppen för samhällets säkerhet inom dataområdet): Ds 1990:44, Samhällsaspekter på säkeheten inom betalningsväsendet, Ds 1990:46, Strukturfrågor och säkerhet.
Rapport från Statskontoret: Dnr 617/91-5, Myndigheternas säkerhetsanalyser av sina ADB-system.
Rapporter från Toppledarforum: Spelregler för samverkan, Arbetsmarknadsstyrelsen 1995, Säkrare IT i offentlig sektor – en gemensam IT-säkerhetslösning baserad på aktiva kort för stat, kommuner och landsting, Landstingsförbundet 1996, Kvalitetssäkrad informationsförsörjning i offentlig förvaltning, förstudie, Överstyrelsen för civil beredskap, 1996.
Rapport från Överstyrelsen för civil beredskap: Säkerhetshöjande åtgärder för samhällsviktiga datasystem inom civila delen av totalförsvaret, 1995.

- Underhåll och reparationer minskar till följd av personal- eller reservdelsbrist eller p.g.a att serviceåtaganden inte fullföljs.

- Personal saknas.

- Störningar i omgivningen (brand, vibrationer, damm m.m).

Flertalet organisationer är i dag beroende av elektronisk information från andra för att kunna producera eller leverera tjänster. Sårbarheten berör således hela flöden av produktion och information.

Landets ledning kräver, oberoende av om det råder störda förhållanden eller inte, tillgång till information som finns lagrad i IT-system.

Fungerande telekommunikationer är en grundläggande förutsättning för att hela systemkedjor skall kunna fungera.

8.2 Totalförsvarets användning av digitala signaturer

De flesta samhällsviktiga företag, myndigheter, kommuner, landsting m.fl.som inom något eller några år kommer att använda digitala signaturer, har kravet på sig att kunna bedriva verksamhet oberoende av om det råder störda förhållanden eller inte.

Olika totalförsvarsmyndigheter har kommit olika långt i att använda digitala signaturer. Försvarsmakten har under åren 1994–1995 upphandlat aktiva kort för användning inom totalförsvaret. Systemet är uppbyggt för att tillgodose främst myndigheternas behov i såväl ostörda som störda förhållanden samt krig. Ett antal tillämpningssystem byggs f.n. upp som kommer att använda tjänster som digitala signaturer, autenticering och distribution av krypteringsnycklar (symmetriska)[100].

[100] Teletrust, CA-policies i praktiken, Rev PA9, 1996-03-01

Överstyrelsen för civil beredskap initierade under åren 1994–95 projektet ELVIRA, med målet att utveckla ett stödsystem för ledning, planering och samordning inom den civila delen av totalförsvaret. Projektet genomförs i nära samarbete med användarna. Stödsystemet skall användas av personal inom kommuner, länsstyrelser och civilbefälhavarorganisationen. Informationsutbyte mellan dessa samt med försvarsmakten och andra myndigheter skall ske både i ostörda och i störda förhållanden. Systemet är ett datorbaserat informationsbehandlings- och kommunikationssystem som växelverkar med berörda användare och organisationer. Det är därför viktigt att, inom hela totalförsvaret, skapa ett gemensamt koncept på säkerhetslösningar för digitala signaturer, autenticering och kryptering.

I störda förhållanden kommer såväl antalet användare som användningens omfattning att öka väsentligt i totalförsvarets system. De servrar som används för verifiering av signaturer och autenticering bör redan i fred ha tillräcklig kapacitet (hårdvarustöd för RSA-beräkningar) för att kunna fungera i en krissituation.

System för kortavläsning bör vara utformade på ett sådant sätt att de kan läsa kort som är producerade av olika tillverkare och med olika teknik.

Kortutgivning, personalisering av kort, tillverkning av certifikat samt databas för CA-verksamhet måste omfattas av hög säkerhet redan under ostörda förhållanden. I normalfallet bör det finnas två alternativa driftställen, varav ett i skyddat utrymme.

8.3 Begränsning av sårbarheten

För att minimera sårbarheten måste förmågan att fungera säkerställas i de steg som nyttjas för att skapa signaturer. Om utgångspunkten är att digitala signaturer skapas med hjälp av privata och öppna nycklar, som lagras på aktivt kort eller i en dator, måste följande säkerställas.

1. Procedurerna för
- beställning och utlämning av kort,
- tillverkning av kort – fysiska kortet,
- skapandet av kort – chipet,
- skapandet av nycklar,
- produktionen av PIN-kod,
- utlämning av PIN-kod,
- personalisering av kort,
- skapande av certifikat,
- lagringen av certifikat, samt
- kontrollen av certifikat.

2. Katastrofrutiner.

3. Procedurer för att skapa elektroniska dokument, som skall åsättas digitala signaturer.

För att kunna säkerställa det första steget "beställning och utlämning av kort" är det väsentligt att bl.a. följande åtgärder vidtas.

Administrativa åtgärder: Organisation och rutiner måste vara tillgängliga och får inte vara nyckelpersonberoende om verksamheten är beroende av att kunna skapa digitala signaturer. System som medverkar i proceduren måste vara tillgängliga.

Fysiska åtgärder: Utrustning och system måste skyddas.

Logiska åtgärder: Vanliga IT-säkerhetsåtgärder måste vara vidtagna.

För att säkerställa det andra och det tredje steget, "tillverkningen av kort – fysiska kortet" och "skapande av kort – chip", är det väsentligt att bl.a. vidta följande administrativa åtgärder.

- Tillgången på kort måste säkerställas. Kortens kvalitet måste vara tillräcklig.

- Tillgången på chip måste säkerställas. Chipens systemkvalitet måste säkerställas genom användningen av evaluerade produkter.

8.4 Försörjningen av tekniska komponenter

8.4.1 Tillverkning

Produktionsprocessen vid tillverkningen av aktiva kort och kortavläsare skiljer sig inte nämnvärt från annan tillverkning av elektroniska system och kräver inte heller från området avvikande, unik kompetens. De ingående komponenterna i hårdvaran är vanligtvis av PVC- eller ABS-plast för kortkroppen samt ledningsbanor av metall (koppar, guld), vissa kemikalier (i små mängder) med tillhörande elektronikkomponenter för kortläsaren.

Den i kortet integrerade processorn samt minnesdelen är det som kännetecknar det "aktiva" i konceptet. Läsaren består förenklat av ett hölje som innesluter elektronik för avläsning av kortet samt kommunikationskretsar och gränssnitt till dator.

Genom hela kedjan finns det ett större eller mindre antal tillverkare av de nödvändiga rå- och insatsvarorna som krävs för systemet. Prognoser pekar mot att användningen av aktiva kort kommer att bli omfattande vilket leder till en ökad produktionskapacitet. Detta innebär att försörjningen av de ingående rå- och insatsvarorna, i en normalsituation, kommer att vara god.

8.4.2 Insatsvaror, leverantörer/underleverantörer

PVC och ABS är de vanligast förekommande materialen för själva kortstommen. Båda plasterna är mycket vanliga och förekommer i många olika sammanhang på marknaden. PVC kan präglas men ej återvinnas. Tillverkningen av PVC har av miljö- och hälsoskäl ifrågasatts i vissa länder. Förslag på att plasten skall förbjudas finns även. ABS kan återvinnas, men ej präglas.

Chip till aktiva kort tillverkas numera i mycket stora serier. Tillverkningen domineras av amerikanska, tyska och franska företag.

Några viktiga förutsättningar för tillverkning av halvledare är att det finns tillgång till rikligt med rent vatten, seismisk stabil berggrund (tillverkningsprocessen är extremt vibrationskänslig), avbrottsfri och effektstark elkraft samt utbildad personal för produktion och produktutveckling.

8.4.3 Val av leverantör

Leverantörer och underleverantörer samt tredjepartsaktörer bör väljas med en viss omsorg. Det finns till viss del rutiner och rekommendationer för urvalsprocessen. ÖCB kommer under år 1998 att utge en handbok ”*Säkra företagets flöden”* som behandlar vissa av frågeställningarna. Boken tar upp riskaspekter och leveranssäkerhet ur ett företagsperspektiv. Inom totalförsvaret finns en lång erfarenhet av riskbedömningar beträffande leverantörer.

Sverige, EU och övriga världen

Produktion av varor och tjänster sker numera i komplicerade internationella logistikmönster där lönsamheten är styrande. Företag blir i allt högre grad transnationella och arbetar över nationsgränserna. Nationalstaternas möjligheter att påverka företagen i monolateral riktning minskar mer och mer i takt med de multilaterala organens

framväxt och ökade tyngd (exempel på sådana är WTO/GATT, OECD och EU).

Inom EU pågår en del projekt som syftar till att minska beroendet från icke EU-länder. Detta gäller inom såväl högteknologin som andra områden. Inom elektronikområdet har man under lång tid satsat stora pengar för att utveckla en stark och konkurrenskraftig europeisk elektronikindustri. FoU-satsningar som ESPRIT, JESSI och MEDEA har gjorts eller är under utveckling, för att ta några exempel. Dessa projekt kan, om de lyckas, leda till att försörjningssituationen för Sverige generellt underlättas vid internationella kriser.

För svensk del kvarstår det faktum att vi knappast kommer att ha någon produktion av chip och vissa andra viktigare rå- och insatsvaror i Sverige. Vi kommer att vara beroende av en fungerande handel och goda relationer med leverantörer i andra EU-länder som Skottland, Irland, Frankrike samt Japan (Ostasien) och USA. Produktionen av de viktiga chipen styrs i allt väsentligt från USA och Japan.

9 Handikappaspekter

För en person som är äldre eller har ett funktionshinder är inköp, post- och bankärenden ofta ett problem i dag. Anhöriga, grannar eller hemtjänstpersonal måste hjälpa till på olika sätt beroende på funktionshindrets art och grad. Har man exempelvis ett rörelsehinder kan man ha svårt att ta sig till och från butiker och att nå varor vid självbetjäning. En synskadad person kan också ha svårigheter att ta sig till och från butiker och att finna de varor han vill köpa.

Att handla elektroniskt möter för närvarande också svårigheter för en person med funktionshinder, men tekniken kan anpassas och utformas så att handikappet elimineras. Detta öppnar möjligheter för att självständigt och på egen hand botanisera i varusortiment och göra sina inköp. Att på så vis slippa beroendet av andra och att kunna handla när man själv vill och i den takt man vill skulle betyda en höjd livskvalitet.

Att handla elektroniskt är alltså ett värdefullt alternativ för flertalet människor, men för äldre och funktionshindrade kan det vara den enda möjligheten att handla självständigt utan hjälp av andra.

Att avge eller ta emot digitala signaturer är en nyckelfunktion i sammanhanget. Det kan vara enkelt eller svårt beroende på hur tekniken utformas. Ställer signeringen höga krav på användarens fysiska eller mentala förmåga hamnar många utanför. Avgörande är om man måste kunna göra vissa rörelser, måste kunna se och höra, måste komma ihåg en kod osv., eller om signeringen enkelt kan anpassas utifrån vars och ens förmåga.

9.1 Problem

Förutsättningarna för att använda digitala signaturer varierar stort beroende på sammanhang och typ av funktionshinder.

De problem som kan tänkas uppstå rör främst personer med synskada, rörelsehinder, dyslexi och utvecklingsstörning. Men beroende på produktens/tjänstens utformning kan även personer med andra funktionshinder komma att beröras.

I detta sammanhang kan det vara värt att beakta det stora antal personer det är fråga om.

I Sverige finns i dag 600 000 rörelsehindrade mellan 16 och 84 år. Av dessa är 220 000 svårt rörelsehindrade och måste ha hjälp att förflytta sig.

Minst 250 000 personer har så nedsatt hand- eller armfunktion att de har påtagliga problem i det dagliga livet.

Av de ca 175 000 personer mellan 16 och 84 år som är synskadade, är ca 13 000 helt blinda eller har mycket små synrester.

Cirka 780 000 personer mellan 16 och 84 år har nedsatt hörsel. Av dessa är minst 300 000 beroende av hörapparat och ca 14 000 är helt döva.

Ungefär 40 000 personer beräknas ha så svåra tal- och språkskador att de har svårt att göra sig förstådda. Antalet vuxna dyslektiker uppskattas till mellan 300000 och 500 000.

Av ca 400 000 personer med nedsättning i begåvningen har ca 40 000 en betydande utvecklingsstörning.

Av dagens drygt 1,5 miljoner svenskar som är över 65 år är 420 000 personer över 80 år. Funktionsnedsättningarna tilltar med ökad ålder.

Problem uppkommer för synskadade på samma sätt som vid användning av datorsystem i allmänhet, dvs. att läsa på display eller bildskärm, att uppfatta grafiska markeringar eller skrivna instruktioner. Problem kan också finnas vid användning av reglage, kontroller och tangentbord, dvs. problemen rör gränssnittet till såväl mjukvaran som hårdvaran. De problem som är direkt relaterade till datoranvändning finns det lösningar på som involverar punktskriftsdisplayer, syntetiskt tal och förstoringsprogram.

Rörelsehindrades svårigheter gäller räckvidd, åtkomlighet samt krav på rörelser, kraft och precision vid användning av reglage och kontroller.

Dyslektikers problem rör att korrekt uppfatta skriven text samt att skriva rätt kommandon. De problem som är direkt relaterade till datoranvändning finns det lösningar på som involverar syntetiskt tal. Att skriva en kod kan t.ex. kräva att dyslektikern erhåller en verifiering som gör att det går att avgöra om koden är rätt eller fel. Syntetiskt tal kan vara en metod. Av detta förstås behovet av att kunna välja en personlig kod och att uppläsningen kan skyddas från obehörig avlyssning.

Personer med utvecklingsstörning är en mycket heterogen grupp med mycket olika förmågor och möjligheter när det gäller datoranvändning. För dem som kan använda datorer, dvs. lindrigt utvecklingsstörda, är det rimligt att de också skall kunna använda digitala signaturer. Problemen för denna grupp vid datoranvändning klaras huvudsakligen med användning av förenklingar, symboler och talsyntes. Många utvecklingsstörda har en god man eller förvaltare som är inblandad i bl.a. ekonomiska sammanhang. Detta innebär att det för utvecklingsstörda kan finnas behov av digitala signaturer med olika behörighet.

Om speciell hårdvara tas fram för att användas vid digitala signaturer så är det mycket viktigt att alla dessa gruppers behov beaktas.

Stora problem kan uppstå, om dessa grupper alltid måste be om hjälp för att kunna använda digitala signaturer. Förutom de stora sociala och ekonomiska konsekvenser det skulle medföra så finns här också stora säkerhetsproblem, som inte bara berör de funktionshindrade själva. Här finns också legala aspekter bl.a. rörande ansvarfrågor. Om den funktionshindrade tvingas ta hjälp från andra, så finns alltid risken att någon missbrukar detta förtroende eller att personlig information sprids otilbörligt.

9.2 Behov

Gränssnittet för digitala signaturer måste vara sådant att det passar så många som möjligt samt att det ger möjlighet till anpassning efter egna behov. Kontroller, portar, in- och utmatningsenheter etc. skall om möjligt uppfylla standarder. Mjukvaran skall erbjuda alternativa presentationsformer.

Digitala signaturer måste kunna läsas eller tolkas med användning av punktskrift och/eller tal. Att lämna respektive läsa en elektronisk signatur måste kunna göras på ett sätt som är både säkert och möjligt att utföra för alla människor.

För utrustning med reglage, knappar, kontroller eller uttag (för t.ex. aktiva kort) bör gälla bl.a. att de

- skall vara märkta och enkla att identifiera taktilt (markeringen kan alternativt göras intill reglaget etc. för bästa läsbarhet),
- skall utformas så att de inte förväxlas eller aktiveras av misstag,
- skall utformas så att de är enkla att greppa och använda med liten kraft,
- inte får innehålla nickel, krom eller andra allergiframkallande material,
- inte skall kräva färgseende, samt
- skall kunna skötas sekventiellt.

Märkningen bör göras med hjälp av relief på eller i anslutning till utrustningen.

Tecken eller skrift bör vara så stor som möjligt och minst 4 mm., ha god kontrast, samt inte ha rött mot grön botten eller vice versa.

Utrustningen bör vara enkel att ansluta till hjälpmedel. Existerande eller de facto standarder bör följas när det gäller serie- och parallellanslutningar, databussar, tangentbordsanslutningar och

andra dataöverföringsmekanismer samt hörtelefonanslutningar och kortanslutningar.

