IDENTIFIERING OCH IDENTITET I DIGITALA MILJÖER

Hearing anordnad av
Kommunikationsdepartementet,
Närings- och handelsdepartementet,
IT-kommissionen, SEIS, EDIS och Swebizz

Andrakammarsalen, Riksdagen 1997–11–12

IT-kommissionens rapport 4/98

Ur KB:s samlingar
Digitaliserad år 2015

KUNGL. BIBLIOTEKET
National Library of Sweden

Secured Electronic Information in Society

EDI-föreningen EDIS i Sverige

Swebizz

Kommunikationsdepartementet

REGERINGSKANSLIET

Närings- och handelsdepartementet

IT-kommissionen 103 33 Stockholm Besök: Regeringsgatan 30–32
E-post: itkommissionen@communications.ministry.se
Webtjänst: http://www.itkommissionen.se

IDENTIFIERING OCH IDENTITET I DIGITALA MILJÖER

Hearing anordnad av
Kommunikationsdepartementet,
Närings- och handelsdepartementet,
IT-kommissionen, SEIS, EDIS och Swebizz

Andrakammarsalen, Riksdagen 1997–11–12

IT-kommissionens rapport 4/98

SEIS
Secured Electronic Information in Society

IT KOMMISSIONEN

REGERINGSKANSLIET
Kommunikationsdepartementet

EDI-föreningen EDIS i Sverige

Swebizz

REGERINGSKANSLIET
Närings- och handelsdepartementet

IT-kommissionen 103 33 Stockholm Besök: Regeringsgatan 30–32
E-post: itkommissionen@communications.ministry.se
Webtjänst: http://www.itkommissionen.se

Ref K
Occ 50

Statens offentliga utredningar
1998:36
Kommunikationsdepartementet

Identifiering och identitet i digitala miljöer

Referat från en hearing den 12 november 1997
IT-kommissionens rapport 4/98

Delbetänkande av IT-kommissionen
Stockholm 1998

SOU och Ds kan köpas från Fritzes kundtjänst. För remissutsändningar av SOU och Ds svarar Fritzes Offentliga Publikationer på uppdrag av Regeringskansliets förvaltningsavdelning.

Beställningsadress: Fritzes kundtjänst
106 47 Stockholm
Orderfax: 08-690 91 91
Ordertel: 08-690 91 90
E-post: fritzes.order@liber.se
Internet: www.fritzes.se

Svara på remiss. Hur och Varför. Statsrådsberedningen, 1993.
- En liten broschyr som underlättar arbetet för den som skall svara på remiss.

Broschyren kan beställas hos:
Regeringskansliets förvaltningsavdelning
Distributionscentralen
103 33 Stockholm
Fax: 08–405 10 10
Telefon: 08–405 10 25

Elanders Gotab, Stockholm 1998

ISBN 91-38-20873-3
ISSN 0375-250X

Identifiering och identitet i digitala miljöer

Hearing anordnad av
Kommunikationsdepartementet,
Närings- och handelsdepartementet,
IT-kommissionen, SEIS, EDIS och Swebizz

Andrakammarsalen, Riksdagen, 1997-11-12

Rapport

Innehåll

Översikt

Innehåll

Detta dokument innehåller följande:

	Sida
Förord	5
Inledning	7
Del 1: Slutsatser från hearingen	9
Del 2: Referat från hearingen (detaljerad innehållsförteckning)	17
Bilaga: Information om SEIS	99

Förord

Kommunikationsdepartementet, Närings- och handelsdepartementet, IT-kommissionen, SEIS, EDIS och Swebizz genomförde den 12 november 1997 en hearing om identifiering och identitet i digitala miljöer.

Väl fungerande sätt för identifiering är grundbulten i en kommande nätbaserad ekonomi. Om många olika typer av angelägen alla-till-alla-kommunikation ska bli verklighet för förvaltningar, näringsliv och enskilda är detta att kunna säkerställa identiteten helt nödvändigt. Identifikationsproblemet rymmer frågor kring digitala signaturer, digital identifiering och konfidentialitet. Samtidigt finns behovet av skydd för den enskildes integritet.

En del av utvecklingen är redan igång. Sjukvården, affärsbankerna och flera myndigheter har uppmärksammat betydelsen av ett entydigt identifieringsförfarande och där pågår ett införande. Toppledarforum har beslutat om ett tjänstekort i offentlig förvaltning för digital identifiering.

Bland väsentliga frågor som belystes i hearingen är

- varför det behövs nya sätt för identifiering i informationssamhället
- vilka som är berörda och vilka behov det finns av identifiering för nya tillämpningar
- vad som krävs för införande i Sverige och vad som kan införas
- hur vi bäst ska införa system för identifiering och hur berörda intressen ska avvägas.

Denna rapport ger ett utförligt referat av hearingen samt ett antal slutsatser från det efterföljande analysarbetet.

Kommunikationsdepartementet	Närings- och handelsdepartementet
IT-kommissionen	Secured Electronic Information in Society (SEIS)
EDIS	Swebizz

Inledning

Magnus Persson, Kommunikationsdepartementet:

Magnus Persson är statssekreterare vid Kommunikationsdepartementet.

"Nu utreder regeringen digitala signaturer"

Det är hög tid att komma vidare när det gäller användningen av Internet. Det räcker inte med att bara kunna kommunicera och hämta information. Vi måste skapa ett brett förtroende för systemen och vi måste kunna agera på nätet med stor säkerhet.

Vägen till säkerhet, till trygghet och förtroende, går bl a via möjligheten till säker identifiering och användning av digitala signaturer. För att kunna göra avtal av vikt via Internet måste det vara möjligt att bevisa att jag är jag och det på ett sätt som är ställt utom alla tvivel. Vi måste kunna sluta skriftliga avtal med rättsligt bindande verkan för att vi ska kunna använda potentialen fullt ut. För detta krävs digital signatur, en säkrad identitet.

Det är först när vi når dit – och det på en nivå som är accepterad av det stora flertalet användare och inte minst myndigheterna – som vi kan ta det riktigt stora klivet in i informationssamhället. Det är då vi kan börja arbeta på olika sätt över näten i stor skala. Det är då vi kan sköta många av våra myndighetskontakter via dator på distans, antingen hemma eller på arbetsplatsen. Därtill kommer en bred spridning av informationskiosker i offentliga miljöer som allmänheten kan utnyttja för tjänster av olika slag. I det perspektivet räcker inte dagens enkla lösenord. Då måste användarens identitet och behörighet vara betydligt bättre säkrad.

På vägen dit finns ett antal problemområden som behöver bearbetas och utvecklas, t ex möjligheterna till kryptering, hanteringen av digitala certifikat och olika sätt att skapa säkra betalningssystem. Ett aktuellt steg på den vägen är att regeringskansliet påbörjar ett arbete för att göra en problem- och behovsbeskrivning om digitala signaturer.

Del 1: Slutsatser från hearingen

Översikt

Slutsatserna från hearingen om identifiering och identitet i digitala miljöer är att

Stor förväntan

1. förväntningarna är stora bland alltfler myndigheter och företag på att kunna utföra arbete av skilda slag i befintliga öppna nät och för att det ska ske behövs införande av säkra system för digital identifiering och digital signatur

Tilliten avgörande

2. avgörande för framgången är att det finns hög tillit till de system som införs och det är helt beroende på systemens utformning. Ett stegvis införande är att föredra framför en snabb komplex helhetslösning som i sig kan medföra bristande tillit. Viktigt är att finna balanspunkten mellan 1) rätten att vara anonym och 2) möjligheten till och skyldigheten att stå för sina handlingar

Uppenbara vinster

3. vinsterna med att införa system för digital identifiering och digital signatur är långsiktiga och svåra att mäta. Det finns knappast några direkta vinster att hämta i själva uppbyggnaden av infrastrukturen, utan vinsterna uppstår först i nästa led som utnyttjar tjänsterna i infrastrukturen. Såväl näringslivet som förvaltningar och vården ser stora uppenbara vinster komma i sina verksamheter genom ett införande av digital identifiering och digital signatur

Politisk debatt

4. tekniken finns i allt väsentligt, men det behöver komma igång en bred debatt och politisk hantering kring införandet. Anledningen till att detta ännu inte sker är att frågan är komplex och att incitamenten för en genomlysning saknas

Rättslig reglering

5. arbetet med att utveckla en näringsrättslig reglering bör påbörjas omedelbart så att ett regelverk i detta avseende kan vara på plats inom 4–5 år. Det finns annars risk för att Sverige kommer efter i utvecklingen. Ur andra rättsliga aspekter är detta ett komplext område som bör få utvecklas stegvis. Lagstiftarens strategi bör vara att följa utvecklingen och ändra vid behov. Alla försök till en heltäckande totallösning riskerar att leda till paralys

Bred front dröjer

6. internt i många stora företag och branscher är det angeläget med ett snabbt praktiskt genomförande och det förefaller som att de tekniska grundverktygen i allt väsentligt finns framme för det. En allmänt förekommande tjänst i Sverige kan däremot dröja 4–5 år eftersom det förutsätter att en infrastruktur är på plats

SEIS har försteg

7. den svenska SEIS-modellen för digital identifiering, digital signatur och kryptering bedöms idag ha ett internationellt försprång. Givet att den går att framgångsrikt införa i Sverige, är det möjligt att under internationella samarbetsformer få alltfler länder att ansluta sig till SEIS-modellen

Kulturell skillnad

8. synen på integritet är kulturbetingad och därför är det vanskligt att importera eller exportera systemlösningar för digital identifiering och digital signatur. Utöver globala system kommer det att finnas lokala system som tar hänsyn till den kulturbetingade synen på identitet och anonymitet.

Slutsats 1: Säkra system för digital identifiering behöver snarast införas

Förväntningarna är stora bland alltfler myndigheter och företag på att kunna utföra arbete av skilda slag i befintliga öppna nät. För att det ska ske behövs införandet av säkra system för digital identifiering och digital signatur.

Befintliga nät ger i grunden förutsättningar för ett mer utvecklat utnyttjande av den alltmer digitaliserade omgivningen i organisationer, samhälle och hushåll.

Väl fungerande sätt för identifiering är grundbulten i en växande nätbaserad ekonomi. Om många olika typer av angelägen alla-till-alla-kommunikation ska bli verklighet för förvaltningar, näringsliv och enskilda är detta att kunna säkerställa identiteten helt nödvändigt.

Identifikationsproblemet rymmer frågor kring digitala signaturer, digital identifiering och konfidentialitet. Det finns samtidigt behov av skydd för den enskildes integritet.

Slutsats 2: Hög tillit för systemen är helt avgörande för framgången

Avgörande för framgången är att det finns hög tillit till de system som införs och det är helt beroende på systemens utformning. Ett stegvis införande är att föredra framför en snabb komplex helhetslösning som i sig kan medföra bristande tillit. Det är viktigt att finna balanspunkten mellan 1) rätten att vara anonym och 2) möjligheten till och skyldigheten att stå för sina handlingar.

För att en infrastruktur som byggs upp för identifiering och identitet ska användas, behövs ett brett starkt förtroende och trygghet, d v s en hög tillit. Därför måste varje teknisk design testas mot tillitsperspektivet innan en lösning införs. Brist på tilltro till dessa (ekonomiska) system kan vara dyrbart. Det är därför viktigt att sträva efter hederliga system. Tillit går endast att skapa genom öppenhet och öppna lösningar och det är endast i undantagsfall som det går i ett slutet system.

System för identifiering kan bli för komplexa och det kan leda till bristande tillit. Därför gäller det att gå fram stegvis och inte göra det för komplext alltför snabbt. Komplexitet är ett hinder för tilliten och därför är det nödvändigt med en öppen debatt om hur lösningarna ska utformas. Det går nämligen inte att informera bort brist på tillit.

Balanspunkten mellan 1) rätten att vara anonym och 2) möjligheten till och skyldigheten att stå för sina handlingar är inte helt uppenbar vid övergången från konventionell miljö till IT-miljö. Det är viktigt att respektera såväl rätten att vara anonym som krav på identifiering.

Det är också viktigt att finna balanspunkten mellan 1) användarens behov av unik och säker identifiering och 2) systembyggarnas förmåga att tillhandahålla rationella och effektiva tjänster.

Det är nödvändigt att skilja på olika grader och nivåer av identifiering. Klassificering av säkerhetsfunktioner kan ge olika identifieringsbehov. Det finns också olika krav på identifiering i olika situationer, d v s olika säkerhetskrav och det är särskilt höga krav i offentlig verksamhet.

För viktiga ärenden inom och till myndigheter används ännu inte e-post, eftersom det inte går att få en säker kvittens på att ett meddelande kommit fram. Säker identifiering är helt nödvändig inom den offentliga sektorn. Förtroendet för offentlig verksamhet måste vara högt. Detta är aspekter som är viktiga att beakta vid varje införande av nya system.

Ett naturligt förtroende förutsätter betrodda miljöer (t ex Posten och banker har en lång tradition som inger förtroende och lämpar sig därför att vara denna betrodda miljö).

Frågan om införande av digitala identitetskort kan vara känslig från integritetssynpunkt, t ex med tanke på hur sådana system kan användas av en diktaturregim.

Slutsats 3: Uppenbara vinster, men de är långsiktiga och svåra att mäta

Vinsterna med att införa system för digital identifiering och digital signatur är långsiktiga och svåra att mäta. Det finns knappast några direkta vinster i själva uppbyggnaden av infrastrukturen, utan vinsterna uppstår först i nästa led som utnyttjar tjänsterna i infrastrukturen. Såväl näringslivet som förvaltningar och vården ser stora uppenbara vinster komma i sina verksamheter genom ett införande av system för digital identifiering och digital signatur.

Några förväntade vinster är att

- det inom offentliga sektorn genom att ett spektrum av nya tjänster blir möjliga går att t ex 1) korta handläggningstider och 2) ge medborgare enklare tillgång till information och tjänster
- inom vården är ökad tillit själva kärnan i verksamheten och därför går säkra system hand i hand med rationaliserande tillämpningar
- i företagen, där snabbhet och ökat tempo är allt tydligare framgångsfaktorer, finns omgående stora interna vinster att hämta när det går att komma ifrån pappershanteringen
- en lösning av identifieringsfrågan i interna system ger möjlighet att även lösa frågor om behörighet till olika uppgifter
- med digital signatur ökar bevisvärdet och därmed skyddet för individen
- Internet blir säkrare, tillgängligare och robustare.

Slutsats 4: Tiden är mogen NU för en politisk hantering av frågan

Tekniken finns i allt väsentligt, men det behöver komma igång en bred debatt och politisk hantering kring införandet. Anledningen till att detta ännu inte sker är att frågan är komplex och att incitamenten för en genomlysning saknas.

Tiden är NU mogen för en politisk hantering av frågan. Tekniken finns, men det behöver komma i gång en bred debatt och samverkan mellan utvecklingsmänniskor, politiker och andra intressenter som t ex media och samhällsdebattörer. Någon sådan debatt pågår ännu inte och det är inte bra för en sund utveckling. I den internationella debatten har det skett en kursändring från tidigare enbart nationella säkerhetsperspektiv till ett mera handelsorienterat synsätt. Ett globalt hinder är de restriktiva regleringarna av t ex bruk av krypteringsteknik. Det är en politisk fråga att hantera.

Det är likaså viktigt att i diskussionen kunna skilja mellan ett kort och ett lite längre perspektiv – vad kan göras nu och vad behövs om 4–5 år?

Det krävs således en helhetssyn på

- införande av digitala identitetsfunktioner
- lagstiftning
- ramverk.

Kommunikationsdepartementet har under hösten 1997 börjat arbeta med en problem- och behovsbeskrivning kring digitala signaturer och eventuellt lagstöd.

Slutsats 5: En näringsrättslig reglering bör påbörjas omedelbart

Arbetet med att utveckla en näringsrättslig reglering bör påbörjas omedelbart så att ett regelverk i detta avseende kan vara på plats inom 4–5 år. Det finns annars risk för att Sverige kommer efter i utvecklingen. Ur andra rättsliga aspekter är detta ett komplext område som bör få utvecklas stegvis. Lagstiftarens strategi bör vara att följa utvecklingen och ändra vid behov. Alla försök till en heltäckande totallösning riskerar att leda till paralys.

Ett generellt hinder är bristen på anpassad lagstiftning. En hämmande faktor är att den bristen gör att näringslivet inte vill ta några affärsrisker och offentliga sektorn vill inte riskera "trampa ut i det moras" som regelverket eller trakterna utanför regelverket innebär. Ett för starkt rättsligt ansvar kan hindra utveckling på området.

Det finns ur lagstiftningssynvinkel såväl hårda som mjuka frågor av olika svårighetsgrad:

	Hård fråga		
Lätt att lösa	Exempel: digital signatur		
		Exempel: tillit	Svår att lösa
		Mjuk fråga	

En näringsrättslig reglering behövs omedelbart. En utgångspunkt kan tas i den finansrättsliga regleringen.

Det finns olika synsätt på en kommande CA-struktur, t ex att antingen att var och en kan vara sin egen CA eller att det inte bör finnas fler CA än dem som idag ger ut identitetskort, d v s Posten och bankerna.

Ett hinder är att det inte är bestämt vilka regler som ska gälla för certifikat. Generellt bör det vara en strävan efter korta verifikationskedjor, även om dessa i princip går att göra mycket långa. Det är viktigt att skilja mellan att ett certifikat är bäraren av den logiska identifieringshandlingen och ett identitetskort är förvaringsplatsen för certifikatet.

När det gäller materiella och processuella frågeställningar finns redan mycket utrett och det bör tas tillvara. När det gäller tempot är det inte nödvändigt att fullständigt heltäckande lagstifta om digitala signaturer.

Detta är ett stort och komplext område som bör få utvecklas stegvis. Det finns t ex principiella skillnader i traditionell och ny teknik och det ställer krav på den nya infrastrukturen. Många frågor hänger samman och därför behövs en strategi. Alla försök till att skapa totallösningar är omöjliga utan att det leder till paralys.

Slutsats 6: Ett genomförande på bred front i Sverige kan ta 4–5 år

Internt i många stora företag och branscher är det angeläget med ett snabbt praktiskt genomförande och det förefaller som att de tekniska grundverktygen i allt väsentligt finns framme för det. En allmänt förekommande tjänst i Sverige kan däremot dröja 4–5 år, eftersom det förutsätter att en infrastruktur är på plats.

Det är viktigt att skilja på vad som går att göra nu på kort sikt och vad som behöver göras på längre sikt, inom 4–5 år. Statskontoret, t ex, tar ett steg i taget när det gäller införandet av system för identifiering i digitala miljöer och upphandlingen av tjänstekort kommer att ske tidigast hösten 1998

Internt i många företag och branscher är det bråttom med ett genomförande – behoven där är uppenbara och angelägna för affärsverksamheten och det verkar som att tekniken finns framme för ett praktiskt införande på kort sikt.