Krav kan vidare komma att ställas kring den strålning eller det ljus som utrustningen avger, kring den form av information och kommunikation som utrustningen fordrar, kring varningssignalers utformning samt kring möjligheten att använda olika språk. Se vidare Handikappinstitutets skrift ”Serviceautomater som vi vill ha dem”.

10 Handlingsvägar

Efter denna genomgång av tekniska och organisatoriska förutsättningar samt juridiska och andra samhälleliga aspekter med avseende på digitala signaturer kan några huvuddrag för olika handlingsalternativ skönjas.

Kraven som kan ställas på användning av digitala signaturer beror på i vilket sammanhang de skall tillämpas. Skall det ske i öppna nätverk eller i sluten användarkrets? Vilken typ av transaktioner skall de digitala signaturerna användas för och finns några begränsningar för hur pass omfattande eller på annat sätt betydelsefulla sådana transaktioner får vara?

10.1 Överlämna utvecklingen till marknaden

Skillnaden mellan alternativa system och aktörer gör att det inte nödvändigtvis finns något enhetligt svar på om marknaden eller lagstiftaren skall forma regelverk för digitala signaturer. System som PGP som till största delen saknar CA-funktion i den mening som begreppet har här torde ha en klar uppgift att fylla och det kan saknas anledning att införa regleringar för sådan verksamhet. En aspekt som bör beaktas är emellertid också systemens utvecklingsmöjligheter.

I vissa sammanhang torde dock fordras för att system med digitala signaturer skall kunna fungera att allmänhetens förtroende för dem säkerställs. För att skapa tilltro till system för digitala signaturer måste flera faktorer uppfyllas. Först och främst fordras tillförlitlig teknik samt tillförlitlig organisation för identifieringen av certifikatinnehavarna och för hanteringen av nyckelcertifikat och

kataloger m.m. Det finns anledning att tro att marknaden kan klara av att få fram kvalificerade organisationer med tillgång till erforderlig teknik för att klara av att framställa säkra digitala signaturer. Marknaden kan också tänkas lösa frågor som gäller ansvarsfördelning i avtalsmässiga förhållanden mellan CA, nyckelinnehavare och förlitande tredje part. En fråga är dock om allas intressen genom sådana lösningar kommer att tas till vara på ett tillfredsställande sätt. Intresseavvägningar kommer dels att ske genom avtalsskrivning, dels genom domstolarnas praxis, varvid i vissa fall skälighetsavvägningar kan förväntas. Leder en sådan marknadsstyrd utveckling till oskäliga resultat kan civilrättslig lagstiftning till skydd för användare, särskilt konsumenter men i viss uträckning även näringsidkare, aktualiseras. Marknaden kan till viss del även lösa problemet med stora skadefall genom försäkringar och genom att endast mycket stora och solida företag och organisationer erhåller förtroendet att agera CA.

Det kan antas vara svårare för marknaden att lösa frågor om ansvar i icke-avtalsrelaterade förhållanden mellan CA och förlitande tredje part. Dessutom kan det vara osäkert i vilken mån en CA kan friskriva sig från ansvar utan lagstöd. En ännu viktigare fråga som marknaden över huvud taget inte kan klara att lösa på egen hand är att öka tilltron till systemet för digitala signaturer genom att under vissa förutsättningar ge ett missbruk av sådana ett förhöjt straffvärde i förhållande till de mera allmänna brotten som ett sådant förfarande kan utgöra ett led i, t.ex. bedrägeri. Andra frågor som marknaden kan få svårt att klara på egen hand är integritetsfrågor. Vilka uppgifter om en användare och dennes användning av systemet skall en CA få lagra och vilket skydd gäller mot att lämna ut sådana uppgifter till utomstående?

En annan sak som endast en lagstiftare skulle kunna åstadkomma är någon slags presumtionsregel vad gäller tilltron till digitala signaturer under vissa angivna förutsättningar. Om en sådan ordning är eftersträvansvärd med hänsyn till den svenska rättsordningens hittills tämligen väl fungerande principer om var bevisbördan skall placeras kan dock ifrågasättas.

Att ändra principen om fri bevisprövning kan över huvud taget inte vara aktuellt.

Stora initialkostnader för CA-verksamhet och möjligheten att klara stora skadefall kan leda till att endast ett mindre antal företag och organisationer kan tänkas agera CA i sådana system där höga krav på tillit kommer att ställas. För en användare kan detta vara en trygghet. Samtidigt kan detta verka konkurrenshämmande. En aspekt som kan vara värd att ta upp i detta sammanhang är att statligt ägda bolag såsom Posten AB och Telia AB kan erhålla en konkurrensfördel just genom att vara statsägda.

10.2 Lagreglering

Vid utformningen av en eventuell reglering av digitala signaturer bör lagstiftaren ha ett probleminriktat synsätt. Det innebär att lagstiftning endast bör ske i de fall där det behövs och att det för varje problem som kan identifieras inom området skall övervägas om lagstiftning är den lämpligaste lösningen.

En lagreglering rörande digitala signaturer avser skilda delar.

- I första hand gäller det näringsrättslig reglering för att bedriva CA-verksamhet.

- I andra hand gäller det verkan av en digital signatur, dels rättsverkan i fall där formkrav på egenhändigt undertecknande eller egenhändig underskrift eller på skriftlig handling kan hindra användningen av digitala signaturer, dels bevisverkan.

- Därtill kommer viss övrig reglering med anknytning till rättsvårdande myndigheters förutsättningar att bekämpa brott samt till exportkontrollen av strategiska produkter.

10.2.1 Näringsrättslig reglering av CA-verksamhet

Något förslag till näringsrättslig reglering av CA-verksamhet finns inte för närvarande i Sverige. En rad utländska lagstiftningar på detta område finns emellertid. Ett förslag från EG-kommissionen om ett EG-direktiv om digitala signaturer där ett licensieringsförfarande torde utgöra en del kan förväntas inom kort. Direktivet kan enligt det ramverk som utarbetats rörande digitala signaturer och kryptering komma att inriktas antingen enbart på det som här närmast motsvarar en näringsrättslig reglering men kan också innefatta att medlemsstaterna skall samordna sina lagstiftningar på så vis att digitala signaturer skall jämställas med traditionella underskrifter. Det senare alternativet är mycket mera ingripande och kan ta mycket längre tid att genomföra. Å andra sidan framgår av vad som nämnts i avsnittet om internationell privat- och processrätt att en enhetlig lagstiftning i medlemsstaterna skulle förenkla för tillämparna av ett system för digitala signaturer.

En generellt giltig näringsrättslig lagstiftning är t.ex. den som införts i Tyskland. Den tyska modellen går att tillämpa på svenska förhållanden. Den kan ha vissa nackdelar pga. att dess detaljrikedom gör den teknikberoende. Mycket av detaljregleringen har också lagts i förordningen, som är lättare att ändra. En lagstiftning där teknikoberoende särskilt har eftersträvats är den Kaliforniska. Det bör eftersträvas att i vart fall det som regleras i lag är så teknikoberoende som möjligt. Bland anant bör krav på användning av aktiva kort inte lagregleras.

Begränsningar i tillämpningsområdet för digitala signaturer, där formkrav finns kan emellertid göras, t.ex. som avsikten är enligt avdelning I i betänkandet Elektronisk dokumenthantering – att begränsa införandet till myndigheternas ärendehantering. Detta är också ungefärligen vad som har skett i t.ex. viss amerikansk lagstiftning.

Några riktlinjer för en näringsrättslig reglering av CA-verksamhet har getts i avsnittet 7.4

Utredningen om elektroniska pengar har i sitt delbetänkande E-pengar – näringsrättsliga frågor (SOU 1998:14) lämnat övergripande förslag till en näringsrättslig reglering av (system för) elektroniska pengar. I bilaga 3 till delbetänkandet ges en skiss över hur en sådan reglering kan se ut. Mycket av det som där föreslås skulle också kunna äga en motsvarighet i en näringsrättslig lagstiftning för CA-verksamhet i system för digitala signaturer. Vissa skillnader föreligger naturligtvis, eftersom förslaget om e-pengar avser en del av finanssektorn medan CA-verksamhet kan vara en mera övergripande verksamhet som kan sträcka sig över alla samhällssektorerna och därför kan få konsekvenser som är mer svåröverblickbara. Samtidigt som all utgivning av e-pengar kan te sig som så pass kvalificerat samhällsviktig verksamhet att det skall erfordras tillstånd för att bedriva den är det inte säkert att detta behöver vara fallet beträffande CA-verksamhet. Slutligen görs i anslutning till skissen i bilaga 3 till delbetänkandet om e-pengar ett konstaterande om att frågor om normgivningskompetens behöver belysas. Motsvarande gäller också vid en reglering av CA-verksamhet, eftersom det i så fall torde bli fråga om en avvägning mellan hur mycket som skall regleras i lag respektive i förordning eller föreskrift.

En näringsrättslig reglering av CA-verksamhet kan också kopplas till rättsverkan (och bevisverkan) för digitala signaturer på så vis att det t.ex. endast är digitala signaturer som framställts med stöd av nyckelcertifikat utfärdade av en CA som har tillstånd enligt näringsrättslig lagstiftning som åtnjuter ett förhöjt straffvärde i händelse av missbruk, som får användas enligt förvaltningslagen etc.

10.2.2 Verkan av digitala signaturer

Rättsverkan av digital signatur

Den första fråga som kan ställas är om en digital signatur – om den uppfyller en viss säkerhetsnivå – generellt skall ges samma rättsverkan som en egenhändig underskrift. Det finns en fördel med en

lagstiftningsmetod som har en sådan innebörd. Alla de lagar och föreskrifter som innehåller krav på underskrift kan på en gång fås att omfattas av användning av digitala signaturer genom en lagregel om jämställande med underskrift. Å andra sidan kan införandet av en sådan lagregel i ett skede där tekniken inte har prövats i större skala i öppna nätverk i transaktioner av alla möjliga slag få oanade konsekvenser.

Mot bakgrund av bl.a. de olika skälen bakom formkraven i olika författningar torde en generellt verkande reglering innebärande att digitala signaturer godtas i stället för egenhändiga namnteckningar över hela rättsområdet inte vara möjlig.

När det gäller rättsverkan av digital signatur har lagstiftning redan genomförts på en rad områden där elektroniska dokument godtas i stället för egenhändigt underskrivna handlingar. Dessa lagar inom förvaltningsrätten har alla det gemensamt att den myndighet som skall tillämpa lagen också har ett inflytande över tillämpningen av reglerna om elektronisk dokumenthantering och myndigheten kan ge närmare anvisningar om hur hanteringen skall gå till. Ytterst kan myndigheten fordra att skriftliga undertecknade handlingar skall lämnas. Även om regleringarna är snarlika förekommer avvikelser som leder till att vad som gäller för en myndighet inte automatiskt kan appliceras på en annan myndighet för vilken annan lagstiftning är tillämplig.

Förslag till generellt tillämplig reglering beträffande digitala signaturer finns i Datastraffrättsutredningens betänkande (SOU 1992:110) såvitt avser straffrätten. I förslagen till ändring av brottsbalken föreslås definitioner av dokument som innefattar, utöver skriftliga originalhandlingar, en bestämd mängd data för automatisk informationsbehandling, om det är möjligt att fastställa att innehållet härrör från den som framstår som utställare. Genom användning av digital signatur kan enligt förslaget ett sådant dokument skapas. Några regler om vilka närmare krav en digital signatur skall uppfylla för att dokumentbegreppet skall bli uppfyllt ges inte i förslaget. Det standardiseringsarbete som försiggår beträffande digitala signaturer omnämns. Samtidigt klargörs dock att även icke standardiserade digitala signaturer kan medföra att

sådan digital signatur föreligger som kan medföra att dokumentkravet i förslaget till ny 14 kap. 1 § BrB om dokumentförfalskning eller att kravet på signatur enligt förslaget till ny 14 kap. 9 § BrB om signaturförfalskning är uppfyllda.

Ett förslag till generell lagstiftning inom förvaltningsrätten finns också i betänkandet Elektronisk dokumenthantering. Däri föreslås att en rad definitioner intas i 1 a § förvaltningslagen, däribland den om digital signatur – 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. Inte heller här föreslås några närmare regler för vilka närmare krav som skall vara uppfyllda för att en digital signatur skall anses föreligga. Myndigheterna skall enligt förslaget ha kvar möjligheten att begära att ett meddelande som saknar avsändarens underskrift i original bekräftas av avsändaren genom en i original undertecknad handling. Förslaget begränsas till myndigheternas ärendehantering. Domstolarnas dömande verksamhet undantas t.ex. Enligt förslaget skall regeringen beträffande sådana förfaranderegler som återfinns i andra lagar än i förvaltningslagen och som därför enligt 3 § förvaltningslagen äger företräde framför sistnämnda lag, ha rätt att bemyndiga berörda myndigheter att föreskriva att krav på traditionella skriftliga rutiner får uppfyllas elektroniskt. Hittills har utvecklingen i denna del av förslaget, som ovan nämnts, i stället skett genom att ändringar har gjorts i de särskilda lagar som gäller för varje särskilt ämnesområde.

Bevisverkan av digital signatur

I fråga om bevisverkan torde det för lagstiftaren enbart röra sig om att kunna uppställa bevisbörderegler, t.ex. vid förnekande av en digital signatur. Något skäl att i fråga om digitala signaturer avvika från de bevisregler som tillämpas i övrigt kan knappast sägas föreligga. Det förefaller därför inte ändamålsenligt att uppställa särskilda bevisbörderegler som avviker från vad som i dag gäller vid förfalskningsinvändningar. Någon lagreglering bör alltså inte göras

beträffande bevisbördan. De fördelar som i bevishänseende kan uppnås genom strukturerade förfaranden för att åstadkomma digitala signaturer med en angiven säkerhetsnivå kan likväl bli betydande. Av betydelse ur bevishänseende är särskilt i vad mån systemen är reviderbara för det enskilda fall där t.ex. äktheten hos en digital signatur sätts i fråga.

10.2.3 Övrig reglering

Digitala signaturer är avsedda för att säkra utställarens identitet och det mottagna meddelandets autenticitet – inte för att skapa konfidentialitet. Det går dock inte att bortse från att metoderna för att säkra identitet och autenticitet respektive konfidentialitet grundas på samma tekniska förfarande. En eventuell reglering av digitala signaturer kan därmed komma att bli beroende av hur en policy för konfidentialitetskryptering utformas.

Frågan om konfidentialitetskryptering är komplicerad, och det torde dröja innan Sverige och andra länder enats om nationella policies. För att inte detta dröjsmål skall utgöra ett hinder för användningen av digitala signaturer bör de båda funktionerna tills vidare separeras. En separat hantering av signatur- och konfidentialitetsfunktioner är också den inriktning som den internationella regleringen för närvarande har (jfr. Tyskland).

I avsnittet 2.4 har redogjorts för att det torde gå att tillgodose såväl krav på integritet för innehavare av signaturnycklar på så vis att extern nyckeldeponering inte skall behöva förekomma för digitala signatur-system samtidigt som polisens och andra brottsutredande myndigheters behov av att kunna avlyssna teletrafik inte motverkas. Användningen av nycklarna för digitala signaturer kan begränsas genom tekniska förfaranden varigenom signaturnycklar inte skall kunna användas för konfidentialitetskryptering av meddelanden.

Som beskrivs i avsnitt 2.4 går det dock troligen inte att till 100 procent skydda sig mot att nycklar används på felaktigt sätt. De tekniska förfarandena kan därför behöva kompletteras med särskilda regler för användningen, t.ex. ett uttryckligt förbud mot

användning av signaturnycklar för konfidentialitetskryptering, samt tydliga krav på CA att tillhandahålla separata certifikat och nyckelpar för respektive användningsområde. En möjlig åtgärd är att knyta nyckelanvändning till ansvarsregler.

I övervägandena kring hur omfattande krav som skall ställas på teknik och användning i syfte att bekämpa brott måste en avvägning göras mellan det samhällsekonomiska värdet av en effektiv brottsbekämpning och de samhällsekonomiska kostnaderna i form av dyrare teknik och minskad flexibilitet för användarna.