"Globalt", d v s som en allmänt förekommande tjänst i Sverige, kan ett genomförande ta 4–5 år eftersom infrastrukturen för detta ännu inte är framtagen. SEIS-modellen finns, men den återstår att införa.

Området är mycket komplext och därför gäller det att ta fram lösningar dels på kort sikt, dels på lång sikt – en stegvis utveckling är att föredra eftersom införande av ett "färdigt" komplext system är närmast omöjligt. En stegvis utveckling går att påskynda väsentligt genom incitament från regeringen och genom att sätta upp tydliga gemensamma mål.

Det är skillnad mellan digital identifiering och digital signatur ur såväl teknisk synvinkel som funktionellt användningsmässigt – därför kan områdena utvecklas/införas var för sig.

Det är nödvändigt att renodla och skarpt åtskilja funktionerna 1) signatur, 2) kryptering och 3) identifiering och sedan klart formulera vad som gäller nationellt och internationellt.

Posten förefaller att skynda på sitt utvecklingsarbete och har inte långt kvar till kommersiella tillämpningar med digitala signatur. Generellt finns tekniken, men tillämpningarna saknas. För att underlätta utvecklingen av tillämpningar har Posten tagit fram en verktygslåda.

Ett hinder kan vara en utdragen införandeprocess och den osäkerhet detta för med sig. Utvecklingen går olika snabbt i olika branscher, bankerna t ex har goda förutsättningar att hålla ett högt tempo – men hinder finns genom bristen på lagstiftning. Tempot i införandet beror på förmågan att samverka – med ett bra samspel kan det vara möjligt att redan under 1998 införa vissa lösningar. Generellt är det bråttom med en del kortsiktiga lösningar. I utvecklingen måste Sverige också hålla jämna steg och vara i samklang med viktiga internationella handelsparter, som t ex Tyskland.

När myndigheter inför system för digital identifiering och digital signatur kommer det att snabbt leda till stora framsteg genom en rad nya tillämpningar blir möjliga. Ett växelspel (höna/ägg) råder mellan utbyggnad av infrastrukturen och utvecklingen av tillämpningar som ger kundnytta – av värde är Statskontorets initiativ och att få lagstiftningen snabbt på plats.

Slutsats 7: Svenska SEIS-modellen anses ha internationellt försprång

Den svenska SEIS-modellen för digital identifiering, digital signatur och kryptering bedöms idag ha ett internationellt försprång och givet att den går att framgångsrikt införa i Sverige, är det möjligt att under internationella samarbetsformer få alltfler länder att ansluta sig till SEIS-modellen.

Generellt anses Sverige ha ett bra utgångsläge och ha värdefull erfarenhet av sådan samverkan som kommer att behövas för en framtida lyckosam spridning av SEIS-modellen internationellt. Sverige har högt anseende vad gäller teknisk nivå och samhälleliga strukturer och finns med i viktigt internationellt arbete som kan ha betydelse för SEIS internationellt.

Det förefaller som att SEIS-modellen har ett försprång internationellt sett – det är en unik standard – och om det går att snabba upp det kvarvarande arbetet för att göra modellen färdig, kan det vara möjliga att sälja den utomlands. SEIS-modellen kan vara gångbar i först i Norden, sedan i Europa och så småningom även andra delar av världen. Men ett krav för detta är att den först måste vara införd i Sverige och visa sig fungera där, sedan går det att genom samarbete (inte "invasion") få alltfler länder att ansluta sig till SEIS.

Det förefaller vara bråttom med den fortsatta utvecklingen och spridningen av SEIS-konceptet, eftersom andra konkurrerande lösningar kan komma att lanseras från andra håll. Sverige kan komma att leda utvecklingen.

Slutsats 8: Synen på integritet är mycket kulturbetingad

Synen på integritet är kulturbetingad och därför är det vanskligt att importera eller exportera systemlösningar för digital identifiering och digital signatur. Utöver globala system kommer det att finnas lokala system som tar hänsyn till den kulturbetingade synen på identitet och anonymitet.

Både globala och lokala system är möjliga. Det är nödvändigt med gemensamma internationella standarder för lokala system som i sin tur tar hänsyn till kulturbetingad syn på identitet. Tekniken som används i Sverige bygger på internationell standard. Ett hinder i utvecklingen är den globala oenigheten om krypteringskontrollen.

Del 2: Referat från hearingen

Detaljerad innehållsförteckning

Innehåll

Hearingen omfattar följande avsnitt:

	Sida
A: Varför behövs digital identifiering och signatur?	**21**
Behov av identifiering *Peter Seipel, Stockholms universitet:* **"Med elektroniska informationsbärare blir traditionell rätt osäker"** När papper som informationsbärare börjat lämna plats för elektroniska bärare har de traditionella rättsliga föranstaltningarna och skyddsmekanismerna blivit osäkra. Det handlar om osäkerhet både om vad som är godtagbara och tekniskt sett tillräckligt säkra tillvägagångssätt och om hur nya tekniska fenomen ska beredas plats i lagstiftningen. Ett grundproblem gäller i vilken utsträckning lagstiftningen kan och bör vara teknikoberoende och inriktas på funktionella krav på använda tillvägagångssätt.	23
Behov av tillit *Lars Ingelstam, Linköpings universitet:* **"Tilliten är nyckeln för att tekniska lösningar ska fungera"** Den rent tekniska designen av lösningarna för identifiering och identitet i digitala miljöer är nödvändiga att testa mot något slag av tillitsperspektiv. Lösningarna är icke neutrala. Tillit går endast att bygga på öppenhet och hederliga system.	27
Behov av IT-utveckling *Ulf Jonströmer, AU-System AB:* **"Smarta kort säkraste vägen för nya tillämpningar"** Smarta kort är det klart bästa sättet för identifiering och identitet i digitala miljöer.	31
B: Vilka är berörda?	**33**
Offentliga sektorns behov *Britta Johansson, Statskontoret:* **"Stora förväntningar på att få en infrastruktur för säker kommunikation"** Nya säkerhetslösningar är på väg i offentliga sektorn, men ett införande kan ta tid eftersom det bl a kan behövas anpassning av lagstiftning. Inom stat, kommun och landsting finns stora förväntningar på att få tillgång till en infrastruktur där i princip alla som vill kan nå alla i hela samhället. Ett första steg är att genomföra en beslutad upphandling av aktiva identitetskort (smarta kort) för tjänstemän. Men osäkerheten är stor om efterfrågan, tillämpningar och vilken teknik som är den mest hållbara för framtiden.	35

Fortsättning på nästa sida

	Sida
B: Vilka är berörda? (forts)	
Individens behov *Louise Yngström, Stockholms universitet:* **"Frågan är komplex och därför behövs ordentlig debatt och samverkan"** En kritisk fråga är att avgöra var balanspunkten ska sättas mellan a) privatpersoners behov att bli unikt och säkert identifierade över flera system och b) systembyggares förmåga att tillhandahålla rationella, effektiva och ekonomiskt försvarbara tjänster. Det finns många skäl att anta att sådana tjänster som vi normalt uppfattar som självklara, inte går att realisera med IT-stöd om inte individens identitet unikt och säkert kan klarläggas.	45
Näringslivets behov *Rabbe Wrede, Telefonaktiebolaget LM Ericsson:* **"Det är angeläget att vi snarast kan börja använda digitala signaturer"** Regeringen bör snarast legalisera digitala signaturer och ta kraftfulla initiativ för att uppnå ett harmoniserat globalt ramverk för digitala signaturer baserat på affärsbehoven för elektronisk handel över gränserna. Vinsterna för näringslivet kan bli enorma.	53
C: Vad krävs för ett införande? Vad kan införas?	**57**
Teknik *Hans Tholander, Dynamic Software AB:* **"Asymmetrisk kryptering skapar möjligheter för säkra tillämpningar"** En digital signatur kan användas för att garantera dels att en informationsmängd inte har förändrats och dels vem avsändaren är. Tekniken för digital signatur kallas "public key"-teknik och bygger på användning av s k asymmetrisk kryptering.	59
Tjänster *Evald Persson, Posten AB:* **"Vi är angelägna om att driva på uppbyggnaden av infrastrukturen"** Posten kommer att tillhandahålla sådana tjänster till marknaden som behövs för att ge en säker digital identitet.	63
Regelverk *Per Furberg, Utredningen om elektroniska pengar:* **"Det är hög tid att starta det näringsrättsliga arbetet nu"** I öppna system behövs en helt ny infrastruktur med alla de juridiska konsekvenser som det för med sig. Internationellt pågår en snabb rättsutveckling som i första hand tar sikte på de näringsrättsliga frågorna. I Sverige sker ännu inget och det är allvarligt eftersom vi ligger i framkant när det gäller att införa konkreta tillämpningar.	67

Fortsättning på nästa sida

	Sida
D: Hur kan system för digital identifiering/signatur införas?	**75**
Utfrågning	
Britta Johansson, Statskontoret	77
Anne-Marie Eklund-Löwinder, SNUS	80
Göran Ribbegård, Spri	82
Stefan Bernhard, Lagerlöf & Leman Advokatbyrå och ICC	85
Berne Landgren, Telia Megacom AB	88
Jerker Sjögren, Stockholms stad	90
Magnus Faxén, UD	92
Strategisk diskussion Thomas Falk, Industriförbundet Ulf Jonströmer, AU-System AB Peter Seipel, Stockholms universitet Gunnar Hedborg, IT-kommissionen	94

A. Varför behövs digital identifiering och signatur?

Översikt

Frågan om varför det behöver införas system för identifiering och identitet i digitala miljöer diskuteras från behovsperspektiven

- identifiering
- tillit
- informationsteknik.

Behov av identifiering

Peter Seipel, Stockholms universitet:
Peter Seipel är professor vid Institutet för Rättsinformatik, Stockholms universitet.

"Med elektroniska informationsbärare blir traditionell rätt osäker"

Inledning

Detta avsnitt belyser behoven av identifiering.

Budskapet

När papper som informationsbärare börjat lämna plats för elektroniska bärare har de traditionella rättsliga föranstaltningarna och skyddsmekanismerna blivit osäkra. Det handlar om osäkerhet både om vad som är godtagbara och tekniskt sett tillräckligt säkra tillvägagångssätt och om hur nya tekniska fenomen ska beredas plats i lagstiftningen.

Ett grundproblem gäller i vilken utsträckning lagstiftningen kan och bör vara teknikoberoende och inriktas på funktionella krav på använda tillvägagångssätt.

Grundfrågor för identifiering

Jätten i grottan, Cyclopen, frågade Odysseus vad han hette. Odysseus svarade: jag heter "Ingen". När sedan Odysseus kört den glödande pålen i jättens enda öga och gjort honom blind så att Odysseus och hans män kunde fly ur grottan vrålade jätten på hjälp. Vad har hänt? frågade hans jättegrannar. "Ingen" har stuckit ut mitt öga, skrek jätten. Nå då så, vad bråkar du om? sa grannarna, gå och lägg dig!

Episoden ur Odysséen handlar om tre grundläggande identifieringsfrågor.

- Den första gäller *krav på att identifiera sig.*
- Den andra gäller *det riktiga eller oriktiga bruket av identifikationer.*
- Den tredje gäller *konsekvenserna av att identifiera sig.*

Med dessa tre grundläggande frågor som utgångspunkt kan man veckla ut nästan hela rättsordningen. Identifiering och identitet spelar nämligen på olika sätt nyckelroller i rättsliga sammanhang av de mest skilda slag. Frågorna kan regleras klart och tydligt genom uttryckliga föreskrifter. Men det kan också handla om indirekt reglering och om skick och bruk som aldrig har fått någon precis formulering.

En sökning i SFS med orden "identitet" eller "identifiering" visar snabbt på bredden hos identifieringsjuridiken. Svaret innehåller 182 författningar som handlar om allt från fingeravtryck till användning av telefon vid rättegång, motorscooteråkning, handel med skrot, folkbokföring, identitetsbeteckningar för juridiska personer, patientjournaler o s v.

Kraven på identifiering

Kraven på identifiering kan avse fysiska personer, juridiska personer eller döda föremål (t ex fordon). I den digitala miljön kan det också bli aktuellt att identifiera procedurer, t ex i form av s k mobila agenter.

Kraven på att identifiera sig kan vara tillfälliga och speciella eller långvariga och grundläggande. Kraven kan avse identifiering på olika nivåer och de kan avse subjektet som helhet eller bara vissa aspekter, funktioner eller egenskaper hos subjektet.

Exempel: Tunnelbaneresenären måste kunna identifiera sig som en legitim, avgiftsbetalande resenär då inspektören kommer. Men det räcker att presentera färdbeviset. Mer än så behövs inte. Den som har biljetten eller månadskortet i beredskap behöver inte identifiera sin person närmare än så.

Identitetens kärna

I de tunga sammanhangen däremot gäller kraven identitetens kärna. Det handlar om en i princip entydig och fullständig bestämning av det subjekt som kravet riktar sig mot.

Förlitan på identifiering förlorar sin mening om det är medgivet att spela med olika identiteter och svårt eller omöjligt att i olika situationer kontrollera uppgivna identiteter.

Rättsordningen har lärt sig att undvika eller minska dessa problem genom att dels föreskriva bestämda tillvägagångssätt för identifiering, dels kringgärda identifieringar – t ex underskrifter på dokument – med särskilda rättsliga skyddsinrättningar, t ex straffrättsligt skydd mot urkundsförfalskning.

När papper som informationsbärare börjat lämna plats för elektroniska bärare har de traditionella rättsliga föranstaltningarna och skyddsmekanismerna blivit osäkra. Det handlar om osäkerhet både om vad som är godtagbara och tekniskt sett tillräckligt säkra tillvägagångssätt och om hur nya tekniska fenomen ska beredas plats i lagstiftningen. Ett av grundproblemen gäller i vilken utsträckning lagstiftningen kan och bör vara teknikoberoende och inriktas på funktionella krav på använda tillvägagångssätt.

Diskussionen om organisatoriska förhållanden kring utfärdandet av identitetsbevis och kontrollen av korrekt användning av dessa har också blivit mer komplicerad genom de digitala hanteringarna och medierna. Rättsordningen måste verka för ett organisatoriskt ramverk som både klarar omedelbara kontrollbehov och kontrollbehov som uppkommer långt efter det tillfälle när en identitet ursprungligen användes – t ex när riktigheten av ett intyg om en laboratorietest ifrågasätts i en produktansvarsrättegång 15 år efter det att testet ägde rum.

Situationen blir inte lättare genom att identifieringsbehoven i växande utsträckning uppkommer i gränsöverskridande sammanhang på globala datanät.

Konsekvens av identifieringen

Konsekvenserna av att identifiera sig har att göra med åtminstone tre i rättsliga sammanhang centrala förhållanden:

- Att ge upp anspråk på anonymitet.
- Att markera eller etablera rättspositioner.
- Att stå ansvar för informationsinnehåll.

Att ge upp anspråk på anonymitet är en förutsättning för många transaktioner. Det kan handla inte bara om en faktisk eller rättslig tvångssituation utan också om situationer där anonymiteten är till nackdel – t ex i sammanhang där identiteten innebär en konkurrensfördel genom sin koppling till renommé och goodwill för den identifierade.

Markering och etablering av rättspositioner sker i en lång rad sammanhang där subjekt företar rättshandlingar (t ex godtar avtalsvillkor) eller agerar för olika syften som har rättsregler knutna till sig (t ex sänder inlagor till en domstol).

Ansvaret för informationsinnehåll kan anknyta till yttrandefrihetsregleringen eller handla om utsagor och meddelanden som lämnas under straffansvar, t ex tulldeklarationer. Det kan också vara fråga om t ex en beslutsfattares ansvar för ett beslut.

Identifiering ofta viktigare än anonymitet

En avslutande reflexion om Odysseus: Hans bruk av identiteten "Ingen" var fyndigt och räddade honom och hans besättning ur en knepig situation.

Situationer där anonymiteten och täckmanteln är legitima förekommer givetvis i juridiken. Men frågan är om inte dessa situationer helt undanskyms av de långt fler situationer där identifieringen och identiteten är viktiga moment i olika rättsliga konstruktioner.

Vad hade hänt om Odysseus fortsatt sin lek och vid återkomsten till Ithaka låtit framföra budskapet till den väntande hustrun att "Ingen" hade kommit hem? Jo, hon skulle bums ha gift sig med någon av de sedan länge väntande friarna. "Ingen" hade haft något att beklaga sig över.

Behov av tillit

Lars Ingelstam, Linköpings universitet:
Lars Ingelstam är professor i teknik och social förändring vid Linköpings universitet.

"Tilliten är nyckeln för att tekniska lösningar ska fungera"

Inledning

Detta avsnitt belyser vikten av att kunna känna tillit till tekniska och ekonomiska system.

Budskapet

Den rent tekniska designen av lösningarna för identifiering och identitet i digitala miljöer är nödvändiga att testa mot något slag av tillitsperspektiv. Lösningarna är ickeneutrala. Tillit går endast att bygga på öppenhet och hederliga system.

Tekniken och tilliten

Kajsa hade plockat korgen full. Hon klev ut över den höga tröskeln och började bära den mot bron. Regnet sköljde ner från hennes ljusblå cellofan. Hon hann emellertid inte gå många steg förrän hon hörde hur Janssons vedboddörr flög upp. Tåbb kom rusande med långa kliv. Han ville ta korgen ifrån henne. Men hon vägrade att ge den helt. "Vi bär den båda två", sa hon. De tog i varsin ände av handtaget och bar in korgen.

Vad har detta utdrag ur en av 1900-talets mer betydelsefulla svenska romaner, Lars Ahlins "Tåbb med manifestet" (1943), att göra med tillitsperspektivet i förening med elektronisk handel o s v?

Texten har något elementärt att säga oss – men något som är lätt att glömma bort. Det är nämligen så att teknikens egenskaper hänger nära samman med möjligheten att bygga förtroende, att skapa tillit. En vedkorg som man lämpligen bär tillsammans, är ett annat slags teknik och ger en annan grund för tillit, än alternativa sätt att bära ved.

Tilliten <u>är</u> nyckeln

Den moderna forskningen om teknik och samhälle handlar ju inte särdeles mycket om vedkorgar. Den handlar snarare om stora, komplexa, svåröverskådliga tekniska system. Det IT-system som är plattformen för dagens överläggningar är i en viss mening det största system som mänskligheten någonsin har haft och någonsin har försökt sig på.

Det kan då vara nyttigt att gå tillbaka till den förra "hjältetekniken", det förra tekniska systemet som på något sätt symboliserade framsteget och stod som symbol för teknik och komplexitet, nämligen kärnkraften. Hur har åsikter och förtroende skapats runt den komplexa tekniken?

Den empiriska forskningen visar att nyckelfrågan kring kärnkraftstekniken tycktes vara tillit. De som i allmänna drag var positiva till denna teknik fäste avseende vid tekniska prestationer, miljö och ekonomi. De som var negativa fäste avseende vid miljö, men också vid det slags sociala system som bar upp tekniken, det som "bäddade in" den och vilka som ansvarade för den.

Från det kan vi bära med oss en viktig iakttagelse, när vi ser på andra tekniska system. Det är inte särdeles poängfullt att försöka <u>informera</u> bort brist på tillit. Brist på tillit eller närvaron av tillit skapas nämligen på andra sätt.

Vad tillit är

Tillit är, enligt en bruksdefinition ur litteraturen,

"tilltron att de som du arbetar med ska ta dina intressen i beaktande, även i sådana lägen när du inte är i någon position att strikt försvara dina egna intressen."

Därför är tilliten särskilt viktig

Det finns tre skäl till att tillitsperspektivet gör sig påmint nu i vår samtida diskussion om teknik, samhälle och människa.

- En del stora komplexa system måste vara så beskaffade att vi till dem kan fästa tilltro om nästan total felfrihet. Det gäller flygledningssystem, många datasystem och energisystem.
- Vi börjar att inse något som ekonomiska filosofer lär ha vetat i flera hundra år, nämligen att en brist på tilltro i det ekonomiska livet är utomordentligt dyrbar. Om man eroderar det slags förtroende som affärstransaktioner och annat hänger på, kommer det att bli mycket dyrbart att installera de kontroller och säkerheter som gör att man trots allt kan fungera. I slutänden kan hela det ekonomiska systemet klappa igenom eftersom grundförtroendet inte föreligger.
- Den politiska demokratin är i växande grad skyldig att ta ställning till vissa av våra större system. Den måste behandla energisystemet och andra publika system som har stor betydelse för samhällslivet. Tillståndsgivning m m kräver politisk demokratisk ansvarighet.

Datasträng – inte ansikte

Det är nyttigt att också här göra en historisk tillbakaåkning. I ett enklare samhälle, säg för drygt hundra år sedan, fanns det egentligen inte någon skillnad mellan tilltro till en människa och tilltron till ett system. Mänskliga processer som t ex handel, krig och konst skulle alla en gång ageras ut ansikte-mot-ansikte med andra människor. Men redan genom den moderna staden och dess tekniska instrumentering, blev det en skillnad mellan system och individ. Det blev en skillnad mellan ansikte-mot-ansikte och tilliten till det hela. En lång rad relationer blev instrumentella, snarare än personliga.

Idag utgår vi mer eller mindre ifrån att vi är inne i en tredje fas, bortom det relativt enkla agrara samhället, men också bortom den moderna staden som arketyp för en samhällsform, till något slags samhällsform där vi har ännu en nivå av mänsklig relation.

Vilket relation kan etableras med en person som möter oss snarare som en datasträng än som ett ansikte? Vi ska inte vara alldeles säkra på att skillnaden är jättestor. Många erinrar sig Joseph Weizenbaums framgångar med den virtuella psykiatern Eliza som han fick att verka väldigt människolik. Så en del av problemet är inte att de identiteter till vilka man ska hysa tillit är så olika. Problemet kan istället vara att de är till förväxling lika.

Så byggs tillit

Slutligen kan det vara bra att fråga sig vad som går att hämta ur litteraturen om sådana faktorer som kan bygga tillit – om vi allmänt är överens om att tillit både till system och till personer, är ett problem som vi behöver tänka på. Tillit mellan två parter bygger på att

- det råder respekt mellan parterna – en respekt som i allmänhet måste bygga på en bekantskap och en ömsesidig förståelse
- det finns en kompetens, en insikt, så att det är möjligt att bedöma den andra partens kompetens och den andra partens syn på sina egna problem
- andelarna i ansvaret för att formulera spelreglerna parterna emellan är ganska lika
- det går att urskilja en positiv historia av relationer och en bevisad förmåga att ta på allvar de omständigheter som påverkar parternas relation
- parterna ska ha möjlighet att bedöma relativt tydligt och klart konsekvenser med en viss handling – en handling som jag gör mot dig, en handling som du gör mot mig. Denna sista egenskap har kanske den mest problematiska innebörden för den tekniska utvecklingen: i komplexa system är orsak och verkan svåra att urskilja.

Testa tekniken i tillitsperspektiv

Dessa dimensioner i tillitsbyggande är inte så lätta att åstadkomma i samband med stora tekniska system. Det är egentligen därför vi behöver föra denna diskussion. De är inte lätta att åstadkomma i energisystemen. De är verkligen inte lätta att åstadkomma i samband med datanät och virtuell kommunikation.

Det leder till tre grundläggande minnespunkter för fortsättningen:

- Testa den rent tekniska designen av lösningarna mot ett tillitsperspektiv! Lösningarna är icke neutrala. I själva verket är de mycket mer ingripande i förmågan att visa tillit än vad vi oftast har lust att räkna med.

- Bygg tillit av öppenhet! Tro inte på den som vill ha slutna system, begränsad insyn, tredubbla lås. Ibland måste man acceptera sådana, men de har alltid bevisbördan emot sig.

- Sträva efter hederliga system! Hederliga människor, hederliga instrumenteringar.

Behov av IT-utveckling

Ulf Jonströmer, AU-System AB:
Ulf Jonströmer är VD för AU-System AB, Stockholm.

"Smarta kort säkraste vägen för nya tillämpningar"

Inledning

Detta avsnitt belyser varför digital identifiering/signatur behövs i IT-perspektivet.

Budskapet

Smarta kort är det klart bästa sättet för identifiering och identitet i digitala miljöer.

Säker identifiering är ett krav

Problemet är idag inte längre att kommunicera genom min PC på ett säkert sätt med t ex bankens dator över Internet på ett säkert sätt som ingen kan avlyssna eller förvränga. Problemet är istället att säkerställa att det är rätt person – och inte någon annan – som sitter bakom tangentbordet och genomför olika transaktioner.

Alternativa sätt för identifiering

Det finns flera alternativa sätt för att lösa problemet i ett IT-perspektiv. Ett traditionellt sätt att identifiera sig på ett säkert sätt, är att ange person- eller kundnummer plus ett lösenord. Efterhand måste vi komma ihåg många sådana lösenord och de är ganska statiska över tiden.

Ett något bättre alternativ är engångslösenord, d v s att banken lämnar ut en lista en lista på lösenord där användaren stryker ett efter ett allt eftersom de används. Ett tredje sätt, särskilt i bankvärlden, att använda en liten säkerhetsdosa (lösenordsdosa) som genererar lösenordet.

Den lösning som SEIS[1] står bakom bygger på användning av smarta kort (aktiva kort) och den har likheter med säkerhetsdosan i bemärkelsen att det är någonting som är fysiskt. Det sista sättet att är biometri, t ex att använda fingeravtryck eller någon annan kroppsdel för att koppla transaktionen till en individ.

Rangordning

En betygssättning med skalan 0–5 för de olika metoderna visar följande:

Metod	Identifiering (betyg)	Signatur (betyg)
Lösenord	1	0
Engångslösenord	2	0
Säkerhetsdosa för lösenord	3	2
Smart kort (SEIS)	4	5
Biometri	5	0

Bland alternativen framstår tekniken med smarta kort som sammantaget den bästa.

[1] Secured Electronic Information in Society, SEIS, är en ideell svensk förening med ett femtiotal förvaltningar och företag som medlemmar. Föreningens syfte är att höja IT-säkerheten främst för nätanvändare som fokuserar på säker kommunikation, säkert distansarbete i nätverk och säker elektronisk handel.

SEIS-konceptet ger plattformen

Tekniken med smarta kort och kryptering med öppen nyckelteknik kan tyckas som någonting nytt, men har funnits sedan femton år.

Det intressanta idag är att SEIS har tagit fram specifikationer och förslag till standarder, som också en rad leverantörer har ställt sig bakom. SEIS har en mycket central roll när det gäller att skapa den viktiga bryggan mellan själva tekniken och befintliga och nya tillämpningar där tekniken är användbar. Det som fordras nu är utvecklingen av ett antal programvarumoduler

- för att kunna skapa det som är identiteterna, att kunna ge ut dem på ett säkert sätt, att stoppa in dem på ett tillförlitligt sätt på det smarta kortet så att det inte går att knäcka och att den som är utgivare kan ställa sig bakom som garant för kortet
- som kan dra nytta av identiteterna, de smarta korten, för att identifiera och generera signaturer o s v.

Öppnar för nya tillämpningar

Det traditionella tekniska perspektivet har handlat mycket om att låsa in information för att skydda den mot skurkar – och det är helt visst fortfarande giltigt.

Men i dagens läge är tekniken också en nyckel för att säkert komma åt information och för att möjliggöra för att göra bankärenden på Internet, studera en sjukjournal eller säkert göra en deklaration över nätet.

B. Vilka är berörda?

Översikt

Här diskuteras vilka behov som finns av digital identifiering och signatur för olika tillämpningar hos

- offentliga sektorn
- individen
- näringslivet.

Offentliga sektorns behov

Britta Johansson, Statskontoret:

Britta Johansson är organisationsdirektör vid Statskontoret, Stockholm.

"Stora förväntningar på att få en infrastruktur för säker kommunikation"

Inledning

Detta avsnitt belyser offentliga sektorns behov av system för säker identifiering och identitet i digitala miljöer.

Budskapet

Nya säkerhetslösningar är på väg i offentliga sektorn, men ett införande kan ta tid eftersom det bl a kan behövas anpassning av lagstiftning. Inom stat, kommun och landsting finns stora förväntningar på att få tillgång till en infrastruktur där i princip alla som vill kan nå alla i hela samhället. Ett första steg är att genomföra en beslutad upphandling av aktiva identitetskort för tjänstemän. Men osäkerheten är stor om efterfrågan, tillämpningar och vilken teknik som är den mest hållbara för framtiden.

Projekt inom Toppledarforum

Det arbete som sker sedan tre år inom Toppledarforum[2] sammanfattar behov och kravställan inom offentlig verksamhet. Projekt inom Toppledarforum berör bl a rättsliga frågor vid övergång till elektronisk kommunikation, de berör elektronisk post, elektronisk handel, plattform för informationsutbyte och en gemensam WWW-ingång.

Nödvändigt med lagändring

Toppledarforum gjorde 1994–95 studien Lexit om lagliga hinder för en "elektronisk förvaltning", d v s om en övergång till elektronisk kommunikation kan innebära samma rättsverkan och samma funktioner som den traditionella pappersbaserade hanteringen.

Uppföljningen Post Lexit visar att en del har hänt. Men fortfarande finns mycket att göra när det gäller lagstiftning. Det är problem och ofullständigheter i bl a förvaltningslagen, datalagen och tryckfrihetsförordningen där offentlighetsprincipen ingår. På väg i datalagskommitténs förslag finns begreppet "allmän uppgift" som ersätter allmän handling.

Sekretesslagen hindrar rationellt utnyttjande av teknik när olika delar av t ex en kommun utgör olika myndigheter. Ändringar i begreppen myndighet kan här rationalisera uppgiftslämnande mellan myndigheter.

Ett exempel är utredningen om Elektronisk dokumenthantering. Där föreslås enkla medel att ändra i förvaltningslagen, så att det enkelt går att acceptera digital signatur.

Det är en hel del som krävs för att åstadkomma den tillförlitliga, stabila och öppna elektroniska infrastruktur som är nödvändig för en IT-baserad dokument- och ärendehantering som inkluderar full rättsverkan och personanknutet ansvar.

---

[2] På senare år har mycket av gemensamt arbete kring IT i offentlig sektor bedrivits inom ramen för Toppledarforum. Toppledarforum är en sammanslutning av generaldirektörer i ett antal stora statliga myndigheter, en landshövding och direktörer i Svenska Kommunförbundet och Landstingsförbundet. Toppledarforum leds av finansminister Erik Åsbrink. Syftet med Toppledarforum är att använda IT för att skapa en effektiv och serviceinriktad offentlig verksamhet. Detta innebär även att använda tekniken för att nå mellan myndigheter, mellan myndigheter och företag, och myndigheter och allmänhet.

Toppledarforum är även ett unikt sätt att samarbeta i sektorsgränserna mellan stat, kommun och landsting. Arbetet i Toppledarforum bedrivs i projektform, där olika deltagare i Toppledarforum har åtagit sig projektledarskapet. Utvecklingen har i stor utsträckning sammanfallit med genombrottet för Internet och det har präglat Toppledarforums arbete. Flera av Toppledarforums projekt har fastslagit att när det gäller informationskanaler med och mellan många, finns det definitivt ingen konkurrent till Internet och dess teknik.

Olika profiler för användning

Toppledarforums projekt "Gemensamma plattformar för informationsutbyte" strukturerar frågeställningarna kring identifiering och användningen av öppna nät. Här framgår vilka olika tillämpningar som är angelägna och när och hur det behövs identifiering och vad det ställer för krav på utvecklingen.

Projektet definierar fyra användningsprofiler när det gäller pålitlig kommunikation mellan myndigheter om omvärlden – dessa är

1. Spridning av myndighetens information (främst webb-information).
2. och 3. Individ- och företagsspecifik information till och från myndigheten.
4. Samverkan i ärenden mellan olika myndigheter.

Klassning för säkerheten

En del av arbetet rör säkerhetsfunktioner, funktioner för identifiering, insynsskydd o s v och resultatet är fem klasser av säkerhetsfunktioner och en definition av säkerhetsfunktionaliteten.

Säkerhetsklassningen av s k spridnings- och hämtningssystem består av:

Klass 1
Det finns även skäl att informationslämnaren är säkert identifierad, när det gäller upplysningar från myndigheter. Det kan, när det gäller spridningssystem, ibland finnas behov av att identifiera vem som efterfråga viss information. Emellertid har detta projekt inte ansett att någon speciell identifiering behövs för spridning av allmän information från myndighet till allmänhet. Exempel: lagtext, bestämmelser, platsannonser.

Klass 2
Offentlig information som sprids mot betalning ställer krav på identifiering av mottagaren.

Klass 3
Information om en enskild individ från myndigheten ställer krav på säker identifiering, åtkomstkontroll och spårbarhet. Även åtkomstskyddad överföring är lämplig. Exempel: utdrag ur datalagen.

Klass 4
Information från en enskild person eller företag till en myndighet, utan krav på underskrift, ställer krav på säker identifiering och spårbarhet. Exempel: tillfällig adressändring.

Klass 5
När uppgifter från allmänhet eller företag till myndighet ställer krav på underskrift kommer krav på säker identifiering, spårbarhet, säker överföring, signering och kvittens. Det kräver tillgång till utrustning som medger digital signatur och att myndigheten har fått möjlighet att acceptera en digital signatur. Exempel: deklaration och ansökan om bostadsbidrag.

Flera av de beskrivna kontaktvägarna realiseras lämpligen med elektronisk post.

Elektronisk post

Toppledarforum har haft ett särskilt projekt kring elektronisk post där vi också har gjort en del struktureringsarbete för olika säkerhets- och pålitlighetsnivåer på elektronisk post, dels hur det ska överföras men också hur det ska tas om hand inom myndigheten, kommunerna eller landstinget. Idag finns det ganska mycket frågor. Människor på myndigheter undrar t ex: "Kan vi ta emot e-post? Vi måste ju se till att det blir diariefört. Måste vi publicera våra listor med inkomna poster?" Många sådana frågor finns fortfarande.

När det gäller användning av e-post i ren myndighetsutövning finns fortfarande en viss försiktighet från offentliga organ. I utredande och kontaktskapande arbeten är det inga större hämningar. Men i sammanhang där man måste följa sina regler finns en stor försiktighet.

Toppledarforums projektet för elektronisk post har definierat e-post på nivåerna

- e-kort
- e-brev
- e-rek.

De har olika grad av förtroende. I första hand rekommenderas SMTP-post för all e-postkommunikation. Den mest pålitliga elektroniska posten är döpt till "e-rek", med en association till rekommenderade brev. Men det ska inte tolkas bokstavligt, utan snarast att det är en elektronisk post som man kan lita på genom att man är säker på vem den kommer från och den får gärna vara insynsskyddad också genom kryptering. Det ska också finnas bra rutiner på myndigheten för att ta hand om inkommande och utgående e-post.

Arbetet med att försöka realisera den typ av säker elektronisk post som sträcker sig längre än mellan parter som kommit överens påbörjar vi nu. Hittills är det mer ett begrepp. Försöksverksamhet kan komma i gång under första halvåret 1998.

Elektronisk handel

Toppledarforums projekt kring elektronisk handel visar på ett definitivt behov av identifiering av de kommunicerande parterna.

Än så länge bygger lösningarna på att det är avtalsbundna parter, d v s det finns i förväg gjorda överenskommelser på papper mellan leverantör och upphandlande myndighet. I planerna för implementeringen av elektronisk handel ingår användningen av smarta kort (aktiva kort) för att hantera certifikat.

Det finns stora förväntningar

Alltså – när det gäller myndigheter, såväl statliga som kommunala och landsting, finns stora förväntningar på att man ska få tillgång till en infrastruktur där i princip alla som vill kan nå alla i hela samhället. I Toppledarforums olika projekt framgår ett stort framväxande behov av säker identifiering, möjlighet till signering och gärna även möjlighet till insynsskydd i form av kryptering.

Men det ställer också väldigt nya krav på förtroende, tillit, tillämpningar. Det gäller ju att vara försiktig, därför att vi får ju absolut inte i glädjen över att rationalisera med ny teknik skada förtroendet för offentlig verksamhet. Det är grundläggande att kunna lita på myndigheterna.

Frågan om säker identifiering är i det avseendet en grundfunktion. Det måste komma till stånd. Utöver det finns mycket annat som man måste kunna lita på näten.

Smarta kort (aktiva kort)

Ett projekt inom Toppledarforum av stort intresse handlar om smarta kort. Nu är behoven av identifiering, kryptering och signering identifierade. Det finns förslag om att dessa funktioner ska införas och att smarta kort ska användas för lagring av nycklar och certifikat. Det ska bilda grunden till en säkerhetslösning för den offentliga sektorn.

Bland önskemålen om ytterligare klarlägganden fanns kortutfärdande och certifieringsrutinerna inklusive den öppna-nyckel-infrastrukturen samt frågor kring sårbarheten. Här fanns också sådant som har att göra med lagstiftning på området och samhällets tillsyn av verksamheten.