Reglerna för export och utförsel av varor med dubbla användningsområden, s.k. strategiska produkter, och deras betydelse för användning av digitala signaturer måste studeras. Samma överväganden som ovan avseende tekniska möjligheter att förhindra felaktig användning av signaturnycklar måste göras även här.

Bilaga 1

Kryptering respektive signering med RSA-teknik och ett alternativ till RSA.

RSA-algoritmen

Låt m vara ett digitalt meddelande, dvs. en ändlig sekvens av ettor och nollor, m kan då tolkas som ett heltal skrivet på binär form. Antag vidare att m som heltal är mindre än heltalet n. Då kan m RSA-krypteras genom

$$m^1 = m\text{^}e \pmod{n},$$

där e kallas exponent och talet n kallas modul. Operationen består av en vanlig potentiering, dvs. m upphöjs till e, följt av subtraktion av den största multipeln av n, som är mindre än m^e. Resultatet kommer således att ligga i intervallet mellan 0 och n.

Ett exempel med små tal:

*Låt n = 55, e = 3 och m = 12. Då erhålles: 12 à 12^3 (mod. 55) = 1728 (mod. 55) = 1728 – 31*55 = 23. Paret (55,3) får representera en öppen RSA-nyckel i detta exempel.*

Motsvarande dekryptering utgörs av modulär potentiering med en annan exponent, d. Värdet av d kan bestämmas effektivt om man känner eller kan beräkna primtalsfaktorerna i n, annars saknas praktisk möjlighet att beräkna d. Därav följer att RSA-systemets säkerhet beror på svårigheten att faktorisera stora heltal.

Fortsättning på exemplet:

Med d = 7 transformeras värdet 23 tillbaka till 12 enligt följande: 23^7 (mod. 55) = 3404825447 (mod. 55) =12. Valet av d = 7 beror här endast på n och e, som är 55 respektive 3, och är oberoende av valet av m. Talet d = 7 representerar den hemliga RSA-nyckeln som korresponderar till den öppna nyckeln (55,3).

Digitala signaturer med RSA – samt redundans- och hashfunktioner

En ren RSA-transformation har formen: m^e (mod. n). Av flera skäl tillämpas inte rena RSA-transformationer direkt för digital signering. Ett viktigt skäl är möjligheten att en förfalskare av signaturer skulle kunna utnyttja ett antal gjorda signaturer för att framställa en korrekt signatur på ett nytt meddelande utan att ha tillgång till den privata hemliga signeringsnyckeln.

Den speciella formen för en ren RSA-signatur medför nämligen att man från signaturerna på meddelandena m1 och m2 lätt kan beräkna signaturen på m1*m2 (mod. n). Normalt ger ju inte den modulära produkten av två meddelanden något vettigt meddelande, men i många sammanhang är risken stor att en angripare kan åstadkomma en användbar attack baserat på denna princip, om inte något görs för att förhindra detta.

Två metoder används allmänt för att förstärka säkerheten hos RSA-baserade signaturer. Den ena består i att endast tillåta meddelanden av en viss speciell form som matematiskt utesluter att den ovannämnda typen av multiplikativa samband kan uppstå mellan tillåtna meddelanden. Vid verifiering av en signatur måste då kontroll också ske av att det signerade meddelandet har tillåten form. Praktiskt definieras den tillåtna meddelandeformen genom att en viss typ av redundans tillförs meddelanden på ett sätt som både kan genereras och kontrolleras helt automatiskt av en dator. Låt r vara den funktion som överför ett godtyckligt meddelande, m, till ett meddelande med erforderlig redundans, r(m). Signaturen på m

erhålles då genom att RSA-transformationen, S, baserad på den privata signaturnyckeln, tillämpas på det tillåtna r(m); dvs. signaturen på m är S(r(m)).

(Observera att funktionen r expanderar meddelandet så att r(m) är längre än m. Därför måste m vara kortare än RSA-modullängden för S för att man skall kunna bilda S(r(m))!)

Den andra metoden för att förhindra att kända RSA-signaturer från en viss användare kan utnyttjas för att skapa nya signaturer utan användning av den privata signaturnyckeln är att alltid först transformera meddelandet med hjälp av vad som kallas en enkelriktad kollisionsfri hashfunktion, h,. Därefter tillämpas den rena RSA-transformationen, S, på hashvärdet. Signaturen på m blir således S(h(m)).

En enkelriktad hashfunktion, h, har egenskapen att det för ett godtyckligt givet värde y är praktiskt omöjligt att finna ett meddelande, m, sådant att h(m) = y. Det enda sättet att finna par (m,h(m)) är således att först välja m:et i paret och beräkna h(m). Kollisionsfrihet innebär att det dessutom är omöjligt att välja två meddelanden m1 och m2 med sammanfallande hashvärden: h(m1) = h(m2). Om man dessutom förutsätter att h bryter eventuella multiplikativa samband mellan meddelanden, så förhindras en angripare att utnyttja multiplikativiteten hos RSA för att beräkna signaturer på formen S(h(m)).

Tekniken med enkelriktade hashfunktioner är också användbar för att effektivisera signering av långa meddelanden. Om man vill använda ren RSA på ett meddelande, m, som binärt representerar ett heltal som är större än n så får man dela upp m i block som representerar värden som är mindre än n, och tillämpa RSA-transformering på varje block för sig. Med en enkelriktad hashfunktion kan man komprimera ett godtyckligt långt meddelande till en storlek som kan hanteras med en enda RSA-transformation.

Om digitala signaturer baserade på RSA i kombination med en redundans- och/eller hashfunktion enligt ovan implementeras i dedikerad maskinvara (t.ex. ett smart kort) som ger ett fysiskt skydd mot förändring av den inprogrammerade logiken, så förhindras användaren att utnyttja signaturfunktionen för krypteringsändamål.

Antag att någon skickar ett meddelande, m, som RSA-krypterats med en öppen nyckel som används för verifiering av signaturer. Betckna detta kryptogram V(m). Låt S vara RSA-transformationen som görs med motsvarande privata signeringsnyckel. Dessa RSA-transformationer uppfyller: S(V(m)) = m. Det vill säga den som känner den privata nyckeln, eller har tillgång till en maskin som gör en ren RSA-transformation med hjälp av denna nyckel kan dekryptera V(m). Men, om maskinen som utför transformationen S först förändrar V(m) till r(V(m)) eller h(V(m)), så ställer det sig helt annorlunda. I det senare fallet gäller att eftersom h är en enkelriktad funktion så har man förlorat all information om ingångsvärdet V(m) och därmed om m, när V(m) ersatts med h(V(m)). I fallet med en redundansfunktion så kan S inte operera på r(V(m)), om detta överhuvudtaget är definierat, eftersom redan V(m) fyller ut den blockstorlek som S är definierad för.

Slutsatsen är således att om man vill förhindra att en infrastruktur för digitala signaturer baserade på RSA-systemet direkt kan utnyttjas för kryptering, så räcker det att paketera signeringsfunktionen i icke-manipulerbar maskinvara, t.ex. smarta kort, på ett sådant sätt att signeringsoperationen utgör en odelbar kombination av en förbehandling av indata i form av en redundansfunktion (t.ex. enligt ISO 9796, jfr SEIS-specifikationerna) eller en enkelriktad hashfunktion, samt en ren RSA-transformation för vilken nyckeln endast finns tillgänglig inuti den skyddade maskinvaran och således är oåtkomlig för andra processer än de som utförs internt i denna enligt dess certifierade program.

Nycklar och nyckelcertifikat för digitala signaturer respektive sekretessändamål kan följaktligen användas och administreras helt oberoende av varandra. Detta gäller även om de bärs i samma smarta kort.

Alternativ till RSA för signering

Det har utvecklats ett antal system för digitala signaturer som alternativ till RSA. De mest användbara av dessa skiljer sig från RSA genom att de inte direkt bygger på en krypteringsmetod. Den gemensamma egenskapen för alla digitala signatursystem, som gör dem värda namnet, är att det krävs tillgång till en hemlig privat nyckel för processen att skapa en signatur och att denna kan verifieras med hjälp av en öppen nyckel. Dessa nycklar är då inte att betrakta som krypteringsnycklar, utan som signaturnycklar; signeringsnyckel respektive verifieringsnyckel. Signaturen skapas då som en checksumma på meddelandet på liknande sätt som ett enkelriktat hashvärde. Vid checksummeberäkningen utnyttjas den privata nyckeln. Checksumman, dvs. signaturen, kommer genom beräkningens konstruktion att uppfylla en ekvation som inbegriper meddelandet och den öppna nyckeln. Denna ekvation har egenskapen att det är praktiskt omöjligt att lösa den utan att använda den hemliga nyckeln för att räkna ut lösningen.

System av denna typ framställer signaturer med hjälp av äkta enkelriktade funktioner utan lönndörrar till skillnad från RSA som utnyttjar enkelriktade funktioner med lönndörrar (”trap-door one-way functions”).

Det har däremot visat sig att man med dessa metoder ändå kan behöva gardera sig mot dolda, s.k. subliminala kanaler för sekretesskydd av meddelanden. Det är även här viktigt att se upp med hur nyckelgenereringen går till för att systemen i alla avseenden skall fungera som man tänkt sig.

Bilaga 2

Elektroniska ID-kort och mjuka elektroniska certifikat

Detta avsnitt beskriver hur processen för att ge ut elektroniska ID-kort och mjuka elektroniska ID-certifikat kan utformas. Detta är endast en exemplifiering av ett regelverk.

Elektroniska ID-kort

Det elektroniska ID-kortet ger hög säkerhet eftersom den privata (hemliga) nyckeln lagras på kortet. Eftersom nyckeln inte kan kopieras eller eljest göras tillgänglig finns det bara en enda originalnyckel och inga kopior. Detta betyder att nyckeln aldrig lagras på hårddisk eller diskett där det är lättare för obehöriga att komma över densamma. Certifikatet kan lagras på kortet och/eller publiceras i en katalog. Därtill kommer att personaliseringen av kortet kan ske under strikta former.

Nedan beskrivs ett såväl elektroniskt som visuellt ID-kort. Elektroniska ID-kort kan också utfärdas utan något visuellt ID, dvs. kortet är blankt eller har annan information tryckt på kortet.

Beställning av ett elektroniskt ID-kort görs enligt följande.

- Beställaren identifieras med hjälp av godkänd ID-handling (saknas godkänd ID-handling görs speciell utredning).

- Foto tas emot och kontrolleras.

- Den sammanställda beställningen läggs i förseglat kuvert och levereras i skyddad transport till kortproduktionen.

För generering av nycklar utifrån ett råkort gäller följande.

- Nyckelpar genereras.
- Den privata nyckeln säkras genom inläggning i det aktiva kortet (smarta kortet).
- En PIN-kod genereras för åtkomst till kortet.

Certifikatgenerering görs enligt följande.

- Identitetsinformation från beställningen registreras i dokumentet.
- Den publika nyckeln i dokumentet registreras.
- Namn på utfärdande CA läggs i dokumentet.
- Pekare till den katalog som lagrar (publicerar) certifikat och spärrar registreras.
- Giltighetstid läggs in.
- Dokumentet signeras med CA:s privata nyckel.

Det signerade dokumentet är beställarens certifikat.

Personalisering av kortet görs enligt följande.

- Certifikatet lagras elektroniskt i kortet.
- Beställarens foto/identitetsinformation graveras på kortet.
- PIN-koden för kortet skickas separat till beställaren.
- Kortet levereras i säker leverans till utlämningsstället.

Certifikaten publiceras i en katalog så att den som önskar skicka säker e-post till innehavaren kan hämta den publika nyckeln där.

För kortproduktionen innebär det att certifikatet läggs upp i katalogen. På utlämningsstället lämnas meddelande att kort finns att hämta. Beställarens identitet verifieras och om allt är riktigt lämnas kortet ut till beställaren.

Mjuka ID certifikat - användargenererade nycklar

Den privata nyckeln lagras i krypterad form på en diskett eller hårddisk. Certifikatet kan lagras på disk och/eller publiceras i en katalog.

Användargenererade nycklar betyder att användaren utnyttjar lokal programvara i sin dator för att skapa nyckelparet. Användaren lämnar då aldrig ifrån sig den privata nyckeln. Detta betyder att användaren svarar för att nyckelgeneratorn uppfyller uppställda krav. CA kan skaffa kontroll genom att enbart acceptera publika nycklar som bevisligen genererats med hjälp av godkända algoritmer i kontrollerade nyckelgeneratorer. Användargenererade nycklar är förhärskande i dagens Internet-lösningar.

Generering av nycklar sker enligt följande (ett unikt nyckelpar skall produceras).

- Användaren genererar ett nyckelpar och sparar den privata nyckeln på ett säkert sätt.

- Användaren lämnar den publika nyckeln tillsammans med övrig certifikatinformation till CA för generering av ett certifikat.

Beställning av certifikat: Beställaren identifieras med hjälp av godkänd ID-handling (saknas godkänd ID-handling görs speciell utredning)

Certifikatgenerering görs enligt följande.

- Identitetsinformation från beställningen i dokumentet registreras.
- Den publika nyckeln registreras i dokumentet.
- Namn på utfärdande CA läggs i dokumentet.
- Pekare till den katalog som lagrar (publicerar) certifikat och spärrar registreras.
- Giltighetstid läggs in.
- Dokumentet signeras med CA:s privata nyckel.

Det signerade dokumentet är beställarens certifikat.

Certifikaten publiceras i en katalog så att den som önskar skicka säker e-post till innehavaren kan hämta den publika nyckeln där. För kortproduktionen innebär det att certifikatet läggs upp i katalogen. Beträffande utlämning av certifikat gäller följande: När beställningar tas emot meddelas att certifikatet finns att hämta. Beställarens identitet verifieras vid utlämning.

Mjuka ID certifikat - CA genererade nycklar

Den privata nyckeln lagras i krypterad form på en diskett eller hårddisk. Certifikatet kan lagras på disk och/eller publiceras i en katalog.

CA-genererade nycklar innebär att CA har kontroll över algoritmer och programvaror som skapar nyckelparen. Ett extra moment tillkommer för att leverera den privata nyckeln på ett säkert sätt till användaren.

Beställning av certifikat sker på samma sätt som vid användargenererade nycklar.

Generering av nycklar sker enligt följande (ett unikt nyckelpar skall produceras).

– Nyckelpar genereras.

– Nycklarna lagras på magnetmedium, den privata lagras i krypterad form.

Certifikatgenerering, publicering och kortproduktion sker på samma sätt som vid användargenererade nycklar.

Vid utlämning av certifikat meddelas att den privata nyckeln och tillhörande certifikat finns att hämta. Beställarens identitet verifieras vid utlämning av nyckel och certifikat.

Spärrning av certifikat

Om beställaren tappar sitt kort eller röjer nyckeln till sitt mjuka certifikat måste motsvarande certifikat spärras.

Kundtjänsten hanterar spärrning av certifikat enligt följande.

– Innehavaren (beställaren) kontaktar kundtjänsten hos den CA som utfärdat certifikatet och begär spärrning.

– Kundtjänsten förvissar sig om att det är innehavaren som begär spärrningen.

Certifikatet förs upp på spärrlista i den katalog där certifikatet är lagrat.

Ovanstående redogörelse visar de viktigaste delarna som ingår i produktionsprocessen. Vissa delar i processen kan utföras parallellt och de behöver inte heller komma i exakt samma ordning som ovan beskrivits.

Bilaga 3

Författningar med krav på underskrift

Nedanstående lista på författningar med krav om underskrift härrör från sökning i Riksdagens databas över författningar i fulltext (SFST).[101] Sökning har gjorts på sökorden ”underskriv-”, ”underskrif-” samt ”underteck-”.

Aktiebolagsförordning (1975:1387)
Aktiebolagslag (1975:1385)
Arvs- och gåvoskatteförordning (1958:563)
Bankaktiebolagslag (1987:618)
Bankrörelseförordning (1987:6479
Bankrörelselag (1987:617)
Bilskrotningsförordning (1975:348)
Biskopsvalsförordning (1965:486)
Bokföringsförordning (1979:1212)
Bokföringslag (1976:125)
Bostadsrättsförordning (1991:630)
Checklag (1932:131)
Datalag (1973:289)
Fartygsregisterförordning (1975:927)
Fastighetsbildningskungörelse (1971:762)
Fastighetsbildningslag (1970:988)
Fastighetstaxeringslag (1979:1152)
Firmalag (1974:156)
Frihandelsförordning (1987:1185)
Förmynderskapsförordning (1995:379)
Förordning (1970:517) om rättsväsendets informationssystem

[101] SFST finns tillgänglig bland Riksdagens databaser (RIXLEX) på http://rixlex.riksdagen.se/

Förordning (1975:1) om protokoll och expeditioner i regeringsärenden m.m.
Förordning (1975:520) om protokollföring m.m. vid arrendenämnd och hyresnämnd
Förordning (1975:932) med dispaschörinstruktion
Förordning (1979:575) om protokollföring m.m. vid de allmänna förvaltningsdomstolarna
Förordning (1980:803) om regionalpolitiskt transportbidrag
Förordning (1980:849) om tillämpning av GATT-överenskommelsen om statlig upphandling
Förordning (1982:3306) om vissa bestämmelser om utlämning för brott till Sverige
Förordning (1982:58) om förfarandet vid utlämning för brott till Danmark, Finland, Island och Norge
Förordning (1982:805) om ersättning av allmänna medel till vittnen, m.m.
Förordning (1983:1031) om särskilt vuxenstudiestöd för arbetslösa
Förordning (1984:463) om avgifter i ärenden om närradio
Förordning (1985:454) om buss- och taxivärderingsnämnden
Förordning (1985:804) om företagshypotek
Förordning (1986:172) om luftfartygsregistret m.m.
Förordning (1987:978) om ekonomiska föreningar
Förordning (1988:1043) med instruktion för de lokala värderingsnämnderna
Förordning (1988:519) med instruktion för Oljekrisnämnden
Förordning (1992:308) om utländska filialer m.m.
Förordning (1993:1091) om assistansersättning
Förordning (1994:2048) med instruktion för Alkoholsortimentnämnden
Förordning (1994:361) om mottagande av asylsökande m.fl.
Förordning (1995:1145) om redovisning av nätverksamhet
Förordning (1995:239) om förmåner till totalförsvarspliktiga
Förordning (1995:667) om bidrag till vissa funktionshindrade elever i gymnasieskolan
Förordning (1995:868) med instruktion för Konsumentverket
Förordning (1995:938) om utbildningsbidrag för doktorander

Förordning (1996:1559) om statligt bidrag till svensk sjöfart
Förordning (1996:1654) om särskilt utbildningsbidrag
Förordning (1996:271) om mål och ärenden i allmän domstol
Förordning (1996:882) om myndigheters årsredovisning m.m.
Förordning (1996:971) om farligt avfall
Försäkringsrörelseförordning (1982:790)
Försäkringsrörelselag (1982:713)
Förundersökningskungörelse (1947:948)
Förvaltningslag (1986:233)
Förvaltningsprocesslag (1971:291)
Gravationsbeviskungörelse (1971:719)
Grundskoleförordning (1994:1194)
Handelsregisterförordning (1974:188)
Hyresförhandlingslag (1978:304)
Inskrivningsregisterkungörelse (1974:1061)
Jordabalk (1970:994)
Kommunalförbundslag (1985:894)
Konkurslag (1987:672)
Konsumentkreditlag (1992:830)
Kungl. Maj:ts instruktion (1918:1080) för kungl. och Hvitfeldtska stipendieinrättningen
Kungörelse (1917:250) angående ströängars utbytande mot annan mark
Kungörelse (1924:423) angående anmälan om återvinnande av svenskt medborgarskap
Kungörelse (1925:465) med särskilda bestämmelser om utförsel från riket av spritdrycker och vin
Kungörelse (1944:285) med tillämpningföreskrifter till lagen den 24 mars 1944 (nr 133) om kastrering
Kungörelse (1950:516) om fastighetsregister för stad enligt lösbladssystem
Kungörelse (1955:630) med närmare föreskrifter om inskrivningsbok för luftfartyg m.m.
Kungörelse (1962:394) med vissa bestämmelser rörande ansökan om pension enligt lagen om allmän försäkring m.m.

Kungörelse (1971:784) med tillämpningsföreskrifter för inskrivningsväsendet enligt jordabalken
Kungörelse (1974:1063) om fastighetsbevis m.m.
Kungörelse (1974:153) om beslutad ny riksdagsordning
Kyrkolag (1992:300)
Körkortsförordning (1977:722)
Lag (1845:50 s. 1) om handel med lösören, som köparen låter i säljarens vård kvarbliva
Lag (1898:64 s. 10) om boskillnad
Lag (1915:218) om avtal och andra rättshandlingar på förmögenhetsrättens område
Lag (1919:426) om flottning i allmän flottled
Lag (1929:145) om skiljemän
Lag (1933:269) om ägofred
Lag (1936:81) om skuldebrev
Lag (1937:73) om befordran med luftfartyg
Lag (1952:166) om häradsallmänningar
Lag (1962:381) om allmän försäkring
Lag (1963:197) om allmänt kriminalregister
Lag (1969:200) om uttagande av utländsk tull, annan skatt, avgift eller pålaga
Lag (1973:1150) om förvaltning av samfälligheter
Lag (1973:188) om arrendenämnder och hyresnämnder
Lag (1974:202) om beräkning av strafftid m.m.
Lag (1974:371) om rättegången i arbetstvister
Lag (1974:610) om inrikes vägtransport
Lag (1975:1132) om förvärv av hyresfastighet m.m.
Lag (1977:595) om erkännande och verkställighet av nordiska domar på privaträttens område
Lag (1978:599) om avbetalningsköp mellan näringsidkare m.fl.
Lag (1980:1103) om årsredovisning m.m. i vissa företag
Lag (1982:352) om rätt till fastighetsförvärv för ombildning till bostadsrätt
Lag (1984:151) om punktskatter och prisregleringsavgifter
Lag (1984:463) om avgifter i ärenden om närradio
Lag (1984:668) om uppbörd av socialavgifter från arbetsgivare

Lag (1985:658) om arrendatorers rätt att förvärva arrendestället
Lag (1987:232) om sambors gemensamma hem
Lag (1987:667) om ekonomiska föreningar
Lag (1989:31) om förvaltning av vissa samägda jordbruksfastigheter
Lag (1990:746) om betalningsföreläggande och handräckning
Lag (1991:1351) om handelsagentur
Lag (1992:1528) om offentlig upphandling
Lag (1993:1392) om pliktexemplar av dokument
Lag (1994:1563) om tobaksskatt
Lag (1994:1564) om alkoholskatt
Lag (1994:1776) om skatt på energi
Lag (1994:243) om Allmänna arvsfonden
Lag (1994:308) om bostadstillägg till pensionärer
Lag (1994:566) om lokal försöksverksamhet med finansiell samordning mellan socialförsäkring, hälso- och sjukvård och socialtjänst
Lag (1994:954) om disciplinpåföljd m.m. på hälso- och sjukvårdens område
Lag (1995:1559) om årsredovisning i kreditinstitut och värdepappersbolag
Lag (1995:1560) om årsredovisning i försäkringsföretag
Lag (1995:1570) om medlemsbanker
Lag (1995:528) om revisorer
Lag (1996:242) om domstolsärenden
Lag (1996:764) om företagsrekonstruktion
Lag (1997:218) om konsumentskydd vid avtal om tidsdelat boende
Lag (1997:239) om arbetslöshetskassor
Lag (1952:167) om allmänningsskogar i Norrland och Dalarna
Lag (1967:531) om tryggande av pensionsutfästelse m.m.
Lag (1975:55) om folk- och bostadsräkning år 1975
Luftfartslag (1957:297)
Mervärdesskattelag (1994:200)
Mönsterskyddsförordning (1970:486)
Mönsterskyddslag (1970:485)
Oljekrislag (1975:197)

Patentkungörelse (1967:838)
Rennäringslag (1971:437)
Resolution (1829:49 s. 269) angående stadfästelse å en, af prosten Siwertsons aflidna syster gjord, donation till stipendiifond wid Kongelfs skola
Rättegångsbalk (1942:740)
Sameskolförordning (1995:205)
Skattebetalningslag (1997:483)
Skuldsaneringslag (1994:334)
Sparbankslag (1987:619)
Stiftelselag (1994:1220)
Studiestödsförordning (1973:418)
Särskoleförordning (1995:206)
Taxeringsförordning (1990:1236)
Taxeringslag (1990:324)
Uppbördslag (1953:272)
Utsökningsbalk (1981:774)
Utsökningsförordning (1981:981)
Varumärkesförordning (1960:648)
Vattenrättsförordning (1983:788)
Växellag (1932:130)
Växtförädlarrättsförordning (1997:383)
Växtförädlarrättslag (1971:392)
Yrkestrafikförordning (1988:1503)
Årsredovisningslag (1995:1554)
Äktenskapsbalk (1987:230)
Ärvdabalk (1958:637)

Bilaga 4

Författningsförslag i betänkandet Elektronisk dokumenthantering, SOU 1996:40

Utredningen SOU 1996:40 Elektronisk dokumenthantering har föreslagit ett antal författningsändringar i bl.a. förvaltningslagen, rättegångsbalken, delgivningslagen, förvaltningsprocesslagen och sekretesslagen. Nedan anges de förslag till författningsändringar i utredningen *som är av direkt betydelse för digitala signaturer.*

Förslag till lag om ändring i förvaltningslagen (1986:223)

Utredningen föreslår bl.a. att följande tre nya paragrafer förs in.

1 a §
I denna lag avses med

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

digitalt dokument: en elektronisk handling med digital signatur eller digital stämpel,

digital signatur: 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, samt

digital stämpel: resultatet av en omvandling av en elektronisk handling som gör det möjligt att kontrollera om innehållet härrör från den juridiska person eller myndighet som framstår som utställare.

7 a §
Om en bestämmelse om handläggning av förvaltningsärenden i en annan lag föreskriver att handlingar skall vara egenhändigt undertecknade eller om den föreskriver något annat som medför att elektroniska handlingar inte kan användas, får regeringen föreskriva att digitala dokument eller, när det kan anses tillräckligt, elektroniska handlingar utan digital signatur eller stämpel får användas.

10 b §
Om det behövs får myndigheten begära att ett meddelande som saknar avsändarens underskrift i original bekräftas av avsändaren genom en i original undertecknad handling. Har myndigheten begärt en sådan bekräftelse men inte fått någon, får myndigheten bortse från meddelandet.

Förslag till lag om ändring i rättegångsbalken

Utredningen föreslår bl.a följande nya paragraf i 33 kap. rättegångsbalken.

3 b §
Om det behövs får rätten begära att ett meddelande som saknar avsändarens underskrift i original bekräftas av avsändaren genom en i original undertecknad handling. Har rätten begärt en sådan bekräftelse men inte fått någon, får rätten bortse från meddelandet.

Förslag till lag om ändring i delgivningslagen (1970:428)

Utredningen föreslår bl.a. att en ny paragraf, 1 a, förs in samt att 6 § skall ha en ny lydelse (förändringar markerade med kursiv text).

1 a §
I denna lag har begreppen elektronisk handling, digital signatur och digital stämpel samma betydelse som i 1 a § förvaltningslagen (1986:223).

6 §
Vid delgivning överbringas handlingen i original eller styrkt kopia. En kopia som har framställts vid en myndighet behöver inte bestyrkas. *När det kan ske skall myndigheten förse elektroniska handlingar med digital signatur eller stämpel*

Är handling som skall delges av vidlyftig beskaffenhet eller är det av annan anledning ej lämpligt att handlingen mångfaldigas, får myndigheten besluta, att handlingen i stället skall hållas tillgänglig hos myndigheten eller på plats, som myndigheten bestämmer. Meddelande därom och om den tid, under vilken handlingen hålles tillgänglig, delges den sökte.

Andra stycket gäller *inte* delgivning av stämningsansökan eller annan handling, *genom vilken förfarandet vid myndigheten inleds*. I fråga om bilaga till sådan handling får andra stycket dock tillämpas.

Förslag till lag om ändring i förvaltningsprocesslagen (1971:291)

Utredningen föreslår bl.a. en ny paragraf, med följande lydelse.

44 b §
Om det behövs får rätten begära att ett meddelande som saknar avsändarens underskrift i original bekräftas av avsändaren genom en i original undertecknad handling. Har rätten begärt en sådan bekräftelse men inte fått någon, får rätten bortse från meddelandet.

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

Utredningen föreslår att 5 kap. 3 § skall ha följande lydelse (ändringar markerade med kursiv text).

5 kap. 3 §

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.

Bilaga 5

Befintliga säkerhetsstandarder för användning på Internet

Källa: Statskontorets rapport 1997:18, Svenska delen av Internet

Standard	Funktion	Styrka	Svaghet	Geografisk spridning
TLS/SSL, m X.509-cert främst för WWW	Verifierar server per session, kan också verifiera klienten. Hierarkier skapas när nyckeln skapas.	Ger integritet och konfidentialitet av sessionen. SSL kan också rätt implementerat ge autentisering.	CA-certifikat i klienten overi-fierat.	Spridd och mycket använd i WWW, dock med icke-hierarkisk X.509 PKI.
PGP PGP-MIME RFC 2015	Säker e-post, signering och kryptering. PP-MIME be-skriver hur man stoppar in PGP-meddelanden i MIME. Både textskyddsformat och nyckel-format.	Ger integritet, autentisering och konfidentialitet för e-post. Använder ”web-of-trust” och inte nödvändigtvis hierarkiska nyckelstrukturer. Hierarkier skapas efterhand genom signering.	Individrelaterat.	Spridd och mycket använt, men enbart genom icke-formaliserade kedjor av förtroende.
SSH	Använder RSA och symmetriska algoritmer för att ge autentisering, integritet och konfidentialitet vid inloggning, kopiering av filer m.m. Nycklar per användare eller per dator.	Mycket spritt och använt vad gäller telenet och ftp mot UNIX-datorer och liknande.	Standard för initial nyckeldistr. saknas. Känslig för ”man in the middle-attacker”. Nyckeldistribu-tion manuell eller osäker. Om det kommer andra fungerande nyckeldistribu-	Spridd och använd, trots problem med initial nyckel-distribution – antagligen p.g.a. dålig kunskap om bristerna.

			tionsmetoder så kommer SSH sannolikt att använda sig av det.	
Kerberos V.4 Kerberos V.5 Symmetrisk	Autentisering av klienter och servrar. Använder symmetrisk kryptering och ett nyckeldistribu-tionscenter (KDC). Används i huvudsak inom en organisation.	Säker autentise-ring av server och klient vid telenet och ftp. Fungerar säkert även från osäker ändpunkt till skillnad från SSH som har problem med initial nyckel-distribution.	Kräver tredje-partsfunktion, som i sin tur kan bli känslig för attacker.	Spridd i organisationer med stort behov av fjärrinlogg-ning via telnet, t.ex. fjärrkon-figuration av nätnoder.
SEIS ID, X. 509-cert	Autentisering, signering, kryptering.	Nyckellagring på kort garanterar att innehavaren inte kan duplicera sin privata nyckel.	Förutsätter tillgång till kortläsare i alla situationer. Osäkert/oklart hur kommunikation med kortläsare sker.	Lokalt.
S/MIME (PKCS#7) X.509	Beskriver hur man stoppar in PKCS#7-meddelande i MIME. Auten-tierar användare per meddelande. Signering och kryptering.	Ger integritet, autentisering och konfidentialitet för e-post.	Applikationerna ger inte stöd för hierarkier. Osäker utveckling.	Begränsad spridning.
IPSEC ISAKMP/ Oakley alt. manuellt	Implementerar säkerhetsfunk-tioner på IP-nivå. Hanterar all trafik mellan 2 IP-adresser på IP-nivå	Tunnling mellan olika brand-väggar för LAN-LAN kommu-nikation.	Standarden är inte klar.	Experimentell
DNSSEC RFC2065	Säkerställer innehållet i DNS. Kan också	Ger genom domännamns-hierarkin	Ännu inte testat i stor skala.	Ett fåtal imple-mentationer finns.

	användas för att distribuera krypteringsnycklar.	automatiskt en PKI för certifikat. Inte ifrågasatt.		Experimentell.