Detta projekt har gjort en omfattande kartläggning av planerna i offentlig sektor på användning av smarta kort. Av kartläggningen framgick, att en tredjedel av de tillfrågade vid tidpunkten för enkäten hade erfarenhet av smarta kort eller beslut, planer och idéer om framtida användning av sådana. De viktigaste användningsområdena var kontroll av användares identitet i olika avseenden och behörighet till datorer och IT-system. Men planer fanns också på nyttiggörande användning av smarta kort som bärare av annan information.

Projektet föreslår att man skiljer på kort för anställda i offentlig sektor (s k anställningskort) och de kort som det är tänkbart att övriga aktörer, allmänhet och företag kan använda i sin kontakt med myndigheter (s k servicekort). I projektets slutsatser ingår till att börja med anställningskorten. Dessa kan användas för intern behörighet, men även för ärenden som hanteras mellan olika organisationer inom offentlig sektor. Förslaget att göra en upphandling av sådana kort bygger på att lösa kortsiktiga problem, men samtidigt bygga upp en struktur som passar in i andra aktiviteter och som har förmåga att växa till en gemensam lösning. Inte minst inom sjukvårdens område är behovet idag stort och flera landsting är på gång med planer.

Införande av smarta kort

Toppledarforum har beslutat att

- utreda rutiner och organisation för kortutfärdande och certifiering och därmed sammanhängande frågor för i första skedet den offentliga sektorn
- etablera av ett samordnings- och kompetenscenter för den offentliga sektorn (samordnat av Statskontoret) med uppgift att ge information, tips, råd och handfast vägledning
- upphandla (i regi av Statskontoret) rutiner för utfärdande och certifiering av smarta kort för tjänstebruk ("anställnings/personalkort") för att möta efterfrågan på kortbaserade säkerhetslösningar hos offentliga myndigheter och organisationer inom den närmaste tiden
- arbeta för att få till stånd de förändringar i lagar och andra regler som är nödvändiga för en effektiv IT-användning och IT-säkerhet – flera av dessa frågor är redan utredda i andra sammanhang

Inga invändningar är framförda i remissyttrandena mot att projektets tredje del även fullföljs, d v s att planer, idéer och tankar om nyttiggörande av "elektroniska servicekort" för allmänhetens kontakter med den offentliga sektorn också blir belysta. Några remissinstanser räknar i själva verket med att sådana servicekort kommer.

Ett bra elektroniskt servicekort för allmänheten är i detta avseende därför inte principiellt sett särskilt annorlunda än ett elektroniskt kort för tjänstebruk. Samma grundläggande funktioner behövs. Till skillnad från förslaget om smarta kort för tjänstebruk kan man däremot tänka sig, att servicekorten blir "bärare" av även annan information än de hemliga nycklarna.

Identitetskort och certifikat

Det är inte tänkt att de digitala kort som kommer att användas av tjänstemän ska bära en mängd information, utan vara inriktade på identifiering, signering och insynsskydd.

Här är en jämförelse mellan det konventionella identitetskortet av plast och den nya digitala identitetshandlingen, certifikatet.

	Fysisk identitetshandling **Identitetskort**	Digital identitetshandling **Certifikat**
Informationssäkring	Säkerhetstryck	Digital signatur
Identitetsuppgifter	Namn, personnummer (land)	Namn, personnummer (land)
Utfärdare	Kortutfärdare	Certifikatutfärdare
Kvalitetsmärkning	SIS	Certifikatpolicy
Unikt kännetecken	Foto, namnteckning	Publik nyckel

	Fysisk karakteristik	Digitalt identitetskort
Verifiering av innehavaren	Personens utseende samt förmågan att skriva namnteckning	Förmåga att använda rätt privat nyckel

Tillämpningar

Tillämpningar där det behövs säker identifiering är

- e-post generellt
- inom hälso- och sjukvården, t ex remisshantering, journaler och samspel mellan kommuner och landsting
- remisshantering mellan myndigheter och departement eller utredningar
- distansarbete (som ökar i betydelse även i offentlig verksamhet)
- behörighetskontroller
- i ett längre perspektiv många tillämpningar potentiellt möjliga för digital signatur i kommunikation med företag och medborgare.

Upphandling – en balansgång

Det kommer att ske en upphandling av smarta identitetskort för tjänstemän. Det arbetet är nyss påbörjat. Men det finns en hel del frågetecken att räta ut och det behöver göras ställningstaganden. Några frågor är

- Vad finns det egentligen för tillämpningar som går att använda?
- Om vi nu köper smarta kort, vilka tillämpningar kan använda dem?
- Vilka myndigheter är det som tänker använda tillämpningarna?
- Finns en tillräckligt stor marknad?

Mycket är alltså oklart och ofärdigt.

Det är t ex inte alldeles säkert att det går att ta SEIS-specifikationen som den är. Certifikaten behöver förmodligen vara olika för olika tillämpningar.

Det är viktigt att anpassa sig till vad som händer med de stora drakarna på programvarumarknaden. Det är ingen större mening att vi i Sverige sätter i gång och använder tillämpningar, om det finns risk för att marknaden efter något halvår köra över vår definition med dunder och brak. Det gäller att anpassa specifikationerna till sådant som vi tror kommer.

Alltså, det är en balansgång när det är dags att göra upphandling.

Konsekvenser för verksamhet

Om vi skapar möjligheter för signerade dokument eller signerad e-post – vad betyder det i myndighetens verksamhet? I vilka fall är det kanske något som kan ersätta en annan metod? Det behöver utredas.

I vissa fall kanske det krävs lagändringar. I andra fall kan det räcka att myndigheten ändrar sin rutin. Det kan behövas en förordning. Regelverk finns på många nivåer.

Den diskussionen behöver gå hand i hand med förberedelser för upphandlingen.

Internet-utredningen

Internet-utredningen, som lämnades av Statskontoret till Kommunikationsdepartementet i oktober 1997, beskriver en säkerhetsarkitektur med funktioner på många nivåer. Utöver nivån för textskydd behövs skydd på nätnivå, t ex för adressinformation i DNS, för vägvalsinformation och annan routing-information.

Alla nät är i grunden osäkra. Användaren kan inte vänta sig att öppna allmänna nät som Internet är säkra och måste därför skydda sin information. Utredningen rekommenderar att försvarets granskning och test av kryptering även kan användas för civila ändamål. Öppna, internationellt kända algoritmer bör användas. Det bör vara enkelt att byta algoritmer.

Utredningsgruppen föreslår bl a, eftersom PGP är relativt utbrett, att möjligheter skapas för signering av PGP-nycklar. I förslaget illustreras ett exempel där Posten och Swedac är involverade. Posten har rollen som Certification Authority för Sverige för PGP-nycklar. Swedac har certifierat Posten. Utredningen föreslår även att Swedac bör få i uppdrag att utreda om det med stöd av Lagen om teknisk kontroll kan skapas en ordning där Swedac bedömer och ackrediterar provnings- och certifieringsorgan med uppgift att prova och certifierar CA. Dessutom bör CA kunna korscertifieras.

Planer för Toppledarforum

Toppledarforum arbetar vidare med

- utredning om servicekort
- försöksverksamhet med signerad elektronisk post (e-rek) och
- rådgivning om teknik lämpad för arbete med geografisk spridning, bl a distansarbete.

Utfrågning av Britta Johansson, Statskontoret

Utfrågare:

- Projektledare Hans H Lindén, Toppledarforums projekt "Aktiva kort".
- Projektledare Jerker Sjögren, Stockholms stad.

- **Internet är på väg att bli det viktiga i en elektronisk infrastruktur – men vilken tillit finns till nätet i den offentliga sektorn?**

Svårt att säga. Myndigheter använder nätet idag huvudsakligen för informationsspridning. Den information som finns på en hemsida litar väl människor på i något skede. Men om det verkligen gäller, ringer man förmodligen och frågar eller ber om att få informationen i ett brev. Ingen vågar nog skicka ett överklagande som måste vara inne ett viss datum med e-post utan att få en kvittens. Det krävs mer av nätet för att det ska fungera.

- **Internet kommer att användas för säker elektronisk post – men hur vanlig är elektronisk post på olika nivåer inom offentlig förvaltning och hur kommer utvecklingen att bli?**

Toppledarforum driver på att myndigheter ska vara mottagliga med elektronisk post, d v s de ska ha en e-postadress som dessutom gärna ska bevakas av registrator. Därutöver får gärna alla handläggare också ha e-postadresser. Någon e-postadress har cirka 75 procent av alla offentliga organisationer idag.

Men det är osäkert hur det används och i vilka volymer. Gissningsvis är det så att ju mer formellt och bundet ett ärende är, desto mer försiktig är man med att använda e-post än så länge. Men om det börjar bli en teknik som liknar vad hur man kommunicerar t ex med sin bank, då ställer man knappast större krav på kommunikation med myndigheter än vad man gör på sin kommunikation med banken. Det som krävs för säker kommunikation med banken, det sätter normerna också för resten.

- **Där är digital signatur är en viktig del?**

Ja, åtminstone identifiering. I vissa fall är det signaturer.

- **Finns det risker med en starkt ökad användning av Internet och elektronisk post på sikt?**

En risk kan vara att man drunknar i kommunikation. Den risken ser kanske politikersidan och man därför kan sätta upp en spärr. Det finns också risk för attacker när någon kan utge sig för att vara någon annan i allvarliga sammanhang. Flertalet myndighetskontakter är inget som människor har frivilligt, utan det är något som har betydelse för ens liv och ibland på ett negativt sätt. Det är klart att det finns risker.

- **Uppslutningen kring förslaget om en gemensam IT-säkerhetslösning är stor. Nu ska Statskontoret genomföra en upphandling. Många är rädda för att upphandlingen blir en utdragen process genom att Statskontoret gör det till ett alldeles för stort paket som tar tid och blir svårt att hantera. Tänker ni äta elefanten genom att dela upp den i mindre bitar? När kommer de första konkreta resultaten?**

Vi har skurit en bit av elefanten genom att begränsa oss till tjänstekorten. Arbetet börjar genom att vi fördjupar behovsanalysen genom att ställa frågorna

1. Vilka organisationer vill ha lösningen?
2. Vad ska de ha den till?
3. Hur ser deras krav ut för att få ett bra underlag för upphandling?

På så vis får vi grepp om volymen och vi får avstämt vad korten faktiskt ska innehålla. Förväntar man sig samma saker? Ska man ha samma typ av certifikat eller är det olika saker? I det arbete vi gör har det inte varit alldeles självklart vilka vi ska kontakta och vilka som vi ska tala med. Snarare har jag upplevt det motsatta att när det verkligen kommer till kritan är det tveksamt om det finns något underlag. Det är jag mer orolig för.

I nästa steg ska det fram en kravspecifikation. Där samarbetar vi gärna om det är andra som är ute i liknande ärenden. Sedan blir det upphandling och den tar ett par månader minst. Vi räknar med att vara klara under hösten 1998 om allt går som det ska och det visar sig att det finns behov o s v.

Ju fler kontakter som vi får att konkretisera, desto lättare blir arbetet. Det är alltid bra att ha med sig organisationer som faktiskt tänker använda det de köper. Det blir mycket bättre krav då. Så kom igen! Då blir det bra.

- **För att utveckla en elektronisk infrastruktur där vi drar full nytta av digitala identiteter och signaturer – vad är det mest väsentliga som fortsättningsvis måste göras för att få en så snabb utveckling som möjligt?**

Det behövs tydliga och entydiga överenskommelser för hur det ska se ut och vad man ska göra. Hur ska det fungera? Vilka läsare ska det vara? Ju mer standardprodukter som kommer, desto lättare är det. Men det behövs också allmänt spridda och lättanvända tillämpningar.

Vi går fram steg för steg. Om vi gör en upphandling kring identitetskorten så att det finns något att köpa, har vi kommit över en tröskel. Men samtidigt, för att det ska användas, krävs det något definierat om hur vi ska använda det. Man måste bestämma sig för hur man ska gå tillväga med e-post där man har en säker identifiering. Webb-läsare – hur går de att kombinera med korten? Frågetecken finns också kring vilka certifikat man ska ha och hur de fungerar. Där finns det problem och hinder. Det är nödvändigt att arbeta på flera fronter samtidigt. Regelverk och lagstiftning är också stora frågor.

- **Du redovisar en väldig försiktighet hos offentliga myndigheter i användningen av elektronisk kommunikation, eftersom man inte gärna vill bryta mot existerande regelverk. När det gäller Lexit och Post Lexit har det hänt väldigt lite. För två år sedan kom utredningen om digital signatur. Sedan har ingenting hänt. Idag tillkännager Kommunikationsdepartementet att arbetet börjar med den frågan. Under tiden har regeringen kritiserats för en obegriplig och oförsvarlig passivitet, speciellt om man jämför med vad som sker i andra länder. Har regeringen varit för passiv?**

Säkert hade det gått att vara snabbare i vissa frågor. I andra frågor kan det fortfarande finnas stora osäkerheter. Ska man t ex lagstifta om att digitala signaturer ska gälla över hela linjen, måste man vara väldigt säker på 1) vad en digital signatur är och 2) vad den står för.

Men det vore mycket bra att få en samlad drivkraft som bygger på att alla har glädje av att rationalisera med elektroniska medel. Det behövs ett helhetsperspektiv, så att vi snabbt får en lösning.

Individens behov

Louise Yngström, Stockholms universitet:
Louise Yngström är universitetslektor vid institutionen för data- och systemvetenskap vid Stockholms universitet/KTH.

"Frågan är komplex och därför behövs ordentlig debatt och samverkan"

Inledning

Detta avsnitt belyser tillämpningar och digital identifiering för människan i privatrollen.

Budskapet

En kritisk fråga är att avgöra var balanspunkten ska sättas mellan

- **privatpersoners behov att bli unikt och säkert identifierade över flera system**

och

- **systembyggares förmåga att tillhandahålla rationella, effektiva och ekonomiskt försvarbara tjänster.**

Det finns många skäl att anta att sådana tjänster som vi normalt uppfattar som självklara, inte går att realisera med IT-stöd om inte individens identitet unikt och säkert kan klarläggas.

Den personliga integriteten

Personlig integritet är ett begrepp som de flesta människor har en uppfattning om – men som svårligen låter sig definieras. Alla kulturer tycks omfatta begreppet i någon mening, men uppfattningarna om vad som ska ingå skiftar.

Det räcker att försöka jämföra europeiska uppfattningar för att man ska se olikheterna – i Sverige har körkorten bild och namnteckning, medan i Storbritannien har de inte ens en bild av innehavaren eftersom det anses integritetskränkande. I Sverige anses uppgiften om en kvinnas ålder inte speciellt integritetskänslig, medan det i Frankrike är en mycket privat uppgift.

Många anser att personlig integritet – och annan form av integritet som t ex familjens eller gruppens integritet – är en kulturell konstruktion, som har sitt ursprung och rationalitet i ett viktigt fysiologiskt behov [t ex Lunheim & Sindre, 1994].

Svensk integritetsdebatt har ofta knutits till våra personnummer och till identifiering av oss som privatpersoner. Personnumret är unikt för varje svensk – och alla som officiellt uppehåller sig här – och utan det kan man knappast klara sig i dagens samhälle. Det används i tid och otid och svaret man får när man frågar varför man ska lämna sitt nummer är att "systemet är upplagt så!". Man menar då datasystemet.

Men i debatten blandas päron och äpplen. Frågan om *behovet* av att bli identifierad ska inte blandas ihop med frågan om det *rationella* i allmän användning av personnummer som identifiering i datasystemen.

Behovet upplevs inte nödvändigtvis lika ur olika parters synvinkel, liksom uppfattningen om vad som är rationellt kanske inte delas av alla.

Unik och säker identifiering

Givet att vi har en genomförbar unik identifieringsmöjlighet av varje individ – i vilka situationer kan det finnas ett gemensamt behov hos både privatpersoner och "systembyggare" att använda den?

I själva verket har vi som privatpersoner många exempel på när vi vill bli unikt och säkert identifierade.

Unik innebär att inte bli sammanblandad med andra personer.

Säker innebär att våra uppgifter gottskrives oss och ingen annan.

Hit hör uppgifter som berör vårt fysiska välbefinnande (vi vill självklart inte bli sammanblandade med andra patienter och kanske få fel behandling på sjukhuset) och uppgifter som berör tjänster eller service som vi efterfrågar (vi vill inte ha våra räkningar sammanblandade med andra kunders eller våra beställda tjänster levererade till andra personer).

Däremot är det inte självklart att privatpersoner upplever behovet av unik och säker identifiering när *syftet* med identifieringen primärt är någon form av extern kontroll av individen.

I sådana fall blir privatpersonens uppfattning om hur hon kan bli påverkad av utförd kontroll avgörande för behovsupplevelsen. Effekterna av t ex en identifiering i samband med en körkortskontroll kan säkerligen uppfattas helt olika i olika situationer.

Finns ingen "rikslikare"

Det finns ingen "rikslikare" för hur privatpersoner uppfattar behovet av unik och säker identifiering, lika lite som det finns en gemensam definition av integritetsbegreppet.

Däremot kan det utvecklas gemensamma uppfattningar om vad som är ett rationellt beteende, givet antaganden och förväntningar om samt förtroende för omgivningens reaktioner i allmänhet.

T ex vill många personer på Balkan idag inte ha en unik och säker identitet – historien har lett dem till att genomgående misstro varje form av överhöghet. Det finns t o m ett speciellt kommunikationsprotokoll, det ottomanska, som är konstruerat för kommunicerande parter där alla misstror alla!

I Norden och i Sverige har vi idag inte riktigt sådana historiska erfarenheter, om vi inte refererar till Gustav Vasas 1500-tal, då fogdarnas räder i landet gjorde att människor inte ville vara unikt och säkert identifierade. Det fanns också en period under 1600- och 1700-talen då stora utskrivningar av soldater till krigen, baserade på kyrkans folkbokföring, gjorde att några barn i starkt utsatta socknar inte registrerades i kyrkoböckerna.

Underskatta inte rädslans makt

Det står rätt klart att vår benägenhet att bli unikt och säkert identifierade är kopplat till vår uppfattning om vilka följderna kan bli för oss som personer – blir de positiva eller negativa och vilken del överväger?

I Danmark har man försökt introducera smarta kort med funktioner för att unikt och säkert identifiera alla danskar elektroniskt. Konceptet är i princip detsamma som det svenska SEIS, men introducerades som ett medborgarkort – inte ett identitetskort.

Precis som i Sverige idag, hade danskarna insett de potentiella fördelarna i att unikt och säkert kunna identifiera danska medborgare och vilka rationaliseringsvinster inom databehandlingen och i kommunikationen mellan människor och organisationer man skulle kunna göra.