Bilaga 6

Svenska författningar som tar upp elektroniska dokument

Frihandelsförordning (1987:1185)
Förordning (1984:247) om punktskatter och prisregleringsavgifter
Förordning (1990:1237) om självdeklaration och kontrolluppgifter
Förordning (1993:965) om frihandel i varuutbytet mellan Sverige och Färöarna
Förordning (1994:1605) om tullfrihet m.m.
Förordning (1994:1606) om vissa tullförfaranden med ekonomisk verkan, m.m.
Förordning (1994:598) om pantbrevsregister
Förordning (1996:877) om tillämpning av en överenskommelse mellan Sverige och Tjeckien om ömsesidigt bistånd i tullfrågor
Indrivningsförordning (1993:1229)
Kriminalregisterkungörelse (1973:58)
Lag (1959:551) om beräkning av pensionsgrundande inkomst enligt lagen (1962:381) om allmän försäkring
Lag (1984:151) om punktskatter och prisregleringsavgifter
Lag (1990:325) om självdeklaration och kontrolluppgifter
Lag (1992:1528) om offentlig upphandling
Lag (1994:448) om pantbrevsregister
Mervärdesskatteförordning (1994:223)
Sjölag (1994:1009)
Skattebetalningsförordning (1997:750)
Skattebetalningslag (1997:483)
Skatteregisterlag (1980:343)
Taxeringsförordning (1990:1236)
Taxeringslag (1990:324)
Tillkännagivande (1990:966) av ett avtal mellan den Europeiska ekonomiska gemenskapen och EFTA-länderna om en procedur för informationsbyte inom området tekniska föreskrifter

Tullag (1987:1065)
Tullförordning (1994:1558)
Tullregisterlag (1990:137)
Utsökningsförordning (1981:981)
Varumärkesförordning (1960:648)

Bilaga 7

Internationell privat- och processrätt

1. Inledning

Varje gång en svensk domstol ställs inför en förmögenhetsrättslig tvist som på något sätt anknyter till utlandet måste domstolen inledningsvis fastställa om den är behörig att ta upp tvisten till prövning, dvs. om den har *jurisdiktion*[102] (domsrätt) eller ej. Om så skulle vara fallet blir nästa steg att avgöra *lagvalsfrågan*, dvs. avgöra enligt vilket lands lag det materiella problemet skall lösas. Till sin hjälp har domstolen en mängd skrivna och oskrivna regler och det är dessa regler som utgör den internationella privat- och processrätten.[103]

Den fråga av internationellt privaträttslig natur som framför allt kan bli aktuell vid användandet av digitala signaturer är *vilket lands lag som avgör om ett avtal skall anses giltigt till formen*. Nedan kommer att redogöras för de svenska internationellt privaträttsliga regler som behandlar denna fråga. Av utrymmesskäl kommer redogörelsen att begränsa sig till de regler som är av direkt relevans för frågeställningen samt i viss mån att präglas av förenklingar.

[102] Jurisdiktionsfrågor är ej av intresse för den vidare framställningen och kommer därför inte att behandlas här.

[103] Den internationella privat- och processrätten utgör en del av den natio - nella rätten; varje land har sitt eget inte rnationellt privat- och processrättsliga regelverk. Reglerna har dock till stor del harmoniserats i flera länder genom internationella konventioner.

2. Lagval

2.1 Allmänt

Även om en svensk domstol skulle vara behörig vid en förmögenhetsrättslig tvist med anknytning till utlandet är det inte säkert att svensk lag skall tillämpas. I svensk internationell privaträtt anses nämligen varje förmögenhetsrättsligt avtal underkastat ett visst lands lag. Denna benämns kontraktets avtalsstatut *(lex obligationis* eller *lex contractus)*. I vissa länder talar man i stället om ”avtalets egen lag” *(the proper law of the contract)*.[104]

Nödvändigheten av att ett avtal i vissa sammanhang uppfyller viss form behandlas i promemorians kapitel 7.1.1 I svensk rätt har ett avtal traditionellt ansetts giltigt till formen om det i detta avseende I) enligt huvudregeln, varit giltigt enligt avtalsstatutet eller II) varit giltigt enligt lagen i det land där avtalet ingicks (*lex loci contractus*). Vid sidan av sistnämnda princip tillfogas i samband med inkorporeringen av EU-staternas konvention om tillämplig lag för avtalsförpliktelser (den s.k Romkonventionen, 1980) med svensk rätt (se nedan) ytterligare principer som klargör när ett avtal skall anses giltigt till formen.

2.2 Huvudregeln: avtalsstatutet

För att kunna undersöka huruvida ett avtal är giltigt till formen enligt avtalsstatutet måste först, med hjälp av internationellt privaträttsliga regler (s.k. lagvalsregler eller kollisionsregler), fastställas vilket lands lag som utgör avtalsstatut. Tidigare fanns skrivna lagvalsregler i princip endast beträffande internationella köp av lösa saker samt beträffande växel och check. I övriga fall fick lösningar sökas i rättspraxis och doktrin. I framtiden kommer dock

[104] Michael Bogdan, Svensk internationell privat- och processrätt, 4:e uppl., 1992, Lund s. 225.

tillämplig lag vid sådana övriga fall i stor utsträckning att kunna fastställas med hjälp av Romkonventionen.

2.2.1 Fastställande av avtalsstatut enligt Romkonventionen

År 1980 antog EG:s medlemsstater Romkonventionen om tillämplig lag för avtalsförpliktelser. Avsikten var att unifiera staternas regler på området. Riksdagen beslöt den 4 februari 1998 att konventionen skall gälla som svensk lag fr.o.m den 1 juli 1998.[105] Konventionens regler är tillämpliga på avtalsförpliktelser i samtliga tillfällen då det uppkommer en valsituation mellan rättsordningar i olika länder, *oavsett* om något av de berörda länderna har tillträtt konventionen. Från konventionens tillämpningsområde undantas bl.a.frågor som rör negotiabla värdepapper och skiljedoms- eller prorogationsavtal. Romkonventionen är vidare, enligt art. 21, subsidiär till andra konventioner, dvs. den skall endast tillämpas om det inte finns någon annan konventionsgrundad regel som är tillämplig. För svensk del innebär det främst att om IKL (se nedan) är tillämplig så skall IKL:s regler tillämpas i första hand.

I Romkonventionen är utgångspunkten, vid fastställande av avtalsstatutet, att parterna har rätt att inbördes komma överens om vilket lands lag som skall tillämpas på avtalet, art. 3.1. En sådan överenskommelse måste åtminstone framgå av omständigheterna och kan ingås eller ändras i samband med eller efter avtalets ingående. En dylik ändring påverkar enligt art. 3.2 ”inte avtalets giltighet till formen”.

Skulle t.ex. avtalet vara giltigt till formen enligt det först valda avtalsstatutet, men inte enligt den lag som sedan valts (och heller inte enligt lagen i det land där avtalet ingicks eller av någon annan anledning) blir avtalet således inte giltigt till formen p.g.a. lagskiftet. Om, vice versa, ett till formen ogiltigt avtal kan bli giltigt genom byte av avtalsstatut är oklart, men det verkar mindre

[105] Konventionstexten återfinns som bilaga till prop. 1997/98:14.

troligt om man ser till den svenska versionen av konventionstexten. I utländsk doktrin har dock uttalats att så åtminstone får antagas vara fallet.[106]

Finns inte någon sådan överenskommelse som avses i art. 3 blir avtalet underkastat lagen i det land som det har närmast anknytning till, art. 4.1 Enligt en presumtionsregel i art. 4.2 skall avtalet antas ha sin närmaste anknytning till det land där den part som skall utföra den prestation som är karaktäristisk för avtalet har sin vanliga vistelseort vid avtalsslutet eller, om det är en juridisk person, sin centrala förvaltning. Med den avtalsprestation som sägs karaktärisera avtalet avses vanligen naturaprestationen (jfr nedan, 4 § 1 st. IKL). Skulle avtalet trots allt uppvisa en starkare anknytning till ett annat land bryts presumtionen. Kan vidare den karakteristiska prestationen inte bestämmas faller enligt art. 4.5 presumtionsregeln bort. Den närmaste anknytningen får då fastställas genom en helhetsbedömning.

Konsumenter skyddas i vissa situationer, angivna i art. 5.2, av tvingande regler i det land där konsumenten har sin vanliga vistelseort – oavsett om överenskommelse om annan lag ingåtts. Detta gäller dock endast om

1 avtalet ingåtts efter ett särskilt anbud riktat till konsumenten i dennes hemviststat eller annonsering där, och om ”konsumenten vidtagit de för avtalets ingående nödvändiga åtgärderna i det landet”,

2 motparten mottog konsumentens beställning i det landet eller

3 konsumenten reste till ett annat land och gjorde en beställning av en vara där, förutsatt att resan arrangerades av säljaren med syftet att förmå konsumenten till köpet. I art. 9.5 finns särskilda lagvalsregler vad avser avtals giltighet till formen.

[106] Se Allan Philip, EU-IP, 2:a uppl., 1994, Köpenhamn, s. 140, och där införd hänvisning.

2.2.2 Fastställande av avtalsstatut enligt IKL

Lagen (1964:528) om tillämplig lag beträffande internationella köp av lösa saker (IKL) innehåller lagvalsregler och enligt 1 § 1 st. äger lagen tillämpning på sådana köp av lösa saker som har internationell karaktär. Lagen bygger på en internationell konvention[107] men tillämpas, liksom Romkonventionen, i förhållande till alla världens länder. Från lagens tillämpningsområde undantas bl.a. frågor rörande köpeavtalets form och köp av värdepapper. I samband med införandet av Romkonventionen kommer också konsumentköp att undantas från IKL:s tillämpningsområde. Fastställande av avtalsstatut vid konsumentköp sker således efter den 1 juli 1998 med hjälp av Romkonventionens regler.

Även i IKL är huvudregeln att parterna har frihet att välja tillämplig lag, 3 § 1 st. Parternas överenskommelse är giltig om den är direkt uttryckt i eller annars otvetydigt framgår av avtalet. I 3 § 2 st. anges att fråga huruvida giltig överenskommelse om tillämpning av visst lands lag kommit till stånd bedöms enligt lagen i detta land, dvs. den genom överenskommelsen valda rättsordningen. Finns inte någon sådan överenskommelse som avses i 3 § skall enligt 4 § 1 st. lagen i det land där säljaren har sin hemvist då han mottar beställningen eller, om beställningen mottas vid ett säljaren tillhörigt fast driftställe, lagen i det land där detta är beläget, tillämpas. Anledningen till att IKL i princip väljer säljarens lag sammanhänger med att säljarens förpliktelser vid ett köp i högre grad än köparens är karakteristiska för transaktionen. De är också mer komplicerade. Säljaren anses ha lättare att uppfylla sina skyldigheter om dessa bestäms av den rättsordning som ligger honom närmast och som kan han antas bäst känna till.[108]

Enligt 4 § 2 st. skall lagen i det land där köparen har sin hemvist eller där han innehar fast driftställe, från vilket beställningen görs, dock tillämpas, om säljaren eller hans representant mottar

[107] 1955 års Haagkonvention om tillämplig lag beträffande internationella köp av lösa saker, SÖ 1964:12.
[108] Michael Bogdan, Svensk internationell privat- och processrätt, 4:e uppl., 1992, Lund, s. 233 f.

beställningen i detta land. Har köparen och säljaren ingått avtal per brev, telex, telefon osv. mellan de två länderna, tillämpas säljarens lag i enlighet med regeln i 4§ 1 st.

Beträffande köp på börs eller auktion skall enligt 4 § 3 st. IKL lagen i det land där börsen finns eller auktionen äger rum tillämpas.[109]

2.3 Alternativreglerna: lex loci contractus m.fl.

Den ovan (avsnitt 2.1) nämnda regeln om tillämpning av lex loci contractus stämmer överens med locus regit actum-principen, enligt vilken det för en rättshandlings giltighet till formen räcker att de formella kraven enligt lex loci actus (contractus) är uppfyllda. I samband med Romkonventionens införande fastställs dessa och en del andra principer i lag.

Romkonventionens regler är tillämpliga såvida inte någon annan konvention kan appliceras. Den enda (här) tänkbara kollisionen skulle kunna ske med IKL:s regler, men dessa omfattar inte avtalets form (se ovan). Således blir Romkonventionens regler i art. 9 om avtals giltighet till formen tillämpliga.

Artikel 9.1 fastslår den ovan presenterade huvudregeln, att avtalet är giltigt till formen om det uppfyller de formkrav som är uppställda i avtalsstatutet, samt den traditionella alternativregeln, att avtalet är giltigt om det uppfyller de formkrav som gäller enligt lagen på den ort där avtalet kom till stånd, lex loci contractus.

Enligt art. 9.2 skall ett avtal, om det ingås mellan personer som befinner sig i olika länder, vara giltigt till formen om det uppfyller de formkrav som är uppställda i avtalsstatutet eller om det uppfyller formkraven i något av dessa länder.

Vid de tillfällen som nämnts ovan, art. 9.1 och 9.2, kan part ha ingått avtalet med hjälp av en representant. Av art. 9.3 framgår att

[109] Betr. var elektroniska börser och auktioner ”finns” eller ”äger rum”, jfr Christina Hultmark, Elektronisk ha ndel och avtalsrätt, 1998, Sthlm, s. 19.

det i sådana fall är det land där representanten agerat som utgör det relevanta landet vid tillämpningen av dessa båda punkter.

Enligt art 9.4 skall en ensidig rättshandling som avser ett existerande avtal (ex. en uppsägning av avtalet) eller ett framtida avtal (ex. anbud eller accept) vara giltig till formen om rättshandlingen uppfyller formkraven i avtalsstatutet eller i landet där den företogs.

I art. 9.5 fastslås att bestämmelserna i art 9.1–9.4 inte skall tillämpas på de konsumentavtal som omfattas av reglerna i Romkonventionens art. 5.2 (se ovan). Giltigheten till formen skall vid sådana tillfällen i stället avgöras enligt lagen i det land där konsumenten har sin vanliga vistelseort.

Enligt art. 9.6 undantas bestämmelserna i art. 9.1–9.4 också vid vissa avtal som rör köp eller nyttjanderätt till fast egendom. Undantaget rör de fall då det finns tvingande bestämmelser rörande formkrav i den stat där egendomen är belägen och som skall tillämpas oavsett i vilket land avtalet ingåtts och oavsett vilken lag som i övrigt gäller för avtalet.

Slutligen kan nämnas att avtalets giltighet till formen enligt Romkonventionens regler kan få vissa rättsverkningar i bevishänseende. Bevisning om ett avtal eller en rättshandling får, enligt Romkonventionens art. 14.2, föras inte bara med de bevismedel som är godkända i domstolslandets lag, utan också med varje slags bevismedel som är erkända i något av de länder där avtalet eller rättshandlingen har giltighet till formen enligt art. 9. En begränsning kan emellertid ligga i att det är en förutsättning att det enligt domstolens rättegångsregler är möjligt att genomföra bevisföringen. Uttryckliga förbud eller praktiska förhållanden som gör bevisupptagningen omöjlig kan således leda till avvisning.[110]

[110] Allan Philip, EU-IP, 2:a uppl., 1994, Köpenhamn, s. 176.

3. Om reglernas tillämpning vid internationell elektronisk kommunikation

Vid fastställande av avtalsstatut bör tolkningen av sådana begrepp som ”hemvist”, ”vistelseort”, ”driftsställe” etc. som utgångspunkt vara verksamhetens fysiska placering i form av t.ex. kontor och medarbetarnas arbetsplatser.[111] De regler i Romkonventionen som tillämpas för att fastställa vilket land som har närmast anknytning till en transaktion torde vid de flesta distansavtal vara oberoende av var de överföringsmedier (telefax, dator, server osv.) som parterna använder sig av befinner sig eller vilken väg meddelandena transporteras på vägen till mottagaren.[112] Vid den helhetsbedömning, som måste göras när presumtionsregeln om den karaktäriserande prestationen inte går att tillämpa, har det hävdats att faktorer som parternas hemvist eller nationalitet, avtalsorter, uppfyllelseort, valuta samt t.o.m. det språk kontraktet är utformat på åtminstone inledningsvis bör tilläggas större vikt än överföringsmediernas geografiska placering.[113]

Vid tillämpningen av reglerna i Romkonventionens art. 9.1–9.4 är det mera tveksamt om det i samma utsträckning går att utgå ifrån att överföringsmediernas geografiska placering bör spela en underordnad roll. Frågan är hur man skall tolka ”det land där avtalet är ingånget” alternativt ”där rättshandlingen är företagen”. När bestämmelserna i Romkonventionen utformades var de som i dag existerar okända, men när reglerna nu skall användas kan man inte helt utesluta att överföringsmediernas geografiska placering kan komma att ha en viss betydelse.