Den danska rapporten om informationssamhället år 2000 gjorde liksom ett flertal liknande svenska rapporter klart, att en unik och säker elektronisk identitet utgör en av grundvalarna för ett säkert IT-samhälle. Människor behöver veta säkert med vem de handlar, av vem de beställer varor, etc. Danmark är relativt likt Sverige och det finns all anledning att studera varför projektet "Medborgarkortet" åtminstone just nu är lagt på hyllan.

En slutsats som dragits av många [t ex Andersen, 1997] är att informationen och den därefter följande debatten blev alltför komplex – och alltför blandad med den allmänna internationella debatten om kryptering.

Professor Mads Bryde Andersens råd vid en stor säkerhetskonferens våren 1997 i Köpenhamn löd:

"Underskatta aldrig rädslans makt, be inte politiker hantera alltför många komplicerade frågor samtidigt och lämna aldrig säkerhetsfrågorna enbart till säkerhetsspecialisterna!"

Olika bruk av kryptering

Om vi skulle ta Mads Bryde Andersen på orden, så skulle vi tvingas stanna här, eftersom unik och säker identifiering idag realiseras med kryptering. Vi kommer inte undan detta faktum.

Många känner olust inför det okända. De har kanske också tagit del av den internationella krypteringsdebatten, där det framgår att krypteringsnycklar på ett eller annat sätt kanske kommer att kontrolleras eller innehas av andra länder. Men detta gäller krypteringsnycklar för att sända förvrängda textmeddelanden – inte nycklar som behövs för att unikt och säkert signera ett meddelande.

Människan gör i alla livslägen olika riskbedömningar. Det visar sig att ju mindre känd en metod eller teknik är, desto högre relativ risk uppfattas den innebära. Hamilton [Hamilton, 1996] påpekar till exempel att vi kan acceptera risken av en bilolycka, men knappast ett haveri i ett kärnkraftverk, trots att alla siffror visar att många fler människor dör i trafiken än i samband med kärnkraftshaverier.

Behovet att vara anonym

Ibland har vi behov av att vara oidentifierade, d v s anonyma, utan namn. Som svenska medborgare har vi både rätt och önskan att vara anonyma i många fall. Vi kan också använda ett andra namn, ett alias eller en pseudonym, utifall någon annan person skulle vilja referera till oss, eller om vi själva i något fall skulle vilja referera till tidigare utsagor eller händelser.

Författare har i alla tider använt sig av pseudonymer – vissa har blivit kända i efterhand, andra inte. Ibland upplevs pseudonymerna som verkliga namn och människor ägnar sig åt att försöka gissa vem som döljer sig bakom en viss pseudonym, som t ex Jan-Jöran Stenhagen eller Bo Balderson.

I Internets chat-grupper kan man välja sig ett nytt namn och bygga upp en helt ny identitet om man vill – ingen kan kontrollera det i alla fall. Och jag kan skriva brev eller tala i telefon i annat namn eller utan att uppge namn alls. I de flesta av dessa fall finns inget behov av att bli identifierad unikt och säkert – och då finns det inte heller något behov av en unik och säker elektronisk identifiering.

I en bok av Rosanne Stone [Stone, 1996] berättas hur en manlig New York-psykiater hade problem att förstå sina kvinnliga patienter. Därför antog han ett kvinnligt alias och gick med i diskussionsgrupper på Internet. Han byggde upp en helt ny identitet, berättade om sitt påhittade liv och gav råd till andra kvinnor. Han blev mycket populär bland sina Internet-väninnor och tyckte själv att han blev en mycket bättre yrkesman genom dessa erfarenheter.

Problemen började när psykiatern ville hoppa av diskussionerna. Han ville inte röja sin rätta identitet och sina ursprungliga syften, utan försökte "dö". Slutet på historien blev att han inte kunde genomföra sin elektroniska död på ett trovärdigt sätt. Hans Internet-väninnor fick reda på hans riktiga identitet. De kände sig lurade och blev mycket arga – även fysiskt.

Koppling mellan virtuell och fysisk verklighet svår att förstå

Historien lär oss bl a att det inte är så lätt att uppträda som ett helgjutet elektroniskt alias, och att trovärdigheten i kopplingen mellan den virtuella och fysiska verkligheten blir avgörande för hur en identitet uppfattas. Det var också huvudbudskapet i boken Samkörarna [Stenhagen, 1983]. När bovarna slutligen skulle transportera de fysiska pengar de tillskansat sig genom ett databrott var detta inte praktiskt möjligt – de hade inte kunnat föreställa sig hur mycket fysisk plats 975 miljoner kronor i sedlar skulle ta.

Ett annat exempel från Stones bok är ännu mer tankeväckande vad avser hur vi uppfattar att en person är en person. Forskargruppen vid Atari som låg bakom de första dataspelen Pac-Man, visade sig vara en ur traditionell managementsynpunkt fullständigt ostyrbar grupp. De gjorde som de själva ville, och visserligen tjänade Atari extremt bra på spelen, men man ville av princip inte ha en självstyrande produktionsgrupp. Företaget konsulterade ett flertal välrenommerade internationella managementfirmor, utan resultat.

Gruppen själv fann dock på råd – de utsåg en talesman, Arthur Fishell, som visade sig både kommunikativ, trevlig och påverkningsbar. Han var dock mycket upptagen och fanns bara tillgänglig via elektronisk kommunikation. I själva verket var han konstruerad av gruppen, och bubblan sprack – men bara nästan, när ledningen för Atari efter enträgen begäran tilltvingade sig ett fysiskt möte där Arthur Fishell spelades av en av gruppens kvinnliga medlemmar. En av Ataris direktörer kände igen medarbetaren Laurel i Arthur Fishell, men höll, enligt uppgift, tyst om sin upptäckt.

Sensmoralen av Stones historier kanske är att vår mänskliga intuition att kunna identifiera en person inte är lika pålitlig för virtuella som för fysiska personer, men också att styrkan i reaktionen till att ha blivit lurad beror på hur vi uppfattar anledningen till bedrägeriet.

Identifiering är grundläggande

Det finns förmodligen fler tillfällen i vår vardag när vi vill bli sedda och korrekt identifierade än när vi vill vara anonyma. Hela den västerländska kulturen bygger på att individer säkert, både i nutid och i efterhand, kan tillgodoskriva sig aktiviteter och materiella och immateriella tillgångar. Hur många gånger per vecka använder du ditt vanliga identitetskort till exempel i samband med inköp?

Att bli identifierad jämförs med att bli igenkänd:

- I vardagen *utan* IT görs det av människor, ofta med stöd av identitetskort.
- I vardagen *med* IT måste det göras på annat sätt, t ex med ett elektroniskt identitetskort.

Scenarier visar möjligheterna

SEIS har tagit fram en bildsvit ("models") som visar hur familjen Andersson i en tänkt framtid skulle kunna dra nytta av sina elektroniska identitetskort inom ramen för de strukturer som redan finns uppbyggda [Bjärbo et al, 1996]. Bildsviten är inte tänkt som en absolut beskrivning av framtiden, utan som förslag till hur vi i vår vardag skulle kunna använda digitala identitetskort som ett rationellt hjälpmedel. Den visar hur digitala identitetskort kan användas som nyckel till bilen, som underlag för meddelande om vem och hur dags barnet blir hämtat på dagis, som passer- och tjänstekort på arbetet eller i samband med distansarbete, som patientkort på sjukhuset, som elev- och lärarkort i skolan och på biblioteket, och som identitetshandling i samband med inköp där elektronisk betalning tillämpas. De flesta av de i SEIS bildsvit framställda händelserna existerar redan, en del utan IT-stöd, andra med IT-stöd.

Många personer, som i det danska exemplet, vänder sig mot denna utveckling, och undrar om kraven på att bli unikt och säkert identifierad måste realiseras på detta sätt. Går det inte att göra på något annat sätt? Jovisst går det att vara "halvidentifierad". Det kan bli säkert relativt ett lokalt system, till exempel i skolan, men det blir inte unikt och säkert i något annat system, till exempel i en annan skola.

I de fallen vi av någon anledning vill avstå från att vara unikt och säkert identifierade som privatpersoner får vi ta på oss att bevisa på annat sätt vilka vi är, vilka tillgångar vi har, och vilka aktiviteter vi utfört. Vi får själva handha och administrera vår identifiering och dess bevisföring.

Någonstans mellan att överlåta all aktivitet för säker och unik identifiering till andra och att själva hantera och administrera detta förfarande ligger en *balanspunkt*. Den bör givetvis beaktas innan man bestämmer sig för ett unikt och säkert sätt att identifiera privatpersoner. Men, vad vi sällan tänker på, är att vi i de flesta (nordiska) sammanhang förutsätter att systemen – både de IT-stödda och de inte IT-stödda, fungerar baserade på unik och säker identifiering av privatpersoner.

Ett exempel från ett annat EU-land kan påminna oss om våra outtalade förutsättningar: en engelsk medborgare i en gammal bil blev stoppad av polisen. Hon uppmanades att visa papper på vem hon var och om hon innehade körkort, vem som var ägare till bilen, om bilen var försäkrad och skattad, och om den genomgått besiktning.

Redan idag klarar vi sådana frågor inom fem minuter i Sverige – i Storbritannien kan det ta en hel dag om man inte själv förberett och administrerat sådana frågor på förhand.

Den kritiska balanspunkten

Balanspunkten måste således beakta vad som ska anses vara rationellt och praktiskt, både ur systembyggares och privatpersoners synvinkel. Det finns många skäl att anta att sådana tjänster som vi normalt uppfattar som självklara, inte går att realisera med IT-stöd om inte vår identitet unikt och säkert kan klarläggas.

SEIS-konceptet till ett elektroniskt identitetskort, digitala identitetskort, är ett förslag till en standard som skulle kunna användas över stora delar av det privata och offentliga samhället. Det finns också andra förslag till standarder, till exempel Visa och Mastercards SET-standard. SET förutsätter att det finns ett konto med ekonomiska tillgångar eller krediter som anledning och garant för kommunikationen; det finns många kommunikationsbehov i IT-stödda sammanhang som inte har en sådan förutsättning, och där andra lösningar måste sökas – om man vill utnyttja IT rationellt, effektivt och ekonomiskt.

En kritisk fråga blir att avgöra var balanspunkten mellan privatpersoners behov att bli unikt och säkert identifierade över flera/många system och systembyggarnas förmåga att tillhandahålla rationella, effektiva och ekonomiskt försvarbara tjänster ska sättas.

Litteraturlista

Mads Bryde Andersen: The role of government in creating the IT security infrastructure. Builder or bystander? i Yngström, L och Carlsen, J (eds) Information Security in Research and Business, Chapman & Hall, 1997 sid 71–77.

Gabriella Bjärbo, Anna Boström och Camilla Åhnberg: Användning av elektroniska identitetskort, magisteruppsats, DSV, SU/KTH 1996, rapport 96–19–DSV-SU.

Gustaf Hamilton: Risk Management 2000, Studentlitteratur 1996.

IT-kommissionen: Inför en svensk policy för säker elektronisk kommunikation. IT-kommissionens rapport 6/97.

IT-sikkerhedsrådet: Danmarks IT-sikkerhedspolitik, Danska Forskningsministeriet 1996.

Rolf Lunheim och Guttorm Sindre: Privacy and computing: a cultural perspective, i Yngström, L. Sizer, R (eds) Security and Control of Information Technology in Society, North-Holland 1994, sid 25–40.

Jan-Jöran Stenhagen: Samkörarna, Wahlström & Widstrand, 1983.

Rosanne Stone: The war of desire and technology at the close of the mechanical age, MIT Press, 1996.

Utfrågning av Louise Yngström, Stockholms universitet

Utfrågare:
- Helle Klein, journalist.
- Anders R Olsson, journalist.

- **Dessa frågor är oerhört viktiga, därför att svaren i flera avseenden bestämmer medborgarnas och demokratins villkor i framtiden. Vi hade en stor integritetsdebatt kring 1970 som resulterade i en datalag 1973. Med undantag för enstaka opinionsstormar, t ex Metropolit-affären 1986, har det sedan varit tyst.**

Då, när vi visste ytterst lite om integritetsproblemen i IT-samhället fördes en debatt. Men nu när vi ser och allvarligt hotas av sådana problem, förs ingen debatt. Detta är djupt politiska problem eftersom ett grundläggande perspektiv är att det gäller att avväga individens rätt gentemot kollektivet eller samhället och kollektivets eller samhällets rätt gentemot individen. Fråga: hur är det möjligt att få till stånd något slags framsteg? Hur ska politiskt ansvariga och tekniskt kunniga samverka för att komma vidare?

Du ger själv ingången till svaret! Det handlar om att skapa samverkan eller snarare interaktion mellan tekniker och icketekniker.

Eller annorlunda uttryckt: å ena sidan de som förstår hur utvecklingen kan klaras av både tekniskt och organisatoriskt och å andra sidan de politiskt ansvariga som behöver bilda sig en uppfattning utifrån de olika värderingsperspektiven.

Det är flera parter som aktivt borde ingå i diskussionerna – som det nu är lämnas det mesta bara över till utvecklingspersonalen. Vi vill så gärna att någonting ska ske på detta område, men det kommer inte i gång därför att diskussionsparter lyser med sin frånvaro. Frågorna är så genomgripande. Jag förstår inte varför integritetsdebatten är död. Mycket ligger i vad Mads Bryde Andersen säger att frågan är så komplex, att människor inte vågar ta itu med den. Men interaktionen är oerhört viktig mellan utvecklarna som skaffat sig erfarenheter och politiker, media, debattörer och andra typer av ledare.

- **Hela frågan förefaller vara en tillitsfråga mer än en säkerhetsfråga. Har teknikerna ansvar att skapa tillit och gör de det?**

Teknikerna har ansvar och vill ta ansvar för att skapa tillit – eller snarare skapa olika typer av strukturer eller modeller inom vilka man kan skapa tillit. I en stor del av utvecklingen inom säkerhetssidan som pågått sedan 1985, förefaller industrin tycka att de kravmodeller för tillit som kom fram på säkra system har varit hämmande för utvecklingen.

Det är inte så att det inte finns intresse, vare sig från utvecklare eller användare, för att få i gång en utveckling. Snarast är det så att teknikerna inte klarar av hela denna komplexa frågan utan hjälp av andra grupper.

- **Om 1970-talets debatt mycket handlade om en misstro mot staten, så kanske det idag när de flesta använder en PC (och märker hur allt ständigt går sönder) är en misstro mot själva tekniken?**

Nej, det har jag svårt att tänka mig. Jag tycker att den unga generationen, de som tar till sig IT, lär sig väldigt mycket den praktiska vägen. De är inte skraja. Delvis handlar det om att man inte har förstått vad det elektroniska identitetskortet ska användas till och vad det är för fördelar.

- **Ska all information ligga på det elektroniska identitetskortet? Eller är det pekare på kortet mot centrala register? Ska vi ha flera kort? Hur många kort orkar vi medborgare använda?**

Det är detta som mycket av diskussionen gäller. Ska allt ligga på kortet? Ska man ha ett kort? Ska man ha flera kort? Min uppfattning är att detta är ett identitetskort och ska användas som ett elektronisk identitetskort. Vi kommer förmodligen att kunna ha andra kort också, men jag vill ha identifieringsfunktionen i detta kortet. Alla har inte samma uppfattning om det.

- **En klassisk fråga är huruvida man ska ha en identitet. I Sverige har vi personnummer. De flesta andra länder har flera identiteter – t ex har man en identitet hos banken, en hos försäkringskassan, en hos skattemyndigheten o s v. Men utvecklingen på senare tid går i nästan alla länder i riktningen mot att man skaffar sig ett nummer eller en identitet som används i alltfler sammanhang. Flera identiteter gör all administration mycket krångligare. Hur förändras förutsättningarna för problemet en eller flera identiteter med moderna krypteringstekniker?**

Krypteringstekniken i sig innebär ingen skillnad alls. Man kan ha olika identitet i olika system. Men jag är då inte unikt och säkert identifierad i alla system, utan bara i de system som accepterar min identitet. Som följd av detta får man själv administrera sina olika identiteter genom kort eller annat förfarande gentemot de olika systemen. Krypteringstekniken gör ingen skillnad här. Men balanspunkten – som jag understryker måste beaktas – gäller individers krav på att få ha olika identiteter i olika system (med egna administrativa arbetsuppgifter som följd) versus systembyggares krav på rationella och kompatibla IT-system.

Vem bestämde en gång i tiden om det vanliga identitetskortet? Det är ingen av oss som tycker att det är något märkvärdigt när vi ständigt använder det kortet. Jag tror att det då var någon form av consensus om att ett identitetskort var något som vi behövde. Delvis är det den modellen som SEIS söker sig fram emot. Medlemmarna i SEIS är många och de har ett gemensamt behov av elektronisk identifiering. Behovet av en gemensam standard för elektronisk identitet kommer alltså inte som ett påbud uppifrån.

Näringslivets behov

Rabbe Wrede, Telefonaktiebolaget LM Ericsson:
Rabbe Wrede arbetar med koncern-IT-infrastrukturen i Telefonaktiebolaget LM Ericsson, Stockholm.

"Det är angeläget att vi snarast kan börja använda digitala signaturer"

Inledning

Detta avsnitt belyser behoven av digitala signaturer i näringslivet.

Budskapet

Regeringen bör snarast legalisera digitala signaturer och ta kraftfulla initiativ för att uppnå ett harmoniserat globalt ramverk för digitala signaturer baserat på affärsbehoven för elektronisk handel över gränserna. Vinsterna för näringslivet blir enorma.

Behovet

En allt större del av meddelandena mellan och inom olika organisationer sker idag med hjälp av IT. Fördelarna med detta är uppenbara, det går fort och är i stort sett oberoende av tid och rum. Jag kan t ex meddela mig med en annan person utan att behöva veta var han befinner sig genom att skicka ett e-post-meddelande. Han kan svara direkt och jag kan ta fram detta meddelande oavsett om jag är på kontoret i Stockholm eller Beijing.

Konsekvenserna blir att den affär vi ska göra inte hindras av att jag är på resa i två veckor. Vi kan trots de förändrade geografiska förhållandena kontinuerligt förhandla om affärsvillkoren. Det innebär att ju bättre tekniska möjligheter jag har att göra detta, desto mer fördelar har jag gentemot min konkurrent, som kanske också förhandlar om samma affär.

Men när vi väl är överens om affären och dess villkor vad gör vi då? Jag måste ju vara säker på att det är rätt person jag förhandlat med. I efterhand ska vi kunna bevisa att vi kommit överens om vissa villkor för affären. Idag måste vi kanske träffas för att skriva på avtalet och signera varje sida. Är det en för mig känd person räcker det kanske med att vi utväxlar de signerade avtalen via någon budfirma. I vilket fall som helst blir vi plötsligt beroende av tid och rum på ett annat sätt än under själva förhandlingarna. Jag ska t ex befinna mig på samma plats som det utskrivna avtalet när jag signerar det.

Detta enkla exempel visar dagens begränsningar i utnyttjandet av IT i affärssammanhang.

"Handslaget"

I ett historiskt perspektiv har nog samma begränsningar funnits tidigare när viktiga meddelanden måst utväxlas mellan parter som befunnit sig på olika orter. I den egna stammen eller byn räckte det med ett handslag eller liknade. När förbättrade kommunikationer möjliggjorde meddelandeförmedling på avstånd uppkom behov av ett formaliserat och materialiserat handslag i form av bomärken eller sigill och senare namnteckning. Problemet är alltså inte nytt, vi måste bara enas om ett nytt sätt att formalisera och materialisera handslaget. Det vi generellt vill uppnå med "handslaget" är

- tillit (trust) till att det är rätt person som gett oss meddelandet
- att vi vid ett senare tillfälle kan bevisa att personen skrivit meddelandet
- att ett viktigt meddelande inte är förvanskat före eller efter vi fått det.

I IT sammanhang kan vi materialisera "handslaget" med hjälp av digitala signaturer. Dessa kan uppfylla alla de ovanstående kriterierna om vi bara enas om det. Vi behöver bara enas om att en digital signatur är precis lika bra och lika trovärdig som en namnteckning. Enas om att en namnteckning är bindande har människan gjort genom sedvänja. Det tar minst 30 år för en sedvänja att bli juridiskt giltig. Den tiden har vi inte. Vi behöver därför lagstiftning som baserar sig på internationella överenskommelser.

Användningen i näringslivet

Behov av system för digitala signaturer i näringslivet finns inom flera områden.

Externa avtal
Det mest uppenbara användningsområdet är i avtal mellan företag. Idag finns EDI som möjliggjort ett helt annat beteende mönster i affärsvärden. EDI har dock sina begränsningar. EDI baserar sig alltid på att två eller flera företag skriver någon form av ramavtal där man godkänner alla köp inom vissa specificerade ramar.

EDI är alltså ingen lösning för avtal mellan tidigare för varandra okända parter. Det går t ex inte att handla på spotmarknader med samma säkerhet. Oformaliserade avtal baserar sig alltid på att man känner eller känner till motparten och att man är beredd att ta en viss risk med att inte formalisera avtalet.

Med digitala signaturer skulle dessa nackdelar försvinna. Det går alltid att göra affärer med säkerhet, men också snabbare. Snabbheten är det som ger konkurrensfördelar.

Interna avtal
Ett annat område som inte är lika uppenbart är de interna avtalen inom en organisation. Många affärer görs mellan olika legala enheter inom en koncern. Inom ett bolag behöver man också attestera många handlingar för att revisorerna ska ha möjlighet att göra sitt arbete. Idag måste vi ta ut ett digitalt meddelande på papper, signera det och arkivera det i pappersform. Dessutom måste vi i många fall registrera i det digitala mediet att underskriften skett.

Detta är ett mycket omständligt och orationellt tillvägagångssätt. Vi arbetar i många fall enbart med ett digitala dokumentet och vid eventuella förändringar i detta måste hela den manuella proceduren göras om. Med detta följer också att det är mycket lätt att det uppstår olika versioner av samma dokument i de olika media.

Införandet av legalt accepterade digitala signaturer skulle i detta sammanhang kunna medföra enorma rationaliseringar inom näringslivet. Detsamma gäller för övrigt inom alla samhällssektorer.

Identifiering
Om vi hade digitala signaturer skulle vi också kunna utnyttja dessa för en säker identifiering av personer vid åtkomstkontroller till system och databaser.

Vi skulle kunna använda samma system i alla olika sammanhang. Idag behöver användare kunna många lösenord och ibland även använda kort eller lösenordsgeneratorer. Detta medför att säkerhetslösningar upplevs som krångliga och hindrande av användarna. Detta i sin tur medför att man försöker gå runt dem med resultat att säkerheten sänks till en alldeles för låg nivå.

Detta är ett välkänt problem som alla inom säkerhetsbranschen brottas med. Men någon bra lösning finns inte idag.

Digitala signaturer skulle alltså även i detta sammanhang medföra stora förbättringar.

Hur får vi digitala signaturer?

Det har inom olika organisationer över hela världen tagits fram förslag och propåer om internationellt harmoniserad lagstiftning kring digitala signaturer. Från näringslivssynpunkt är mycket angeläget att detta sker – nu!

Det finns bara ett sätt för oss i Sverige att få digitala signaturer och det är att den svenska regeringen bör snarast

- ta officiell ställning till att digitala signaturer ska jämställas med andra typer av signaturer
- snabbehandla de underlag till lagstiftning som finns
- ta kraftfulla initiativ till internationella överenskommelser i t ex FN, OECD, EU för att uppnå ett globalt harmoniserat legalt ramverk för digitala signaturer baserat på affärsbehoven för elektronisk handel över nationsgränserna.

Dessa initiativ kan basera sig på de förslag som SEIS tagit fram. Inom SEIS har genom ett bra samarbete mellan offentlig förvaltning, bankerna och övrigt näringsliv tagits fram förslag inom detta område. Vi inom Ericsson har från början tagit aktiv del i detta arbete eftersom vi ser alla de fördelar som beskrivits ovan och de konkurrensfördelar detta kan ge oss.

Utfrågning av Rabbe Wrede, Telefonaktiebolaget LM Ericsson

Utfrågare:
- Säkerhetschef Ronald Skoog, Scania AB.
- Marknadschef Eva Cederbalk, S-E-Banken.

- **Integritet är den springande punkten i debatten som gäller privatpersoner ("rädsla för att storebror ser dig"), men vad finns det för fokus på diskussionen på företagssidan – är det sekretessen kring företaget och dess affärer o s v?**

Eftersom ett företag omsätter så mycket information så snabbt, är det frågan om hur mycket intern sekretess som vi egentligen behöver. Informationen blir snabbt gammal. Men det är egentligen en helt annan debatt.

När det gäller integritet går det att vända på perspektivet. Sett det från individens synpunkt – vilka förbättringar medför det? Det måste ju ligga ett värde i att jag som individ kan vara säker på att någonting som tillskrivs mig (t ex ett uttalande som jag har skickat på något sätt eller skrivit på papper) kan jag faktiskt säkra genom en digital signatur. Det ger ett plus för mig som individ att jag är säker på att den som läser dokumentet, kan se att det är jag och att innehållet inte är förvanskat. Den aspekten är viktig.

- **Var står Ericsson konkret när det gäller denna nya teknik och tänkandet kring den? Var står övriga näringslivet? Finns tillämpningar eller ligger det mesta fortfarande framåt i tiden?**

Det finns tillämpningar. De tekniska möjligheterna finns. Det som kan ta lite tid är att få igång administrationen (CA, Certification Authority) inom ett företag.

Vi har kommit ganska långt inom Ericsson, men det är ett uppbyggnadsskede och vi har ett intimt samarbete med flera andra företag. Det är inga problem för att lösa detta, men vi har respekt för att den administrativa delen är lite trögare.

- **Är det någon skillnad mellan stora och små organisationer?**

Sättet att göra det är detsamma. Men det är rimligtvis enklare att införa detta i en organisation på 25 personer än i en på 100 000.

- **Du säger att vi måste se till att SEIS-standarden som vi har utarbetat i Sverige blir internationell. Det föresvävar mig att det finns liknande lösningar utarbetade på andra marknader. Vad är det som gör att Ericsson – som ju är ett extremt internationellt företag som möter lösningar och leverantörer i andra världsdelar – mest intresserar sig för en svensk lösning?**

Därför att jag tror att vi har kommit längre än utlandet. Vi har en stor fördel i Sverige på detta område och det är att vi har lätt att samarbeta mellan näringsliv och offentlig förvaltning. Det är tradition. Den ska vi utnyttja. I början på 1995, när SEIS var nytt, var jag över och talade med en del stora amerikanska företag om detta. De var fullt medvetna om våra unika förutsättningar. De sa ungefär att: "Ni har en jättefördel i Sverige och jag kan inte se hur det denna utveckling kan drivas på detta sätt i något annat land."

Därför är det intressant med en svensk lösning. Det är nämligen en helhet som måste göras. Det är inte bara tekniken som ska utformas. Det är också hur kortet ska se ut och hur lagstiftningen ska se ut. Det måste bildas ett ramverk så att det passas in i samhället.

Vi har gedigen erfarenhet av identitetskort för fysisk identifiering. Vi har erfarenhet av hur vi ska få in alla synpunkter och snabbt kunna få fram lagförslag. Vi har också gjort ett gediget arbete på tekniksidan i Sverige. Flera svenska företag med utländska kopplingar har plockat åt sig. Därför är det intressant hur Ericsson tar det som ligger närmast. Hade samma arbete gjorts i USA eller på Nya Zeeland hade vi varit intresserade av det. Vi är intresserade av en snabb lösning.

- **Ligger denna utveckling på företagsledningsnivån eller är det på lägre nivåer?**

Det är relativt bra etablerat på ledningsnivån inom Ericsson. Vi har en plan för vår IT-utveckling som antogs av den verkställande ledningen den 18 april 1996. Där står det klart uttalat att vi ska arbeta för att införa digitala signaturer inom Ericsson innan 1998 års utgång. Huruvida vi kommer att hålla sista kvartalet 1998 eller inte, kan vi sätta ett litet frågetecken kring. Men det är en klart uttalad ambition att vi ska genomföra detta inom Ericsson.

C. Vad krävs för ett införande? Vad kan införas?

Översikt

Följande belyser vad som krävs för införande av system för digital identifiering och signatur vad gäller

- teknik
- tjänster
- regelverk.

Teknik

Hans Tholander, Dynamic Software AB:
Hans Tholander är VD för Dynamic Software AB, Stockholm.

"Asymmetrisk kryptering skapar möjligheter för säkra tillämpningar"

Inledning

Detta avsnitt belyser den tekniska grunden för identifiering och identitet i digitala miljöer.

Budskapet

En digital signatur kan användas för att garantera dels att en informationsmängd inte har förändrats och dels vem avsändaren är. Tekniken för digital signatur kallas "public key"-teknik och bygger på användning av s k asymmetrisk kryptering.

Grundläggande teknik

Den teknik som möjliggör användning av digital signatur kallas "public key"-teknik och bygger på användning av s k asymmetrisk kryptering.

Asymmetrisk kryptering innebär att man i en avancerad matematisk beräkningsprocess skapar ett nyckelpar, d v s två nycklar som hör samman. Den ena nyckeln används för kryptering och den andra för dekryptering – eller vice versa. Den ena nyckeln hålls hemlig, d v s den är privat. Den andra nyckeln kan göras publikt tillgänglig och kallas därför för den publika nyckeln. Trots att den ena nyckeln görs allmänt tillgänglig, så går det inte att med hjälp av denna lista ut den hemliga privata nyckeln.

Med denna teknik (ofta i kombination med mer traditionell, s k symmetrisk kryptering) går det att bygga olika system för att

- skapa konfidentialitetsskydd (= krypterade informationsmängder) och
- skapa digitala signaturer.

Digital signatur

En digital signatur kan användas för att garantera dels att en informationsmängd inte har förändrats och dels vem avsändaren är. Exempel: Jag vill sända ett elektroniskt dokument till en annan person. Denne vill kunna kontrollera att dokumentet inte har förvanskats i samband med överföringen och att det verkligen är jag som har skickat brevet.

Steg	Aktivitet
1	Jag skapar ett kondensat (checksumma) av det elektroniska dokumentet (informationsmängden) som jag vill skicka.
2	Checksumman krypteras med min privata nyckel och det är blir min unika digitala signatur för detta dokument.
3	Denna digitala signatur "hängs på " det elektroniska dokumentet som krypterat eller okrypterat skickas till mottagaren
4	Mottagaren kan kontrollera dokumentet genom att med min publika nyckel (som finns i en katalog) dekryptera checksumman. Min publika nyckel är knuten till mitt namn (min identitet) i ett s k certifikat utställt av en Certification Authority eller CA som garanterar äktheten.
5	Om de båda checksummorna är lika vet mottagaren att dokumentet är oförvanskat och det var jag, Hans, som skickade dokumentet.

Digital identifiering

För att göra en säker digital identifiering används asymmetrisk krypteringsteknik med ett förfarande som kallas *challenge response.*

Exempel: Jag ska logga in på min dator med hjälp av mitt digitala identitetskort och datorn ska kontrollera att det verkligen är jag.

Steg	Aktivitet
1	Jag sätter in mitt digitala identitetskort i kortläsaren och öppnar kortet med min hemliga PIN-kod.
2	Datorn skickar ett slumptal till kortet.
3	Kortet krypterar slumptalet med min privata nyckel som finns på kortet och skickar tillbaka det till datorn.
4	Datorn verifierar det krypterade slumptalet med min publika nyckel som den har tillgång till (t ex via katalog eller på kortet.)
5	Om allt stämmer blir jag inloggad på datorn.

Mycket svårt att göra intrång

En säker elektronisk identifiering har genomförts. Med en sådan förstärkt identifieringsprocess försvåras avsevärt för oönskade användare att göra intrång. Det skapar möjligheter för säkrare tillämpningar och ger kontrollerad tillgång till datorsystemen för behöriga användare.

För att digital identifiering och digitala signaturer ska fungera är det viktigt att

- lagra den privata hemliga nyckeln på ett säkert sätt
- komma åt och lita på den publika nyckeln och dess certifikat som talar om vem innehavaren av den publika nyckeln är, d v s säkerställa identiteten.

Smarta kort (aktiva kort)

De grundläggande kraven på ett smartkort är att

- beräkningskapaciteten är tillräcklig för att göra en krypteringsberäkning på kortet
- minneskapacitet tillräcklig för att lagra certifikatinformation, nycklar och identitet
- innehåll och format är standardiserat
- informationen går att lagra på kortet på ett säkert sätt.

Det finns kort som uppfyller samtliga krav och utvecklingen av mer kraftfulla kretsar för smarta kort fortsätter. Priset för ett kort inklusive både visuell och elektronisk personalisering är 250–350 kronor per kort i volymer på ett par tusen kort per sats. Det finns standarder för kortens innehåll, format och utseende. I Sverige har SEIS utarbetat standardförslag när sådana har saknats och verkar nu för att få dessa förslag internationellt accepterade. För innehållet i ett certifikat dominerar X.509-standarden. SEIS-förslaget till standard omfattar främst normer för hur informationen (certifikatet och nycklar) ska lagras på kortet. Information finns på *www.seis.se.*

Det har hittills ansetts vara omöjligt att obehörigt komma åt informationen som finns lagrad i smartkortet utan att förstöra det. Men på senare tid har det dock hävdats att det ska vara möjligt och studier av kortens säkerhet pågår. Oavsett detta är ett smartkort det bästa praktiska sättet att mycket säkert lagra nycklar och certifikat.

Är smarta kort nödvändiga?

Det är inte nödvändigt att använda smarta kort för att få en säker identifiering och digitala signaturer. Det går även att använda s k mjuka kort eller disketter. Då läggs motsvarande information (som annars lagras på det smarta kortet) antingen i en krypterad fil på datorn eller på en diskett.

Detta ger inte samma höga säkerhet för den lagrade informationen som man får med ett smart kort. Kortet fungerar ju dessutom som ett visuellt identitetskort. Det smarta kortet bär man också med sig och det kan låsas vid missbruk.

Å andra sidan behövs med mjuka kort inga kortläsare eller rutiner för kortframställning och distribution. Följaktligen är en lösning med mjuka kort billigare.

Kortläsare

Det finns tre typer av läsare för smarta kort:

- fristående från datorn med eller utan s k pin pad (nummertangenter)
- PCMCIA läsare som sätts in i t ex den bärbara datorn
- inbyggda läsare, antingen i tangentbordet eller i datorn.

Priserna varierar beroende på prestanda och typ men ligger i intervallet 500–1 500 kronor vid måttliga volymer (500–2 000 läsare). Standarder för läsare håller på att etableras.

CA och kortutgivning

Utfärdande av certifikat samt personalisering och utgivning av kort behöver inte göras samtidigt men så sker ofta i praktiken. När ett företag, t ex en bank, bygger upp sitt eget system som ska kunna göra säker digital identifiering, skapa digitala signaturer och utföra kryptering med hjälp av "public key"-tekniken, skapar man ofta sin egen CA-funktion som personaliserar korten med nödvändig digital och visuell information samt lägger in certifikaten.

Det går att vara sin egen CA, men det behöver inte vara så. Man kan istället framställa sitt kort med viss information. Sedan lämnar man in en begäran om certifiering till en CA (Certification Authority) som utfärdar certifikatet enligt en kontrollerad och säker procedur som kopplar identiteten till certifikatet.

Det är heller inget generellt krav att certifikatet ska ligga i kortet som SEIS-standarden föreskriver. Det går istället att lägga en s k pekare i kortet som hänvisar till var man kan hitta certifikatet, t ex i en viss utställares katalog. Fördelen med att ha certifikatet i kortet är i ett läge då det inte finns tillgång till en CA-katalog. Nackdelen är att det är svårare att utfärda ett nytt certifikat om det gamla blivit ogiltigt av tidsskäl. Kortet måste då uppdateras med ett nytt certifikat och det blir viss hantering kring detta.

Viktigt är också att man mot aktuella spärrlistor kontrollerar om certifikatet är återkallat eller inte. Det kallas revokering och innebär återkallning av certifikat. Revokeringslistor måste fungera och finnas lätt tillgängliga. En annan viktig aspekt är att det behöver vara policies eller villkor inskrivna i certifikatet – detta för att en användare ska kunna bedöma i vilken grad han kan lita på certifikatet. I en sådan policy anges t ex vilka procedurer som används när certifikatet ställs ut. Det går att ha olika sådana policies för olika ändamål beroende på bl a kravet på säkerhet.

SEIS har angett en CA-policy som lämpar sig för det digitala identitetskortet som har godtagits av bl a Posten, Telia och bankerna. Policyn anges också i certifikatet (enligt version 3 av X.509-standarden). Om kortutgivaren också utfärdar certifikatet måste denne kunna garantera att t ex SEIS CA-policy har följts. För att skapa trovärdighet till systemet bör det även finnas ett organ som kan verifiera (och kontrollera) att utgivaren följer angivna policies.

Praktisk tillämpning

Att skapa en digital signatur för ett dokument t ex en orderbekräftelse, faktura eller ett bokföringsallegat måste vara – och det är – mycket enkelt. I princip "klickar" användaren på en ikon med funktionen att skapa en digital signatur för dokumentet.