Vid internationell elektronisk kommunikation kan en del av de i denna redogörelse nämnda begreppen visa sig svåra att närmare tolka och definiera. Detta kan få konsekvenser för såväl frågor som

[111] Jfr Christina Hultmark, Elektronisk handel och avtalsrätt, 1998, s. 17.
[112] Jfr Christina Hultmark, Elektronisk handel och avtalsrätt, 1998, s. 17.
[113] Jfr Christina Hultmark, Elektronisk handel och avtalsrätt, 1998, s. 17.

rör avtalets giltighet till formen som beträffande allmänna internationellt privat- och processrättsliga spörsmål om vilken domstol som är behörig och vilket lands lag som skall tillämpas vid t ex internationell elektronisk handel. En vidare redogörelse för sådana problemställningar ligger utanför ramarna för denna bilaga.

Bilaga 8

Utdrag ur ”Legal and Regulatory Issues for the European Trusted Services Infrastructure – ETS”, kapitel 1:a

Rapporten finns tillgänglig i sin helhet på http://www.cordis.lu/infosec/src/stud2fr.htm

Chapter 1:a

3. WHAT A DIRECTIVE SHOULD RULE

In a framework where only one country (Italy) has its own national law and only two countries (Germany and United Kingdom) have a draft law, a directive could easily define the guidelines the national lawgivers should follow. A general harmonisation is obviously easier when no national law has been issued, and a common platform is essential in order to create an European central Trusted Third Party and a unique regulation for the issuing and government of digital signature certificates.

However, it is very difficult to point out what a directive should rule. We would like to underline that there could be two different approaches:

A) a directive could define an electronic document, a digital signature and a trusted third party and rule only their attribution, role and use;

B) a directive can define and rule the use of electronic documents, digital signature and trusted third parties and could also define to which kind of acts this system can be applied, where and when an agreement is concluded, what a virtual domicile is, etc.

A) The first solution is accepted in the German[114] and in the British[115] proposal. In those proposals, the lawgiver outlines the requirements of digital signature and electronic documents, lays out the powers, attributions, responsibilities and requisites of trusted third parties, the contents of digital signature certificates.

From those proposals, and from the Italian law and draft of regulations, we can take out some useful suggestions for an hypothetical directive.

- First of all, a directive should define digital signature and electronic document. There should be a legal and a technical definition. In Chapter 1 we mentioned some definitions and we pointed out that they are, more or less, quite similar.

- The technical definition of digital signature, as well as the indication of the technical requirements of trusted third parties, shouldn't be too much detailed, in order to allow the speed of any useful modification.

- The lawgiver should decide and the directive should decree where the private signature key should be kept.

In this decision, the legislator should bear in mind that this support should be economic, easy to be used, trustworthy and sure. All the researches show that the best support is a smart card, used with a personal identification number (P.I.N.). The use of biometrics instruments of identification is inadvisable, because of the mistrust of common people. Biometric instruments are regarded as an attack to privacy and to physical integrity. Furthermore, from the introduction of a finger into an identification machine can hardly be

[114] German Draft Digital Signature Law (SigG), Reporter's draft, Version of September 19, 1996 and of November 4, 1996.
[115] Minister for Science & Technology, *The licensing of trusted third parties for the provision of encryption services, Consultation paper on proposals for legislation,* page 3, March 1997, United Kingdom.

deduced the animus signandi, i.e. the will to sign and to be bound to the content of the document.

- There should be a definition of the requirements for the reliability of digital signature: for instance, it must be pointed out that a signature is trustworthy if it has been issued from a licensed certification authority, if its time validity is not expired, if the signature and its certificate has not been revoked or suspended etc.

- The lawgiver should define the complete procedure of signing and should decree that a digital signature is validly affixed only if this procedure has been completely performed. Particularly, the interruption of the signing procedure should be equivalent to the refuse of signing.

- There should be the provision of a system of time stamp, in order to

  – allow the verifier to determine reliably whether the digital signature was created during the operational period stated in the certificate;
  – to prevent an unlawful pre and/or post dating of digital documents and
  – to grant fixed data to the document.

  The time stamp should be a digital attestation of a certifier, marked with its digital signature, that an identified electronic document, subscribed with a digital signature, has been presented to the same certifier at a certain time.

- Digital signature should always be related to a physical person.

- If a physical person acts as legal representative of a juridical person or in representation of a non compos mentis person, the power of agency or representation should be detectable in the

digital signature certificate of the author. In the same certificate, there should be a clear indication and limitation of the representative's powers.

- The key pair of signature should be issued only to an identified physical persons who has legal capacity: the directive should determine the attribution of this duty to trusted third parties.

- There should be a prevision on the value of proof of an electronic document signed with a digital signature and the value of proof of its duplicates, extracts and copies, either reproduced on another electronic document or on a paper one. In the same way, there should be the prevision of proof of a document originally formed on a paper support and in a second time copied on an electronic document.

- The lawgiver should decree that an electronic document subscribed with a digital signature, its copy, its transmission with telematic instruments and its recording are valid and effective for all legal purposes. The lawgiver should also decree that, in order to be valid and effective, the electronic document subscribed with a digital signature should be formed using the mechanism and the security levels defined in the annexed regulations. Those regulations should be brought up to date quite frequently, in order to keep abreast the technical evolution.

- In order to remain indecipherable, the signed document should be re-signed after a pre-determined period of time.

The directive should decree that the new signature should not be affixed by its original subscriber/subscribers, but from the trusted third party who has generated and keeps the signer's key. In this way, the signers could not refuse to sign again their document and the document could remain secure. The directive should determine which type of documents should be re-signed and the manner of the new signature.

- The signature key pair should not be transferred.

- Every physical person has his own hand-written signature and should have his own signature key pair. The signature key pair is related to a determined physical person, who signs for himself or for the person/company he represents, so that each signature identifies a person and binds the signer to the content of the act. The directive should prohibit the assignments of the signature key pair and should determine the consequences of the assignment and of the use of the signature key pair. The directive should also provide for the responsibility of the forged signature, in order to protect the bona fide holder. This prevision could simply refer to the just existing similar rules for the false representative and the forged signature.

- It should be impossible to generate twice the same signature key pair.

- The directive should determine whether the signature key pair should be generated only by licensed trusted third parties or it could be generated by everybody. This second solution is inadvisable.

- When the trusted third parties generate and assign the signature key pair, it should advise the applicant of the legal consequences of the affixing of the digital signature at the bottom of an electronic document. At the same time, the trusted third parties should tell the applicants the use of digital signature, should inform them on the effects of the assignment, loss, breaking, stealing of the smart card.

- The directive should decree whether trusted third parties should prepare a declaration form that each applicant should sign after the consignment of the signature key pair.

- With this declaration the applicants acknowledge that they have been informed of the legal consequences of the affixing of the digital signature at the bottom of a document and that they accept them. In practice, this document can consist of declaration with which the originator of a data message on which he has affixed his digital signature accepts to be bound by the content of the message, in the same manner as if the message had existed in a manually signed form in accordance with the law applicable to the content of the message.

- The lawgiver should decide whether all the public signature keys, together with their certificates, should be verifiable at any time by everyone. If the legislator decides that the public signature key can be publish edonly with the permission of its owner, he should provide for the allegation of the public signature key certificate to the signed document.

- The directive should define also the conditions and ways of verifiability of the public signature keys and should harmonise this provision with the national laws on protection of personal data.

- The directive should also harmonise the data collection, indispensable for the formation of digital signature certificates, with the national laws on protection of personal data.

- The legislator should rule the contract between private persons and trusted third parties.

- This contract should also define the distribution of responsibility between the applicants and the certification authorities for the misuse of the signature key pair, for the non-notified suspension or revocation of the key, for the non-identification of the applicant, for the non-re-subscription of the document after the predetermined period of time etc.

- The directive should define trusted third parties, ruling their powers and duties, their structure and responsibilities, their legal form and requirements.

- A certification authority could not be third: the directive should decree whether a bank could be the certification authority of its clients, and so whether a bank could generate and keep its client's signature key certificates.

- The legislator should define the manner of attribution of the capacity of trusted third party. Particularly, the lawgiver should decree whether this capacity should be practised under a monopoly system or under a competitive system and whether the Public Administration should control the activity of trusted third parties.

- The directive should decree whether the trusted third party could/should take part in trials, where the authenticity and integrity of an electronic document signed with a digital signature is denied.

- The directive should introduce a crossed recognition system for digital signature keys generated in foreign countries.

- A cross recognition system is indispensable for a system of conclusion of contracts between parties of different countries. This is one more reason for the introduction of a directive before the issuance of many national laws.

The legislator should decree whether a central trusted third party has to control the validity of the technical instruments the peripheral certification authorities use in order to generate and keep digital signature key pairs and public keys certificates.

B) The second solution aims at ruling all the legal consequences of the use of digital signature, in order to solve the imaginable

problems private persons will come across. Although no draft law or law has adopted this second way, it could be useful to indicate and give a possible solution to some of those troubles.

– The legislator should define the place and time of conclusion of a digitally signed contract. In several legal systems, the time when the contract is formed is used to determine, for instance:
  – when the offerer is no longer entitled to withdraw his offer and the offeree his acceptance;
  – the time of transfer of the title and the passage of the risk of loss or damage in the case of the sale of an identified good;
  – the law applicable;
  – the price, if it has to be determined by market price at the time of the formation of the contract.

  In the same way, the place where the contract is concluded is used to determine:
  – the competent court in case of litigation;
  – the law applicable in private international law[116].

– If the legislator decides to use the general rule: "a contract is formed when both parties are aware of each other's consent", there should be the definition of the place where the proponent has cognisance of the acceptance. This place should be the virtual domicile, which could correspond to the e-mail address. This virtual domicile should be declared in the signature key certificate. Every variation of this domicile should be declared to the trusted third part. From the moment when the document has arrived in the proponent's virtual domicile, there comes a presumption iuris tantum that the proponent has cognisance of the acceptance. If parties want a presumption iuris et de iure, the

[116] For more details, see United National Commission on International Trade Law, *Electronic data interchange, Preliminary study of legal issues related to the formation of contracts by electronic means, Report of the Secretary-General*, New York, 25 June-6 July 1990, page 18.

certification authority could act as bailiff. The certification authority could act as bailiff also for deed polls.

– The directive should define the category of acts where digital signature can be affixed. For a first period, there should be a general limitation of value and some acts, like the ones defined as ”notary acts” should be excluded. The notary acts category is a problem only in those countries where the legal system provides for some agreements that can be concluded only in particular forms, such as using the instrument form. For those countries where the certification function of notaries is weaker, there is no need to exclude such category from the subscription with digital signature.

The lawgiver should define the manner of registration and transcription of digitally signed documents. There won’t be problems in the use of general principles on registration and transcription, if the organisations appointed to these functions are correctly equipped.

Författare:
Mr. Luca Remotti,
Istituto per lo Studio della Vulnerabilità delle Società
Tecnologicamente Evolute – ISTEV,
Via Roberto Scott 62,
I - 00147 Roma,
Tel. no.: +39-6-5141393
Fax no: +39-6-5137868
E-Mail: 100446.1214@compuserve.com

Bilaga 9

Utdrag ur ”Legal and Regulatory Issues for the European Trusted Services Infrastructure – ETS”, kapitel 2:a

Rapporten finns i sin helhet tillgänglig på http://www.cordis.lu/infosec/src/stud2fr.htm

Chapter 2:a

LAW, DRAFT LAW, CASE LAW

Summary

The digital signature and trusted third party system is a new experience for the European countries. This can probably be the first reason for the lack of legislation ruling its use.The importance of the introduction of a complete legal system, on the contrary, is highlighted from the number of draft laws proposed in the different countries. In this Chapter, we will report the results of our research on the laws, draft laws and case law in all over Europe.

Austria

In Austria there is no law, no case law and no draft law on digital signature and trusted third parties, but the Prime Minister’s Office has sent a set of questions on it to all the Public Administrations. This questionnaire aims at collecting information and

recommendations on requirements of a law on digital signature. The results of the questionnaire are still under elaboration.

According to Prof. Walter Jaburek, the use of digital signature and electronic documents should not meet serious juridical problems, if it won't be applied to those acts which need written form.

Belgium

One of the best studies on electronic documents and digital signature is Belgian. In the book: "Aspects juridiques du mouvement électronique de fonds"[117], Dr. D. Syx, legal advisor in the Kredietbank S.A., defines digital signature for electronic fund transfer and gives some interesting personal suggestions for the solution of the evidence problem in Belgium.

In his article: "Vers de nouvelles formes de signature? Le probléme de la signature dans les rapports juridiques électroniques", Dr. Syx affirms that the modern technologies make possible the creation of new forms of signature, if they can respect all the functions performed by the hand-written signature. This article can be considered the base of the current legal conceptions on digital signature and it is one of the first paper where digital signature is considered legally equal to a hand written one.

In Belgium there is no law, no draft law and no case law on digital signature.

[117] D. Syx, Aspects juridiques du mouvement électronique de fonds, edit from the Kredietbank, April 1982. From the same author, Vers de nouvelles formes de signature? Le probléme de la signature dans les rapports juridiques électroniques, Droit de l'informatique, 1986/3 page 133 and Le transfert électronique de fonds. Le droit hésitant face à une réalité galopante, in La Télématique, Tome 2: Aspects techniques, juridiques et socio-politiques, Story-Scientia, Gand, 1985, 219 – 253; Poullet, Y., Les transactions commerciales et industrielles par voie électronique. De quelques réflexions autour du droit de la preuve, in Le droit des affaires en évolution, Bruylant & Kluwer, Bruxelles - Anvers, 1996, 39 – 67.

Denmark

- -

Finland

- -

France

As mentioned in the first Chapter, digital signature is one of the possible applications of cryptography. There must be a clear distinction between the two applications of cryptography,

– confidentiality, which allows to cipher a text;

– integrity and

– authentication.

In France, there is no law ruling directly the use of digital signature, but the use of cryptography is strictly limited by law.

The use of cryptography is ruled in the art.17 of the Law n.96-650, 26/7/1996[118]:"the use of a method or of a tool of cryptography is free if the method or the tool of cryptography doesn't allow to provide confidentiality functions. In particular, the use is free if the method or the tool can only authenticate a communication or guarantee the integrity of the sent message."

There are two different projects of decree which try to define the rules of application of the law n.96-650, but, up to now, no one has been presented to the Conseil d'Etat.

[118] JO 27/7/1996.

Federal Republic of Germany

- -

United Kingdom

On June 1996 it was announced that the Government would be bringing forward a proposal for the licensing and regulation of Trusted Third Parties for the provision of encryption services.

This announcement "recognised the growing demand from industry for strong encryption services to safeguard the integrity and confidentiality of electronic information transmitted on public telecommunications network. It also recognised the need to balance this demand with the requirements to preserve the ability of intelligence and law enforcement agencies to fight serious crime and terrorism[119]".

In the first days of March 1997 a public consultation paper on the Government's proposal for the licensing of trusted third parties for the provision of encryption services has been issued. It invites comments on the issues set out in the consultation paper.

In the proposal, cryptography is considered useful to protect the confidentiality of data, stored or transferred, to verify the integrity of data, by revealing whether it has been altered, and to identify the person or device that sent it. Cryptography can also be used to establish authenticity, prevent undetected modification, non-repudiation and unauthorised use.

The British proposal aims at defined TTPs which would be used to offer value added services to users wishing to enhance the trust and business confidence in the service they receive, and to facilitate secure communications between business trading partners. TTPs

[119] Minister for Science & Technology, The licensing of trusted third parties for the provision of encryption services, Consultation paper on proposals for legislation, page 3, March 1997, United Kingdom.

could be established in both public and private domains, at the local, national and international level and should have trust agreements arranged with other TTPs to form a network, therefore allowing a user to communicate securely with every subscriber to every TTP with whom his TTP has an agreement.

The law provides that bodies wishing to offer or provide encryption services to the public in the UK will have to be licensed. The Department of Trade and Industry has been chosen as the initial authority for the licensing, in view of its experience in licensing telecommunications operators. The duration of licenses will be a minimum of five years. The law inhibits the provision of encryption services in the UK without licence.