Användaren anger exakt vilket dokument det är och sin identitet (fås i regel automatiskt från det smarta kortet, men det kan också ske genom att åter ange t ex lösenord/PIN-kod) för att bekräfta att det är rätt person som sitter vid datorn). Systemet skapar därefter den digitala signaturen som läggs till dokumentet och bekräftar till användaren att signeringen har skett.

Utfrågning av Sten Sörenson, Dynamic Software AB

Frågorna besvaras av Sten Sörenson som är Norden-chef inom Dynamic Software AB, Stockholm.

Utfrågare:

- Produktchef Christer Öberg, Bull AB.
- IT-utredare Anne-Marie Eklund-Löwinder, Statskontoret.

- **Äktheten i ett certifikat garanteras av en CAs signatur. För att kunna verifiera en CAs signatur måste jag också ha tillgång till CAs öppna nyckel och den måste jag ha fått på ett säkert sätt. Hur får jag tillgång till aktuell CAs öppna nyckel på ett säkert sätt? Hur långa förtroendekedjor kan vi acceptera?**

  När man får sitt certifikat första gången på ett kort innehåller det också CAns certifikat. Hur långa kedjorna kan vara finns det ingen absolut gräns för. Det är mera en fråga om förtroende på förtroende på förtroende. Ett exempel är konceptet PGP, Pretty Good Privacy, som bygger på ett sådant orsakssammanhang. Om jag garanterar din identitet och du känner någon som känner någon o s v är det möjligt att skapa mycket långa förtroendekedjor.

  Det är en fråga om vem jag väljer att lita på. Vad får jag lita på? I hur många led? Industrin har ingen aspekt på detta. Jag litar inte obetingat på alla. Frågan är vilken tillit som jag har till en CA. Är det någon som regering och riksdag har utsett och som omfattas av svensk lag? Finns en tillsynsmyndighet? Möjligheten finns att korscertifiera eller certifiera i flera led. Många CA som gör anspråk på att vara den absoluta CAn för ett visst tjänsteområde.

  Teoretiskt är det möjligt att bilda hur långa kedjor som helst. Det är antagligen inte krångligare än på det sätt som vi umgås med varandra som människor. Vi introduceras till varandra, även om det sedan visar sig att det finns en och annan katt bland hermelinerna likafullt.

- **Det viktiga är egentligen inte att ha rätt certifikat, utan att kunna ta reda på om certifikatet fortfarande är giltigt och inte är återkallat. Hur vet jag, när jag har fått ett digitalt signerat brev, från vilken revokeringslista jag ska kunna kontrollera giltigheten i certifikatet?**

  Genom att titta i certifikatet. Där framgår vem som är utställare och vilken policy som gäller. Det går att gå bakåt i orsakskedjan. Det är när vi börjar bygga kedjor med flera CA som det blir komplext. Det finns alltid en länk från den CA som certifierat nästa CA i certifikatet.

- **Hur genomför jag det praktiskt? Ringer jag CAn för att kontrollera om certifikatet är revokerat?**

  Det är nästan det enda sättet att göra det på, särskilt om certifikatet redan finns på kortet. Det kan vara för gammalt.

Tjänster

Evald Persson, Posten AB:
Evald Persson arbetar med strategisk utveckling hos Posten AB, Stockholm.

"Vi är angelägna om att driva på uppbyggnaden av infrastrukturen"

Inledning

Detta avsnitt belyser införande av tjänster för identifiering och identitet i digitala miljöer.

Budskapet

Posten kommer att tillhandahålla sådana tjänster till marknaden som behövs för att ge en säker digital identitet.

Digital identitet

Vad innebär en digital identitet? Det är ett sätt att över ett datanät kunna visa vem jag är för den person eller tillämpning som finns i andra änden av nätet. På det sättet kan jag alltså åstadkomma fjärridentifiering. Nästa steg är att kunna verifiera att något kommer från en viss avsändare, d v s att ha den digitala signaturen tillgänglig. Sedan vill man ofta tillföra konfidentialitet och det innebär kryptering av informationen.

Posten kommer att tillhandahålla den sortens tjänster till marknaden som behövs för att ge en säker digital identitet. Dessa kommer att finnas dels i form av mjuka tillämpningar, alltså mjuka certifikat för programvarutillämpningar i persondatorn och dels i form av hårda certifikat, d v s elektroniska identitetskort, EID.

Certifikat

Det som är bäraren av den digitala identiteten är certifikatet. Ett certifikat innehåller de attribut som behövs för att unikt fastställa en persons identitet. Det kopplar också ett nyckelpar, en hemlig och en publik nyckel, till denna identitet. Den publika nyckeln är en delmängd av certifikatet. Ett certifikat har en begränsad giltighetstid (idag 2–5 år) på grund av att det inte går att garantera att de nyckellängder som finns idag kommer att hålla i all framtid.

Den information som finns i ett certifikat måste vara undertecknad/garanterad av någon som kan ta ansvar för informationen. Postens ambition är att ta ansvar för att utföra identifieringsprocesser som fastställer att innehavaren av certifikatet verkligen är den han ger sig ut för att vara, när han får ut certifikat med nycklar eller det elektroniska identitetskortet.

Postens roll är alltså att ge ut identitetskort och signera innehavarens (individens) identitet. Sedan kommer företag och myndigheter att vilja identifiera ansvarsförhållanden inom organisationen och på så sätt kunna förmedla att en viss individ har en viss roll eller rättighet. Den måste också kunna knytas till en digital identifiering.

Som individer kommer vi framgent att ha hundratals olika certifikat (roller) som fastställer olika saker. Den viktigaste är identiteten. Andra exempel är kundförhållande, rättigheter, patientförhållande i sjukvården, funktion i en organisation, attesträtt, tillfälliga begränsade rättigheter (biljet, tidsbegränsad nyckel), o s v.

Betrodd tredje part

För detta bygger Posten ett antal funktioner. Tekniken finns brett tillgänglig. Det Posten gör är att bygga upp de administrativa system som behövs och att ha en IT-struktur som gör att det kan fungera. För att det ska finnas nödvändiga garantier behövs en betrodd tredje part (TTP) så att man inte ständigt behöver ställa sig frågan om det går att lita på en uppgift. När man följer en verifieringskedja är det ofta för att verifiera identiteten hos ett helt okänt företag eller en person någon annanstans i världen. Om man – över nätet – ska kunna lita på att företaget eller personen är vad som uppges, gäller det att få in ett naturligt förtroende för de organisationer som tar på sig TTP-rollen. De måste vara allmänt betrodda på sin marknad.

Identifiering av användaren

TTP-organisationen måste kunna hantera användaridentifiering. Vi behöver kunna generera nycklar som har gått igenom vissa kontrollprocesser så att de är så säkra som möjligt. Vi ska också kunna hjälpa till i kedjan som behövs för att ett företag ska kunna ställa ut sina roller. Företaget ska alltså kunna agera sin egen CA, utan att för den skull dra på sig hela den infrastruktur som behövs för att bygga upp en rollhierarki inom företaget. Det gäller att kunna slå fast rollhierarkin i ett certifikat och på så sätt förmedla information om sådana roller.

Viktigt är också att vid misstanke om någon typ av kompromettering kunna spärra och revokera certifikatet. Det innebär att Posten sätter upp en katalogfunktion med verifierbara och säkra driftrutiner. Information finns i certifikatet om var det är möjligt att kontrollera certifikatet.

Utgivningsprocessen

Processen för att ställa ut ett digitalt identitetskort börjar med att individen fyller i en beställningsblankett. Sedan går denne till en postkassa för att lämna in blanketten. Det kan också vara en bank, eller annan organisation som vi generellt litar på i samhället. Där sker en handskakningsprocedur genom att man kontrollerar med andra legitimationer för att säkerställa att den som vill ha det digitala identitetskortet också är den som ansöker om det.

Därefter gör Posten en rad kontroller i bakgrunden mot folkbokföringsregistret SPAR och andra register. Vi tar hänsyn till om personen i kassan känner personen, för att också få in detta i utvärderingsprocessen. När anmälan är mottagen, sätter Postens produktionsapparat i gång med att producera det fysiska kortet med visuella utsidor, att ställa ut certifikatet som innehåller den digitala informationen, placera certifikatet på kortet där också nyckelparet som är knutet till certifikatet finns placerat. Sedan publiceras detta i katalogen för att revokeringsprocessen ska fungera.

Utlämning av kortet till mottagaren sker genom att en transport-PIN-kod skickas ut till mottagaren i ett slutet kuvert. Kortet skickas till postkontoret närmast mottagaren eller till annan vald distributionspunkt. Där möts kortet och kortägaren. Mottagaren byter sin transport-PIN-kod mot en egen av denne vald kod, varefter identitetskortet aktiveras och blir en aktiv fungerande digital identitetshandling.

IT-miljön

Så återstår att få IT-delen att fungera. Där är katalogtjänsten en mycket väsentlig del. Allt detta är byggt kring SEIS-specifikationerna, d v s det följer det regelverk som vi har kommit överens om i Sverige för att etablera säkra funktioner och procedurer. Vi använder oss av kända standardalgoritmer, som RSA, DES och Trippel DES.

Detta ska också kunna fungera i normalmiljö för användaren. Det ska vara möjligt att kunna byta ut säkerhetsfunktionerna som t ex kommer med en webbläsare till säkerhetsfunktionerna som finns i det digitala identitetskortet och på så sätt använda säkerhetsfunktioner och certifikat som garanteras av en allmänt betrodd tredje part.

Det krävs också att användaren, förutom kortet, har tillgång till en kortläsare. Användaren måste veta hur man kommunicerar med katalogen och hur man utför spärrprocedurerna. Det är Postens roll att som betrodd tredje part förmedla den informationen till användaren. Att vara betrodd tredje part är inte någonting som någon bara kan tilldelas eller ackrediteras till, utan det är något som man måste vinna på basis hur man själv agerar och hur man har genomfört de aktuella procedurerna. Posten har förutsättningar för detta efter att ha varit en betrodd tredje part i över 350 år vad gäller transport av information och efter att ha gett ut vanliga fysiska identitetskort i över 30 år och hittills inte blivit ifrågasatt i dessa roller.

Internationellt samarbete

För att sprida vår lösning internationellt arbetar vi tillsammans med andra postverk i Postal Security Services där postorganisationer samarbetar för att föra in samma infrastruktur och samma nivå av förtroende på de certifikat ges ut i andra länder. De nordiska postverken och Irland är överens. Diskussioner förs med ett stort antal andra postverk. Detta kan leda till en infrastruktur som kan fungera på samma sätt i många länder. Via samarbete med organisationer som Netscape och Microsoft hoppas vi kunna bredda detta ytterligare. Vi kommer att korscertifiera varandra mellan organisationer som etablerar TTP/CA-tjänster och ger ut certifikat på samma förtroendenivå.

Utfrågning av Evald Persson, Posten AB

Utfrågare:

- Direktör Bengt-Åke Eriksson, Nordbanken.

- **Vilken är den egentliga affärsidén för Posten att bli utgivare av tjänster på detta område?**

  När vi ska använda de osäkra kommunikationsnäten på många olika sätt behövs denna typ av infrastruktur inklusive våra egna tjänster. Vi har många tjänster som behöver få tillskottet av säkerhet, så Posten har primärt en egen användning.

  Posten har också en samhällsroll. Därför vill vi hjälpa till i uppbyggnaden av infrastrukturen och driva på utvecklingen. Posten har lite mer bråttom än vad marknaden i övrigt har, så vi driver på för fullt.

- **Som köpare till dessa tjänster tar man väldigt stora affärsrisker som inbyggda i tjänsten. Vilka risker är Posten som tjänsteleverantör beredd att dela med kunden?**

  Vi ger ut certifikat under ett antal olika policies. Varje nivå i policyn har en viss säkerhet. Där anger vi vad vi tar ansvar för. Det är klart att det kommer att hända saker och det kommer att behövas förändringar löpande. Vi kommer att tvingas till att ha stor flexibilitet i systemen. Men vi tar inget direkt ekonomiskt ansvar för tillämpningar som använder tjänsten, utan vi presenterar hur vi har byggt upp infrastrukturen och sedan är det upp till den som väljer att tillämpa den att tro på den eller inte.

- **En fråga är längden på CA-kedjorna – tar Posten ansvar för kedjorna?**

  Vi vill ha så korta CA-kedjor som det bara går att åstadkomma. Helst skulle vi vilja se att det bara fanns en enda CA i Sverige [d v s Posten], fast det är väl en utopi. De naturliga CAna är de som idag ger ut identitetskort, i princip bankerna och Posten som det finns ett utbrett förtroende för.

- **När kommer vi att kunna se resultat av den internationella samverkan med andra postverk?**

  Jag tror inte att vi ska hoppas att det går alltför fort. Det tar säkert minst ett år innan vi börjar se att vi har korscertifieringar åt andra håll. Men det kommer. Det viktiga är att utvärdera den policy som ligger bakom certifikatet. Det är dem som man ska korscertifiera, inte företagen som ger ut. Därför kommer man att ge ut certifikat under ett antal olika policies även inom ett företag som betraktas som säkert. En del är programvarubaserade certifikat och de är ju lätta att stjäla tillsammans med säkerhetsinformationen med hjälp av s k trojanska hästar och liknande saker i persondatorer.

- **Hur mycket av detta är kommersiellt tillgängligt från Posten?**

  Det är kommersiellt tillgängligt för testprojekt idag, men inte till marknaden. Det går inte att gå in på ett postkontor för att köpa ett kort ännu. Men det är inte långt borta.

- **Hur mycket kompetens kommer det att krävas av Postens tänkbara kunder?**

  Kunden ska kunna göra väldigt mycket utan att egentligen skaffa sig någon extra hjälp. Många tjänster, t ex digital signatur och konfidentialitet, kommer att vara inbyggda i standardprodukter för e-post och använda identitetskortets säkerhetsfunktioner.

- **Men det är ändå ett komplext område och det är farligt att i varje fall den närmaste tiden se för mycket till standardlösningar. Därför är det viktigt med ordentlig egen kompetens och att följa med i utvecklingen så att man vet vad man ger sig in på för något, hur trovärdiga än olika leverantörer kan vara.**

  Det går att skaffa hjälp från de exportföretag som vi är välförsedda med i Sverige, t ex Security Dynamics, Dynamic Software, AU-System, QA Information, Nexus. Nu börjar kompetensen också uppstå hos Nordbanken, Posten och ett antal andra ställen. Intema dataavdelningar på storföretagen börjar också kunna mycket. Så det finns en hel del kompetens att tillgå för den som inte har egen kompetens.

- **Kan kortutgivarna, t ex Posten, formellt garantera att kortets privata krypteringsnyckel inte kopieras eller lagras vid tillverkningsprocessen?**

  Att ge garantier är alltid svårt. Posten har inte för avsikt att kopiera eller lagra nyckeln. Vi kommer att göra allt för att se till att ha verifierade processer, där en extern revisionsorganisation kan intyga att Posten uppträder enligt gjorda åtaganden i policyn.

  Men får vi ett lagkrav på oss, att vi måste lagra nyckeln, har vi inget val. Då gäller det att se till att ha rutiner som inte kan missbrukas och att återskapande endast sker efter det i lagkravet fastställda regelverket.

Regelverk

Per Furberg, Utredningen om elektroniska pengar:

Rådmannen Per Furberg är sekreterare i utredningen om elektroniska pengar.

"Det är hög tid att starta det näringsrättsliga arbetet nu"

Inledning

Detta avsnitt belyser frågor om regelverk med anknytning till digitala signaturer.

Budskapet

I öppna system behövs en helt ny infrastruktur med alla de juridiska konsekvenser som det för med sig. Internationellt pågår en snabb rättsutveckling som i första hand tar sikte på de näringsrättsliga frågorna. I Sverige sker ännu inget och det är allvarligt eftersom vi ligger i framkant när det gäller att införa konkreta tillämpningar.

Rättsliga utgångspunkter

Traditionella underskrifter produceras på ett nästan självklart sätt och förmågan att underteckna är fysiskt knuten till individen, så skrivdonet kan ju inte komma på avvägar. Det går inte att skära av armen på någon och ta med sig armen för att underteckna. Någon närmare kontroll av en traditionell underskrift görs inte heller förrän någon ifrågasätter äktheten. Det finns också metoder för att med hög säkerhet analysera om en traditionell underskrift är äkta. Underlaget för sådana kontroller samlar man in, men inte förrän det behövs och den som inte är expert kan lätt bli vilseledd.

Digitala signaturer bygger istället på kryptografi och innehavet av en hemlighet – den hemliga nyckeln. Medan användaren "föds" med förmågan att underteckna på ett unikt sätt, tilldelas han nyckeln för digitala signaturer. Det innebär att vem som helst som har tillgång till signaturnyckeln (och de hjälpmedel som behövs i anknytning till det) kan signera. Alltså, skrivdonet kan komma på avvägar utan att den som skriver behöver vara inblandad med sina handrörelser. Därför måste det finnas säkra administrativa rutiner.

Den som tar emot ett digitalt signerat dokument (eller något annat signerat objekt) måste dessutom kunna verifiera att det är äkta. Men naturligtvis ska han därmed inte kunna signera med "avsändarens namn". Tekniskt går detta att lösa med öppna och hemliga nycklar. Signeringen sker med den hemliga nyckeln, medan den publika nyckeln används för verifiering.

Många juridiska konsekvenser

Resultatet blir en annan struktur än den i traditionell miljö. Underlaget för att skapa och verifiera signaturerna måste byggas upp på förhand, bevaras och i publika delar hållas tillgängliga så att mottagaren kan verifiera om signaturen är äkta. Öppna system förutsätter alltså en helt ny infrastruktur med alla de juridiska konsekvenser som de för med sig.

Från praktiska utgångspunkter är det helt avgörande om den som verifierar en signatur kan lita på den öppna nyckeln och den därtill relaterade hemliga nyckeln – och att den tillhör den angivna personen och ingen annan. Är det verkligen rätt person? Lika viktigt är det att den som verifierar, kan lita på att hemligheten inte har kommit på avvägar. Tekniskt kan IT-baserade rutiner göras mycket säkra, men om man administrerar dem illa så att hemligheter kommer på avvägar blir skyddet nästan värdelöst.

Frågan om insynsskydd är också förknippad med de digitala signaturerna, eftersom samma kryptografiska rutiner som används för att signera kan användas för att göra data oläsbara för den som inte har tillgång till krypteringsnyckeln. Detta aktualiserar en mängd motstående intressen, som behandlats bl a av regeringskansliets referensgrupp för krypteringsfrågor.