TTPs will be held responsible for the protection of the private encryption keys of clients at all times they are in their possession. In the event of loss or disclosure of keys, deliberate or accidental, the TTP will be required to have in place adequate arrangements to compensate any loss suffered by its clents or clients of other TTPs.

A TTP will have to be able to offer Data recovery Services. Actually, if the encrypting key is stolen, lost or deliberately withheld by disaffected employees, the information will remain encrypted and may be lost to its owner for ever. TTP will have to offer recovery of the keys to their clients as they will store or escrow the keys.

On the other end, cryptography can also be used to improper applications, such as hiding the illegal activities of criminals and terrorists.

For these reasons, the British draft proposes that legal access should be achieved by making use of a key escrow/recovery system. “Key recovery allows authorised persons (for example users, officers of an organisation and law enforcement authorities) under certain conditions, to decrypt messages with the help of cryptographic key information, held in escrow, and supplied by one

or more trusted parties. In such cases legal access is to private confidentiality key[120]".

The legislator will provide that the Secretary of State may issue a warrant requiring a TTP to disclose private encryption keys, but protecting the confidentiality of information. There will be safeguards broadly similar to those in the Interception of Communications Act 1985, under which a Secretary of State may issue a warrant requiring the interception of communications. For the purposes of legal access, a central repository could be established. According to contractual arrangements between parties, TTP will be able to release the private encrypting key of the client under contractual arrangements between the two parties.

It must be highlighted that the proposed legislation is directed solely towards the provision of encryption services to subscribers in the UK and not the use of encryption. In the same way, users will remain at liberty to choose whether to make use of TTPs, or to make other arrangements for their encryption requirements.

In Chapter III, par. 3, we have evidenced the problems that the British system of evidence will give in case of use of the digital signature system without the provision of a proper regulation.

Greece

Since now, in Greece there is no law, no draft law and no case law.

From our interview with Dr Stavros Karageorgiou, we have concluded that in the Greek civil system, the only acceptable legal method for the authenticity of a document is the subscription with a hand written signature (art.160 of the Greek civil code).

An exception is the mechanical signature of bank notes and stocks (art.163 g. c.c.). It can also be noted that an order for cash to a bank using an ATM is verified only by the use of the PIN, and that this system is accepted by the Greek legal order.

[120] Minister for Science & Technology, The licensing of trusted third parties for the provision of encryption services, Consultation paper on proposals for legislation, page 10, March 1997, United Kingdom.

But, the digital signature system does not include a signature affixed by mechanical means, so that this rule cannot be used as analogy in order to rule a digital signature system.

Ireland

No law, no draft law and no case law can be registered in Ireland. The analysis of its legislation, conducted together with Dr. Karen Murray, an attorney at law, has not pointed out serious problems for the introduction of digital signature and trusted third parties, especially if is limited to private transactions.

Italy

- -

Luxembourg

Luxembourg can be considered one of the countries where the use of digital signature and electronic documents won't conflict with the law of evidence. A law of 1986[121] has modified the law of evidence expressly allowing computer records to be produced in litigation,

[121] R.G. 22/12/1986, which has modified art. 1348 of the civil code: "lorsqu'une partie ou le dépositaire n'a pas conservé les titres originaux et présente des reproductions micrographiques et enregistrements informatiques efféctuées à partir de ce originaux sous la responsabilité de la personne qui en a la grade, ces reproductions et enregistrements ont la méme valeur probant que les écrits sous seing privé dont ils sont présumés, sauf preuve contraire, étre une reproduction ou un enregistrement fidéle lorsque les originaux ont été déstruits dans le cadre d'une méthode de gestion réguliérement suivie et qu'ils répondent aux conditions fixées par un réglement grand-ducal".

and giving to such records the same evidentiary value as that of the documents they purport to reproduce.

We would like to thank Maitre Albert Moro, of Faltz & Associes Avocats a la Cour, for the valuable effort.

Portugal

In Portugal there is neither a law nor a draft law ruling the digital signature and, up to now, there has been no case law.

In our research, thanks to Dr Nuno CastelloBranco, researcher in the Law Faculty of University of Coimbra, we found that there is one law, the Decreto-Lei n.352/86 de 21/10/1986[122], that rules the transport contract, which admits, at the third article, also telex, fax and all the other modern techniques as valid system for the conclusion of the agreement.

In the 5° point of the introduction of the same decree, you can find that "in the art.3 the legislator wants to accept the new ways of formalisation of the contractual agreement, coming from the use of the informatics and telematic items." In that introduction, it is also reported a Pierre Bonassies's statement, where he says that the use of informatics items doesn't prejudice the trustworthiness of the agreements and declarations and doesn't increase the risk of fraud.

This provision of the law allows to retain that the Portuguese legislator wants to admit the use of the new informatics methods for the conclusion of contracts. The digital signature system, however, needs a proper regulation.

Spain

In Spain there is no law ruling the digital signature from a technical point of view, but there are some ordinances which authorise its use. The most important is the Ley 30/92[123], which rules the

[122] Diàrio da Repùblica de 21/10/1986, pag.3172 et ss.
[123] B.O.E. n.285 27/11/1992.

juridical regimen of the Public Administration and of the ordinary administrative procedure and the consequent Real Decreto 263/1996[124] which rules the utilisation of the electronic and telematic techniques for the General Administration of the State.

The article n.45, sub-Paragraph n.5, orders that all the documents created with electronic, informatics or telematic instruments for a Public Administration, and the documents that are a copy of a document created in that way, have to be considered as an original if their authenticity, integrity and conservation is guaranteed. We have discussed this rule with Prof. Inaki Vicuna De Nicolàs, of the Vice Presidency of the Gobierno Vasco, and he suggested that it could be used until the complete regulation of the digital signature system.

No case law and no draft law is yet known.

Sweden

- - -- - - - - - - - - - - - -

The Netherlands

From a number of interviews, we discussed a deal of information from Dr Grutters and Prof. Berkvens, of the Law and IT Faculty, University of Nijmegen.

In this country, there is neither a law nor a draft law ruling the use of digital signature. In the Dutch civil code there is no obstacle regarding the use of Ds , so they believe that there is no need to issue a new law.

According to Prof. Berkvens' and Dr. Grutter's opinions, digital signature and hand-written signature could be equalised: the use of a digital signature in order to sign a document signifies that the signer wants to be identified as the author (i.e. he is manifesting his *animus signandi*) and that he accepts the content of the text.

124 B.O.E. n.52 29/2/1996.

In The Netherlands there is probably the only case law in Europe concerning directly the use of a digital signature.

It is known as the COVA case and it has, as parties to the case, the Stichting Centraal Orgaan Voorraadvorming Aardolieprodukten and the International Netherlands Bank[125].

The bank had granted to COVA a credit facility. All the payment orders had to be sent from COVA by telex, adding to each message an identification code derived from a code list supplied by the bank. COVA had also entered an agreement of full responsibility for damages resulting from telexes sent from unauthorised persons if these messages contained the right identification code.

One of COVA's employees, not authorised to use the identification code, sent a payment order, with a telex message containing the agreed identification code. He asked the bank to transfer an amount approximately of nine million Dutch guilders to a bank account held in Switzerland. The bank assumed that the message, containing the identification code, was correct and original and executed the payment. COVA submitted a claim against the bank, claiming that as a general rule, the owner of an identification code is not bound by the message that contains its code if the code was used by an unauthorised person..

In November 1993, the Dutch Supreme Court, decided against COVA. It solved the question who should bear the risk of misuse of an identification code deciding that it is important to consider all the circumstances of the case, and, in particular, to establish who can be held responsible for the code being used by an unauthorised person.

In this case, the unauthorised person was an employee of the owner and had easily access to the code. The owner could be held responsible as it may be assumed that the misuse was a result of his own negligence.

[125] Nederlandse Jurisprudentie 1994, n.622.

An exception to this rule can be found in the case in which the owner can prove that he has fulfilled his duty of care.

Författare:
Mr. Luca Remotti,
Istituto per lo Studio della Vulnerabilità delle Società
Tecnologicamente Evolute – ISTEV,
Via Roberto Scott 62,
I - 00147 Roma,
Tel. no.: +39-6-5141393
Fax no: +39-6-5137868
E-Mail: 100446.1214@compuserve.com

Bilaga 10

Lista med ordförklaringar[126]

ADB (automatisk databehandling): Innebär att datorer används för lagring och bearbetning av information.[127]

Algoritm: En matematiskt definierad serie av instruktioner som kan lösa ett specifikt problem t.ex. när de görs om i ett ADB-program. Ordet används ofta i en vidare betydelse som det tekniska idéunderlag som finns implementerat i eller ligger bakom ett ADB-program.[128]

Allterminalen: Säkerhetslösning baserad på aktiva kort för person-datorer i nätverk.[129]

Autenticering (verifiering av identitet): En funktion som fastställer giltigheten av den uppgivna identiteten på en användare, en apparat eller en funktion i ett informations- eller kommunikationssystem.[130]

Binära talsystemet: Talsystem med basen 2. De ingående siffrorna kan anta värdet 0 eller 1. Det krävs fler siffror för att representera ett visst tal med det binära talsystemet än med det decimala, i

[126] En utförlig samling förklaringar av dator- och Internettermer finns på http://www.whatis.com
[127] IT-ordlista & www-adresser, STF Ingenjörsutbildning AB, utg. 3, Sthlm, 1996.
[128] Danmarks IT-sikkerhedspolitik - et baggrundspapir, Forskningsministeriet, nov. 1996, sv. översättn. PTS.
[129] Se vidare http://www.seis.se/arkiv/seisfunkspec.html
[130] Ur kap. 2 Kryptopolitik - möjliga svenska handlingslinjer, Regeringskansliets referensgrupp för krypteringsfrågor, 1997. Definitionerna i rapporten hämtade ur OECD-riktlinjerna för krypto-policy.

genomsnitt 3–4 ggr så många, men i gengäld blir de matematiska operationerna mycket enkla och och väl lämpade för datorer.[131]

Bit: Förkortning av eng. binary digit. Bit representerar endera siffrorna 0 eller 1 i ett binärt talsystem.[132]

Bredband: Avser överföring av flera signaler samtidigt via en förbindelse, digitalt genom tidsindelning i kanaler, analogt genom modulation av flera bärvågor i ett system.[133]

*Byte: E*n grupp av bitar, vanligen åtta stycken.[134]

CA: Certification Authority. Den instans som i ett system för asymmetrisk kryptering uttalar sig om vilken identitet som gömmer sig bakom en utställd nyckel och som – allt efter det underliggande lagstödet – uttalar sig om att utställda nycklar har mist sin giltighet.[135]

CEN: Comité Européen de Normalisation (Europeiska Standardiseringskommittén).[136]

Certifikat (för signaturnycklar): Begreppet certifikat används i en teknisk mening som skiljer sig från traditionell juridisk mening. Ett certifikat används i teknisk mening som ett sätt att koppla ihop den

[131] IT-ordlista & www-adresser, STF Ingenjörsutbildning AB, utg. 3, Sthlm, 1996.
[132] IT-ordlista & www-adresser, STF Ingenjörsutbildning AB, utg. 3, Sthlm, 1996.
[133] IT-ordlista & www-adresser, STF Ingenjörsutbildning AB, utg. 3, Sthlm, 1996.
[134] IT-ordlista & www-adresser, STF Ingenjörsutbildning AB, utg. 3, Sthlm, 1996.
[135] Danmarks IT-sikkerhedspolitik - et baggrundspapir, Forskningsministeriet, nov. 1996, sv. översättn. PTS .
[136] IT-ordlista & www-adresser, STF Ingenjörsutbildning AB, utg. 3, Sthlm, 1996.

privata nyckeldelen med den publika. Det är alltså fråga om hur man i samband med verifikationen skall kunna ”hitta” vilka nyckelpar som hör ihop. I traditionell juridisk mening brukar man förknippa ett certifikat med ett intygande av ett visst förhållande. Ett certifikat utgör i juridisk mening det dokument vari intygandet manifesteras. Användningen av digital signatur syftar i första hand till att intyga nyckelinnehavarens identitet och att meddelandets innehåll är intakt. Detta intygande sker emellertid inte alltid i själva certifikatet – eftersom uppgifterna i certifikatet inte nödvändigtvis visar sig för den som intyget riktar sig till (den förlitande parten) utan kan ligga hos nyckelinnehavaren. Intygandet sker i sådant fall i stället genom det meddelande som den förlitande parten erhåller att nyckelparen passar ihop och att meddelandet inte har förändrats. Detta meddelande genereras vid den procedur varigenom nyckelparen kopplas ihop (och avstäms mot en revocation list).

Data: Från latin; datum, dvs. något givet. Data i informationsteknisk mening är representation av fakta, begrepp eller instruktioner i en form lämpad för överföring, tolkning eller bearbetning utförd av människor eller av automatiska hjälpmedel.[137]

Databas: En organiserad mängd data som är konstruerad så att data kan framkallas efter användarens närmare instruktioner. Detta sker genom användning av en därtill särskilt inrättad applikation (databas management system).[138]

DES: Data Encryption Standard, krypteringsalgoritm konstruerad av NBS med 56 bits nyckel.[139]

[137] Datastraffrättsutredningens betänkande SOU 1992:110, s. 83; inledn., PTS. Seipel beskriver data som symboler som bär information (Seipel, ADB och juridik. En problemöversikt, publicerad som Ds Fi 1975:3, s. 254. Jmfr prop. 1985/86:65 s. 12).
[138] Danmarks IT-sikkerhedspolitik - et baggrundspapir, Forskningsministeriet, nov 1996, sv. översättn. PTS.
[139] IT-ordlista & www-adresser, STF Ingenjörsutbildning AB, utg. 3, Sthlm, 1996.

Digital: (av eng. digit = siffra) Ett exakt värde som kan representeras med ett tal.[140]

Digitalt dokument: En elektronisk handling med digital signatur eller digital stämpel.[141]

Digital signatur: 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.[142]

Digital stämpel: Resultatet av en omvandling av en elektronisk handling som gör det möjligt att kontrollera om innehållet härrör

[140] IT-ordlista & www-adresser, STF ingenjörsutbildning AB, utg.3, Sthlm, 1996.
[141] Förslag till definition från IT-utredningen i betänkandet Elektronisk dokumenthantering, SOU 1996:40, att tas in i förvaltningslagen (1986:223).
[142] Förslag till definition från IT-utredningen i betänkandet Elektronisk dokumenthantering, SOU 1996:40, att tas in i förvaltningslagen (1986:223). Datastraffrättsutredningens betänkande innehåller ett förslag till införande av brottsrubriceringen förnekande av signatur i 14 kap. 9 § BrB. Begreppet signatur omfattar enligt förslaget såväl underskrift som digital signatur. Begreppet digital signatur föreslås inte definieras i BrB. I betänkandet redogörs för det internationella standardiseringsarbete inom Internationella standardiseringskommissionen (ISO) som pågår beträffande autenticering och integritetsskydd för datameddelanden. I den allmänna motiveringen till förslaget till 14 kap. 9 § BrB anges att förslag till ISO-standard, där det direkt anges att digitala signaturer avses kunna motsvara en för hand skriven signatur i ett pappersdokument, föreligger. Utredarna anför vidare, s. 305, att de föreslår att uttrycket digital signatur används som beteckning på digitala ersättare för underskrifter men tillägger att bestämmelsen emellertid avses vara teknikneutral så att motsvarande rutiner som fyller samma funktion men inte ryms inom någon standard skyddas.

från den juridiska person eller myndighet som framstår som utställare.[143]

DNS: Domain Name System. Funktion som översätter dators namn som t.ex. www.pts.se till IP-nummer som t.ex. 130.237.123.30 Varje Internetdomän har minst en dator som fungerar som DNS-server och gör översättningar till IP-nummer. Kallas också name-servers.[144]

Dokument: En skriftlig originalhandling eller en bestämd mängd data för automatisk informationsbehandling, om det är möjligt att fastställa att innehållet härrör från den som framstår som utställare. Som dokument anses också legitimationskort, biljett och dylikt bevismärke.[145]

DSA: Digital Signature Algorithm.[146]

DSS: Digital Signature Standard.[147]

EDI: Electronic Data Interchange. Elektronisk dataöverföring mellan datorer. Data som är strukturerad enligt i förväg överenskomna regler.[148]

[143] Föreslag till definition från IT-utredningen i betänkandet Elektronisk dokumenthantering, SOU 1996:40, att tas in i förvaltningslagen (1986:223).
[144] IT-ordlista & www-adresser, STF Ingenjörsutbildning AB, utg. 3, Sthlm, 1996
[145] Datastraffrättsutredningens förslag till specialdefinition i 14 kap. 1 § BrB för angivna kapitel; med data för automatisk informationsbehandling menas enligt betänkandet SOU 1992:110, s. 115, information som uttrycks i en för datorn omedelbart bearbetbar representationsform; se närmare betänkandet.
[146] Se vidare http://www.rsa.com/rsalabs/newfaq/q26.html
[147] Se även här http://www.rsa.com/rsalabs/newfaq/q26.html
[148] IT-ordlista & www-adresser, STF Ingenjörsutbildning AB, utg. 3, Sthlm, 1996.

Elektroniskt dokument: en upptagning vars innehåll och utställare kan verifieras genom ett visst tekniskt förfarande.[149]

Elektronisk handling: en bestämd mängd data som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel.[150]

EMV: Europay Mastercard Visa. Standard för betalning med smarta kort.

Escrow-lösning: (eng= deponering) Lösning på kontrollproblem som består i att det som skall kontrolleras deponeras hos en trovärdig tredje part (se d.o.) eftersom båda parter har förtroende att den ifrågavarande tredje parten bara kommer att ge ut det deponerade under särskilt angivna och godtagna förhållanden.[151]

EDIFACT: Elektronic Data Interchange For Administration, Commerce and Transport. (Elektronisk dataöverföring inom administration, handel och transport)[152]

ETSI: European Telecommunications Standards Institute.[153]

[149] 11 a § Tullagen (1994:1550), 17 § 3 st. lagen (1994:448) om pantbrevsregister, 2 kap. 2 §, 2 st. lagen (1990:325) om självdeklaration och kontrolluppgifter m.fl. lagar.
[150] Föreslag till definition från IT-utredningen i betänkandet Elektronisk dokumenthantering, SOU 1996:40, att tas in i förvaltningslagen (1986:223). Med definitionen avses enligt betänkandet endast sådana handlingar vars innehåll har bestämts av utställaren, dvs. inte s.k. potentiella handlingar, s. 56.
[151] Danmarks IT-sikkerhedspolitik - et baggrundspapir, Forskningsministeriet, nov. 1996 sv. översättn. PTS.
[152] IT-ordlista & www-adresser, STF Ingenjörsutbildning AB, utg. 3, Sthlm, 1996.
[153] Se vidare http://www.etsi.org

Handling: Framställning i skrift eller bild samt upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel, enligt 2 kap. 3 § Tryckfrihetsförordningen (TF). Definitionen torde innefatta en utvidgning av ett handlingsbegrepp som uppfattats som givet genom att framställning i bild tagits med liksom upptagningar som kan uppfattas endast med tekniska hjälpmedel. Beträffande upptagning för ADB anförde departementschefen i anledning av offentlighets- och sekretesslagstiftningskommitténs betänkande att med sådan upptagning bör avses ”uppgift som är fixerad på någon form av datamedium och som antingen finns i eller kan matas in i en datamaskin [...] läsbar endast med ADB-teknik”, prop. 1973:33 s. 74 f. Begreppet upptagning infördes i datalagen utifrån samma motivuttalanden som i TF. I 21 § 1 st. datalagen lades till att med upptagning avses härvid även uppgifter som är under befordran via elektroniskt eller annat liknande hjälpmedel för att användas för automatisk databehandling. Datalagskommittén tar i sitt betänkande 1997:39, s. 494 f., upp problematiken med avgränsningssvårigheter för elektroniska handlingar genom att datamediet medger att olika konstellationer av uppgifter kan tas fram ur samma innehållsmängd. Upptagningsbegreppet omfattar således enligt nuvarande datalagen uppgiftssammanställningar som inte har ett på förhand bestämt innehåll (potentiella handlingar). Kommittén föreslår ett handlingsbegrepp avseende en specifik samling uppgifter, nämligen sådana som har ett bestämt innehåll, oavsett om den förekommer på papper eller i elektronisk form. Innehållet har oftast bestämts av utställaren och skall inte förändras till skillnad från register- och databasbegreppen. Någon övergripande legaldefinition för handling som är giltig i alla sammanhang finns inte i svensk rätt.

Hashvärde: Numeriskt värde som med hjälp av en matematisk algoritm kan tas ut som en entydig representation av en informationsmängd (t.ex. en text) och som omfattar mindre än den ifrågavarande informationsmängden. Genom att ta ut hashvärden kan man undvika att behandla den större informationsmängden vilket t.ex. kan vara en fördel om det är tal om att kunna utföra en komplicerad

matematisk databehandling av denna mängd (t.ex. kryptering för åstadkommande av digital signatur som ett led i asymmetrisk kryptering).[154]

ICC: International Chamber of Commerce. Den internationella handelskammaren.[155]

IC-kort: Integrated Circuit-kort.

IDEA: International Data Encryption Algorithm[156]

IETF: Internet Engineering Task Force[157] Samarbetsorgan för utveckling av Internets infrastruktur.

Integritet (hos data och meddelanden): En egenskap att data eller information inte har ändrats på ett icke behörigt sätt. (Observera att personlig integritet, eller bara integritet, har en speciell betydelse i datalagssammanhang.)[158]

ISO: International Standards Organisation. Internationella standardiseringskommissionen som lyder under FN och som standardiserar industriprodukter inom en rad olika områden. Medlemmar i ISO är olika länders nationella standardiseringsorgan, från Sverige SIS.[159]

[154] Danmarks IT-sikkerhedspolitik - et baggrundspapir, Forskningsministeriet, nov. 1996 sv. översättn. PTS.
[155] Se vidare http://www.iccwbo.org
[156] För mer information, se http://www.rsa.com/rsalabs/newfaq/q77.html
[157] Se vidare http://www.ietf.org
[158] Ur kap. 2 Kryptopolitik - möjliga svenska handlingslinjer, Regeringskansliets referensgrupp för krypteringsfrågor, 1997. Definitionerna i rapporten hämtade ur OECD-riktlinjerna för krypto-policy.
[159] IT-ordlista & www-adresser, STF Ingenjörsutbildning AB, utg. 3, Sthlm, 1996. Se vidare http://www.iso.ch

ITSEC: Information Technology Security Evaluation Criteria. Europeisk samarbete på IT-säkerhetsområdet.[160]

Konfidentialitet: En egenskap hos data eller information att inte vara tillgänglig eller läsbar för obehöriga individer, organisationer eller processer.[161]

Kryptering: Den process varigenom en mängd information som är sammansatt genom användande av ett allmänt tillgängligt språk, transformeras till data som inte kan förstås genom användning av ett allmänt tillgängligt språk. Transformationen sker med hjälp av en algoritm som styrs av en ingångssignal, en s.k. nyckel. Mottagaren av det krypterade meddelandet kan härefter genom att använda nyckeln få fram den ursprungliga informationsmängden.[162]

MD2 och *MD5*: Message-digest algoritmer. Används vid beräkning av hashvärde (se detta ord).[163]

Nyckelcentraler: Den instans som i ett system för asymmetrisk kryptering står för utställande av nycklar eller som tillhandahåller den utrustning m.m. som är nödvändig för att generera nycklar och (typiskt sett även) verktyg för att ta ut hashvärden.[164]

Paketförmedling: SIS: Datapaketförmedling. Metod för befordran av data som adresserade datapaket varvid erforderlig kanal tas i anspråk enbart för överföring av datapaket och därefter friställs för annan överföring. En internationell teknik för hantering av datanät.

[160] Se t.ex. http://www.itsec.gov.uk/
[161] Ur kap. 2 Kryptopolitik - möjliga svenska handlingslinjer, Regeringskansliets referensgrupp för krypteringsfrågor, 1997. Definitionerna i rapporten hämtade ur OECD-riktlinjerna för krypto-policy.
[162] Danmarks IT-sikkerhedspolitik - et baggrundspapir, Forskningsministeriet, nov. 1996 sv. översättn. PTS.
[163] Se vidare http://www.rsa.com/rsalabs/newfaq/q99.html
[164] Danmarks IT-sikkerhedspolitik - et baggrundspapir, Forskningsministeriet, nov. 1996 sv. översättn. PTS.

Informationen sänds ut till nätet i form av datapaket med information om avsändare och mottagare. Ett meddelande kan komma att styckas upp i flera datapaket. Tekniken identifiers som CCITT X.25. I Sverige finns Datapak som följer denna standard.[165]
PCMCIA: Personal Computer Memory Card International Association. Kort med vilket man utökar funktionerna på persondator, företrädesvis bärbara persondatorer.[166]

PGP: Pretty Good Privacy. En metod och en uppsättning program för kryptering av textmeddelanden som sänds på Internet. PGP använder sig av en krypteringsmetod med en privat och en publik kodnyckel. Trots att PGP är baserad på den omdebatterade krypteringsalgoritmen RSA, som är förbjuden att exportera från USA, är PGP-programmen nu spridda över hela Internet.[167]

PIN: Personal Identification Number[168]

PKI: Public Key Infrastructure.

PKIX: Public Key Infrastructure som bygger på X.509 säkerhetsstandard.

Protokoll: Regler för datakommunikation. De regler för sändning och mottagning som gäller för alla terminaler anslutna till en gemensam kommunikationslinje.[169]

[165] IT-ordlista & www-adresser, STF Ingenjörsutbildning AB, utg. 3, Sthlm, 1996.
[166] Se vidare http://www.mot.com/MIMS/ISG/Products/pcmcia/pocket_guide/pcmcia_faqs/
[167] Se vidare http://www.pgp.com samt http://www.pgpi.com
[168] IT-ordlista & www-adreser, STF Ingenjörsutbildning AB, utg. 3, Sthlm, 1996.
[169] IT-ordlista & www-adresser, STF Ingenjörsutbildning AB, utg. 3, Sthlm, 1996.

Public key-krypteringssystem: Kryptering som bygger på asymmetrisk kryptering. De kommunicerande parterna är var och en utrustad med två nycklar som är förbundna med varandra på så vis att en text som är krypterad med hjälp av den ena nyckeln (oavsett vilken) bara kan dekrypteras med hjälp av den andra nyckeln. Namnet ”Public Key” föranleds av att man genom ett sådant system kan etablera en instans hos vilken den ena (den offentliga) av nycklarna är registrerad och som i förhållande till potentiella kommunicerande parter förklarar vilka personer det är som har registrerat de offentliga nycklarna.[170]

RC2 och *RC4:* Kryptografiska metoder som med vissa begränsningar tillåts exporteras från USA.[171]

SSL: Secure Socket Layer. [172] Krypteringsprotokoll för direktkommunikation på Internet.

SHA-1: Secure Hash Algorithm. Amerikansk federal standard för ”information processing”[173]

S/MIME: Secure Multipurpose Internet Mail Extension. Säkerhetsanpassad standard för epost på Internet.[174]

SOGIS: Senior Officials Group – Informations Security. Grupp bestående av ämbetsmän som skall ge råd till EU-kommissionen i frågor om IT-säkerhet.[175]

[170] Danmarks IT-sikkerhedspolitik - et baggrundspapir, Forskningsministeriet, nov. 1996 sv. översättn. PTS.
[171] För mer detaljerad information, se http://www.rsa.com/rsalabs/newfaq/alg_tech.htm
[172] Se vidare http://www.rsa.com/rsalabs/newfaq/q134.html
[173] Se vidare http://www.rsa.com/rsalabs/newfaq/q100.html
[174] Se vidare http://www.rsa.com/rsalabs/newfaq/q131.html
[175] Danmarks IT-sikkerhedspolitik - et baggrundspapir, Forskningsministeriet, nov. 1996, sv. översättn. PTS.

Standard: en teknisk beskrivning eller annat för allmänheten tillgängligt dokument, som är utformat i samarbete med alla berörda intressenter i samstämmighet eller med allmänt godkännande, grundat på det samlade resultatet av vetenskap, teknik och erfarenhet, inriktat på att uppnå de bästa fördelar för samhället samt fastställd av ett standardiseringsorgan.

TCP/IP: Transmission Control Protocol/Internet Protocol. Protokoll som används på Internet och som delar upp strömmen av data i paket och ser till att paketen ankommer till rätt destination.

Telemeddelande: Ljud, text, bild, data eller information i övrigt som förmedlas med hjälp av radio eller genom ljus eller elektromagnetiska svängningar som utnyttjar särskilt anordnad ledare.[176]

Telenät: en anläggning avsedd för förmedling av telemeddelanden[177]. Internet är ett allmänt tillgängligt datanät och utgör därmed ett allmänt tillgängligt telenät enligt telelagen.

Teletjänst: Förmedling av telemeddelande för någon annan.[178] (Tjänster som tillhandahålls över Internet är t.ex. elektronisk post (e-post), filöverföringar (FTP), News och webb-tjänster (WWW).)

Televerksamhet: Förmedling av telemeddelanden via telenät eller tillhandahållande av nätkapacitet.[179]

TLS: Top Level Security. Säkerhetsnivå överst i en hierarkisk CA-struktur.[180]

TTP: Trusted Third Party, tillförlitlig tredje part[181]

[176] 1 § telelagen (1993:597).
[177] 1 § telelagen (1993:597).
[178] 1 § telelagen (1993:597).
[179] 1 § telelagen (1993:597).
[180] CA-policies i praktiken, TeleTrust/Telia Promotor AB. Rapporten finns tillgänglig på http://www.teletrust.se/capol/capolsve.doc

UNCITRAL: United Nations Commission on International Trade Law.[182]

Uppgift: En uppgift skulle enligt Datalagskommittén, SOU 1997:39, s. 499, kanske kunna betecknas som den minsta uppfattbara enhet som har ett sakligt innehåll. Kommittén ansåg att det inte behövde införas någon sådan definition i lagen.

Urkund: Protokoll, kontrakt, skuldebrev, intyg och annan handling, som upprättats till bevis eller eljest är av betydelse såsom bevis, så ock legitimationskort, biljett och dylikt bevismärke. (14 kap. 1 §, 2 st. Brottsbalken)

X. 500: Standard för katalogfunktioner i meddelandehanteringssystem/epost.[183]

[181] Danmarks IT-sikkerhedspolitik - et baggrundspapir, Forskningsministeriet, nov. 1996, sv. översättn. PTS.
[182] Se http://www.un.or.at/uncitral
[183] IT-ordlista & www-adresser, STF Ingenjörsutbildning AB, utg. 3, Sthlm, 1996.

Bilaga 11

Lista på personer som bidragit i arbetet på denna promemoria

Följande personer har varit behjälpliga vid utarbetandet av promemorian: Stefan Bernhard, Lagerlöf & Leman, Per Christoffersson, Telia Promotor AB, Simon Corell, AU-system, Per Furberg, Göteborgs tingsrätt, Patrik Fältström, Tele2, Ingela Halvorsen, Datainspektionen, Sören Hansson, Handikappinstitutet, Stefan Hellberg, QA Information Security, Mari-Ann Ahlström-Hjulbäck, SEIS, Kerstin Wiss Holmdal, Kommunförbundet, Christina Hultmark, Göteborgs universitet, Pär Höglund, Telia Promotor AB, Torbjörn Hörnfeldt, Riksarkivet, Ulf Jonströmer, AU-system, Ingemar Kjellberg, SET-projektet, Gunnar Klein, GK AB, Hans Lindén, Apotekarsocieteten, Patrik Lindskoug, Lunds universitet, Eva Lundevall, Säkdata AB, Lennart Malmström, Posten, Bengt-Erik Nilsson, ÖCB, Hans Nilsson, AU-system, Jari Nyholm, Nordbanken, Jan-Åke Olander, ÖCB, Jesper Skagerberg, Nexus Technology AB, Hans Tholander, Dynamic Software AB, Christian Wettergren, KTH/IT samt Erik Woodcock, Advokafirman Delphi.

Från Post- och telestyrelsen har följande personer deltagit i arbetet: Britt-Marie Arne-Hellström, Jan-Olof Borgén, Karoline Boström, Ann-Sofi Hovmöller, Henrik Nilsson, Christian von Szalay, Malen Lindman Terud, Lars Trägård samt Hans Öjemark.