De aktuella rättsfrågorna

De rättsfrågor som är aktuella när rutiner för digital signatur införs gäller

- dels hur infrastrukturen bör utformas och hur ansvaret för den bör fördelas mellan de olika aktörerna
- dels hur de signerade objekten och anknytande rutiner inom handel, administration och förvaltning bör sorteras in i regelsystemet.

Näringsrättsliga frågor

Den första frågan gäller näringsrättsliga frågor. De beskriver man enklast genom en jämförelse med de skyddsregler som finns för finansiella institut, som t ex banker. Både nationellt och i form av EG-direktiv finns sådana regler. Lika viktigt som det är att skydda betalsystemen mot obalans och dominoeffekter etc, är det att skapa system för digitala signaturer som är säkra, sunda och stabila.

Dessa tre s k honnörsord från den finansiella sektorn passar som handen i handsken vid överväganden om digitala signaturer, bl a när CA-funktioner diskuteras, d v s Certification Authorities som har till uppgift att

- utfärda bevis, s k certifikat (legitimation om vem som har en viss öppen nyckel)
- att tillhandahålla de uppgifterna för den som ska verifiera en signatur.

Frågeställningar är

- om marknadskrafterna helt bör styra utvecklingen eller om det behövs regler i lag om tillstånd och tillsyn – jämför Riksbankens och Finansinspektionens uppdrag att ge skydd på det finansiella området
- vilken rättslig betydelse certifiering av aktörer och standardisering av rutiner bör ha
- vilket ansvar som en aktör som tillhandahåller tjänster för digitala signaturer bör ha
- hur civilprocessuella och straffprocessuella frågor om nycklar och anknytande uppgifter bör hanteras
- vilka krav som följer av Sveriges internationella åtaganden mot EU om en fri rörlighet.

Regler som bör gälla

Den andra gruppen av rättsfrågor avser vilka regler som bör gälla för handlingar och andra objekt som signeras elektroniskt och de rutiner som hör till. De materiella och processuella regler som då aktualiseras, kan sägas motsvara vad som hade gällt vid en rättslig prövning av rutiner baserade på traditionella underskrifter och de digitala signaturerna blir då aktuella på en mängd rättsområden.

Ofta imiteras de traditionella rutinerna så att analogier med nuvarande synsätt kan framstå som naturliga. Samtidigt kan vi konstatera att de digitala signaturerna sätter IT-rutiner för handel, betalningar och ärendehandläggningar "på hjul" så att hela handels- och handläggningsmönster förändras. Påfrestningarna på regelverken blir därmed stora.

Exempel på disparata rättsfrågor är

- materiella frågor om rättshandlingar i IT-miljö med användning av signerade objekt inom t ex avtalsrätten, köprätten, fordringsrätten, skadeståndsrätten och förvaltningsrätt samt anknytande konsumentfrågor

- civilprocessuella frågor, t ex när ett företag eftersträvar att förenkla sin administration och få räkenskapsmaterialet i helt digital form – hur ska man då i nästa led när en process uppstår hantera frågor om skriftligt bevis eller rättare sagt om dokumenterat bevis? Rättegångsbalken använder ju uttrycket "skriftligt bevis". Här kan också missbruk tänkas, t ex genom en begäran om edition. Om er motpart vill slippa en tvist kanske han begär ett editionsföreläggande som tar sikte på era hemliga nycklar under åberopande av att intresset är att kontrollera om bevisningen är äkta, medan avsikten är att därigenom förstöra skyddet eller att få käromålet återkallat.

- straffrättsliga och straffprocessuella frågor: Kan bestämmelserna om straffansvar tillämpas i den nya miljön som reglerna ser ut idag? Kan husrannsakan, beslag, teleavlyssning, teleövervakning m m ske?

- övriga frågor, som berör t ex offentlighetsinsyn, sekretess, persondataskydd, redovisningsförfattningarna och arkivförfattningarna.

Nya regelverk som krävs

Internationellt pågår en snabb utveckling som i första hand tar sikte på de näringsrättsliga reglerna för digitala signaturer. Det finns alltså i många amerikanska delstater redan sådan lagstiftning. Tyskarna har nyligen fått en sådan reglering och arbete pågår i bl a Danmark och Belgien. Ett intensivt arbete pågår i vissa internationella organisationer, t ex EG, OECD och UNCITRAL.

Men i Sverige finns ingenting inom den rena näringsrätten. En hel del utredningsarbete har dock redan gjorts när det gäller regleringen av de signerade objekten och de rutiner som hör dit, t ex de frågor som uppkommer inom elektronisk handel och när myndigheterna vill gå över till IT-baserade rutiner för ärendehandläggning.

Förvaltningsrättsliga frågor har behandlats av flera svenska utredningar på tullområdet, skatteområdet och för exekutionsväsendet. Lagstiftning har redan genomförts.

IT-utredningen har under 1996 i betänkandet Elektronisk dokumenthantering (SOU 1996:40) föreslagit bestämmelser om digitalt signerade handlingar för hela förvaltningen. IT-utredningen har också behandlat frågor om avtal och anknytande civilrättsliga frågor i IT-miljö. Elektroniska betalningar övervägs nu av utredningen om elektroniska pengar. Straffrättslig och straffprocessuella frågor har behandlats av Datastraffrättsutredningen i ett betänkande från 1992 med förslag till anpassningar av bl a brotten mot urkunder.

Dessa utredningsförslag – som har skrivits just med tanke på rutiner för digitalt signerade objekt som ersätter traditionella motsvarigheter – har inte lett till lagstiftning[3]. Tvärtom är det så för de straffrättsliga och processrättsliga frågorna att det pågår en ny utredning. Många andra frågor har också utretts där IT-rutiner med anknytning till digitala signaturer berörts, t ex frågor om offentlighetsinsyn, persondataskydd, arkivering och bokföring.

Behovet av nyskapande

Det finns ett uppenbart behov av att utreda de näringsrättsliga frågorna. Den omfattande användningen av digitala signaturer som planeras och som delvis redan håller på att införas ger dessa frågor helt nya dimensioner. Sverige finns i främsta ledet när det gäller att införa konkreta tillämpningar.

Men näringsrättsligt sker i stort sett ingenting. Skulle en genomlysning inte bli av, kommer Sverige naturligtvis på efterkälken i det rättsliga skyddet för t ex

- allmänhetens tillit till de digitala signaturerna och
- skyddet för den infrastruktur som byggs upp.

[3] Det nära sambandet mellan utredningsförslagen och digitala signaturer blir särskilt tydligt vid en genomgång av följande åtgärder som avses kriminaliseras också i IT-miljön.
Materiell förfalskning innebär att bevismedlet – helt eller delvis – inte är framställt av den, från vilken det har sken av att härröra; det är oäkta. *Positiv* materiell förfalskning (se 14 kap. 1-3 och 7 §§) innefattar förfaranden, genom vilka ett oäkta bevismedel framställs eller begagnas (t ex att signera med någon annans namn eller att åberopa ett på sådant sätt manipulerat dokument).
Negativ materiell förfalskning (14 kap. 4 § BrB) innebär att ett äkta bevismedel helt eller delvis utplånas (t ex att förstöra en journal).
Vid *immateriell* förfalskning angrips bevismedlets funktion, medan bevismedlet som sak lämnas oberört. Dessa angrepp hänför sig sålunda endast till äkta bevismedel.
Positiv immateriell förfalskning kan bestå i ett förfarande som även kallas intellektuell förfalskning (15 kap. 10 § och 11 § första stycket BrB), nämligen att den som framställer ett bevismedel ger det ett oriktigt innehåll (t ex att en läkare lämnar felaktiga uppgifter i en journal eller ett läkarintyg). Positiv immateriell förfalskning kan också bestå i att någon, med ett bevismedel som både är äkta och sant, söker bevisa någonting annat än vad som skall styrkas med det; exempelvis att utge sig för att vara någon annan under åberopande av dennes legitimation (15 kap. 12 § BrB).
Negativ immateriell förfalskning består i att exempelvis att förneka sin underskrift på en urkund (15 kap. 13 § BrB).

Påverkar alla rättsområden

När det gäller regleringen av de signerade objekten och anknytande rutiner, bör i första hand undersökas om det omfattande utredningsarbete som redan har gjorts går att ta till vara. Även om de förslagen skulle leda till lagstiftning, återstår mycket att göra.

Införande av digitala signaturer på bred front påverkar nära nog varje rättsområde.

Konsekvenserna går att se ur många olika rättsliga perspektiv:

- Skadeståndsexperten ser en massa ersättningsfrågor och komplicerade samband mellan olika aktörer där man kan fråga sig om oaktsamhet finns vid ett visst förfarande och om det behövs strikt ansvar, d v s oberoende av fel eller försummelse eller om s k presumtionsansvar bör införas.

- Familjerättsexperten börjar fundera över om en revokering går att jämställa med att beröva någon rättshandlingsförmågan i digital miljö.

- Konsumenträttsexperten börjar borra i allt det "finstilta" som olika aktörer försöker foga till själva signaturerna eller de överenskommelser som signeras.

- Immaterialrättsexperten börjar att överväga olika ideella rättigheter knutna till kryptosystem, m m.

- Bolagsjuristerna börjar överväga t ex frågor om hur firmateckning ska gå till i den nya miljön eller om datorerna med automatik och rättsligt bindande verkan kan signera för bolagets räkning vissa rättshandlingar som dokumenteras i digital form.

- Bankjuristerna undrar om man kan ge ut elektroniska pengar eller löpande handlingar i digital form och om dessa går att tradera med samma sakrättsliga verkan som för traditionella fysiska objekt.

- Och så vidare.

Rättspolitiska avvägningar

Det svåraste blir, emellertid, att göra de känsliga rättspolitiska avvägningarna som kommer att krävas. Vi är ju vana vid att det i varje lagstiftningsärende måste göras vissa avvägningar mellan olika rättsområden. I anknytning till digitala signaturer blir balansfrågorna så oerhört mycket svårare. Allt hänger ihop som i en webb, att drar man i ett hörn av webben rör sig alltsammans.

Detta kommer att vålla problem därför att

- de berörda intressena har en sådan styrka,
- vissa avvägningar ser ut att bli omöjliga att göra
- kopplingarna mellan olika rättsområden blir omfattande.

Än en gång – det är viktigt att starta det rättsliga arbetet nu.

Utfrågning av Per Furberg, Utredningen om elektroniska pengar

Utfrågare:

- Professor Peter Seipel, Institutet för Rättsinformatik, Stockholms universitet.
- Advokat Stefan Bernhard, Lagerlöf & Leman Advokatbyrå, Stockholm, och ICC.

- **Det är intressant att samma nycklar kan användas för många olika funktioner. Man kan fråga sig hur önskvärt det är att var och en har sitt identitetskort med – i värsta fall – en mängd nycklar. Även om identiteten klarläggs på den som företar en rättshandling, så säger det ingenting om dennes rättsliga handlingsförmåga, t ex om han är omyndig, står under förmyndare eller har gått i konkurs. Är sådana frågor av betydelse?**

De är av utomordentlig betydelse i ett brett rättssäkerhetsperspektiv. Det finns en tendens att vilja flytta över bevisbördor, t ex för behörighet att vidta en rättshandling. Idag får den som drabbas av en förfalskning stå där med lång näsa, om vi tittar på skuldebrevslagens regler. En invändning om förfalskning gäller även mot t ex en ny innehavare av ett skuldebrev. Ett exempel på motsatsen finns i EDI-avtal 96 som förenklat beskrivet säger att om systemet har sänt, så ansvarar den som har systemet.

Spinner vi vidare på tråden om alla dessa certifikat, finner vi att det är utomordentligt betydelsefullt vad ska det ha för verkan att det framgår att någon är firmatecknare eller att någon är t ex läkare. Ska vi helt bryta ner de regelverk som vi har idag för att pröva frågan om behörighet? Först måste man fundera på rättsfrågorna, innan man inför sådana lösningar. I annat fall blir de utomrättsliga.

- **Kan det leda till att man har ett certifikat för själva identiteten och ett annat certifikat för handlingsförmågan?**

Det verkar vara så som många tänker. Jag har haft många mål i domstol på frågan om någon ska anses ha varit behörig företrädare. Då går man till Patent- och registreringsverket och tittar i bolagsbyråns register som har rättsverkan. Vilken blir då följden om vi byter metoder? Är vi beredda att göra det utan att lagstiftaren också har sett till att det nya systemet hänger ihop?

- **Du beskriver detta som ett stort fält med en lång rad rättsliga frågor som alla hänger samman på olika sätt – det verkar lite paralyserande. Finns det inte något slags dominospel där vissa regleringsfrågor är mer fundamentala och andra kan betecknas som sekundära, tertiära o s v så att det går att skaffa sig en genomtänkt lagstiftningsstrategi?**

Det är inte praktiskt möjligt att ta hela greppet och göra en enda plan. Det skulle bli övermäktigt för lagstiftaren. Man bör istället gå in på de områden som är mest akuta – och göra det snabbt. Samtidigt behöver man på något vis skaffa den kompetens som krävs för att se hur alltsammans hänger ihop, så att man inte gör något som är alldeles tokigt i ena änden med beaktande av vilka följderna blir på ett annat rättsområde.

När det gäller att utforma en strategi har jag inte inblick i hur sådant arbete går till inom departementen. Men det är nödvändigt att detta helt enkelt lyfts upp på dagordningen, så att frågan inte kommer i sista hand. Annars kanske vi får en utveckling där frågan löses praktiskt, men utan att lösningen kanske är rättsligt acceptabel. Därför är det viktigt att detta kommer upp på dagordningen.

- **Det är oklart i vilken omfattning man är beredd att ta ett civilrättsligt skadeståndsansvar för oriktigheter i CA-hanteringen. Fråga 1: Är det möjligt enligt svensk lag idag att friskriva sig på ett omfattande sätt? Fråga 2: Skulle den modell som gäller för Värdepapperscentralen och hanteringen av digitala aktier (och som föreskriver strikt ansvar) kunna ligga till grund?**

  Om det strikta ansvaret skulle genomföras fullt ut, kanske det inte skulle bli så många fler praktiska tillämpningar eftersom det nog inte skulle vara så många som vågade.

  Däremot kan det finnas fog för ett skärpt ansvar, kanske i stil med hur det fungerade när bilförare blev tvungna att exculpera[4] sig. Om du har ett system och jag är användare, hur ska jag kunna gå in i ditt system och kolla att du har skött dig rätt och föra bevisning om att du har varit oaktsam. Jag tror att vi måste lägga oss någonstans däremellan. Tanken går till t ex fastighets- och miljörätt där man vid svårbevisade orsakssamband tenderar att lätta på kärandens bevisbörda.

  När det gäller friskrivningar går tanken till avtalslagens ogiltighetsregler, om friskrivningen gör att den enskilde står där utan möjligheter att hantera sin situation; d v s denne är i händerna på CAn. Det borde ju också vara aktuellt att titta på vad det finns för regelverk på konkurrensområdet o s v.

- **Ska man lagstifta om nyckellängder? Eller ska man nöja sig med allmänna uttalanden i lagstiftningen att saker och ting ska ske på betryggande sätt o s v?**

  Frågan indikerar att du menar att vi naturligtvis inte kan gå tillväga på det sättet. Vi ska kanske istället titta på hur väl t ex avtalslagen, som är teknikneutral (och gammal), verkar kunna fungera på IT-området. Vi behöver söka sådana övergripande koncept, där det blir lätt för en domstol att förstå vad det är frågan om och där vi också kan anpassa de tekniska lösningarna och de juridiska lösningarna till varandra på ett flexibelt sätt.

- **Varför arbetar Justitiedepartementet med IT på ett plottrigt sätt i de befintliga enheterna – vore det inte bättre med en lagstiftningsenhet för IT-frågor?**

  En särskild lagstiftningsenhet för IT går knappast att inrätta. Skulle man samla på en sådan enhet all den kompetens som behövs kommer ju den enheten att efterhand inrymma hela verksamheten, så som utvecklingen går.

[4] Exculpera innebär att styrka att man inte förfarit vårdslöst för att därigenom befria sig från ansvar.

D. Hur kan system för digital identifiering/signatur införas?

Översikt

Denna del innehåller en utfrågning och diskussion kring frågan hur system för digital identifiering och signatur praktiskt ska kunna införas i Sverige på kort och lång sikt.

Utmaningar

Det finns en stor förväntan på att det ska ske ett införande av system för identifiering och identitet i digitala miljöer. Väl fungerande sätt för identifiering är en grundbult i en kommande nätbaserad ekonomi. Om många olika typer av angelägen alla-till-alla-kommunikation ska bli verklighet för förvaltningar, näringsliv och enskilda är detta att kunna säkerställa identiteten helt nödvändigt. Vi står på tröskeln till den utvecklingen.

Bilden ter sig komplex. Identifikationsproblemet rymmer frågor kring digitala signaturer, digital identifiering och konfidentialitet. Mycket av tekniken förefaller att finnas tillgänglig, men därutöver finns ett antal utmaningar att ta sig an.

1. Standarder och marknadsutveckling
En viktig fråga är utvecklingen och acceptansen av standarder och i vilken utsträckning detta kan driva fram en marknad. Mycket handlar det om politik. Det pågår en internationell utveckling och det gör att det inte går att se detta enbart ur ett svenskt perspektiv. En utmaning är att få internationella acceptans och spridning för de lösningar som SEIS har utvecklat.

2. Regler och tillsynsfunktioner
Det behöver utvecklas regler. Frågor att skyndsamt lösa är om det vara en lagstiftning om digitala signaturer och hur den ska se ut. Behövs det regelverk för CA och en tillsynsmyndighet för detta?

3. Individens acceptans och användning
I grunden handlar det om att individen ska vara identifierad och kunna identifiera sig och därför gäller det att utveckla system som individen accepterar och använder. Utmaningen är att förmå användarna att förstå nyttan av att kunna legitimera sig och bekräfta rättshandlingar i digitala miljöer.

Hur kan system för digital identifiering/signatur införas?

Utfrågningar

Inledning

Om inriktningen på utvecklingen råder i stora drag enighet – det är en nödvändighet att införa system för identifiering och identitet i digitala miljöer. Den stora frågan gäller tempot i genomförandet. Är det möjligt att gå fram med den brådska som en del förespråkar? Eller är det frågan om en stegvis utveckling under de närmaste åren? Följande utfrågning belyser det.

Utfrågare

Göte Andersson, journalist.

Utfrågade

- Organisationsdirektör Britta Johansson, Statskontoret.
- IT-utredare Anne-Marie Eklund-Löwinder, Statskontoret, och representant för Snus.
- Utredare Göran Ribbegård, Spri.
- Advokat Stefan Bernhard, Lagerlöf & Leman Advokatbyrå, och representant för ICC.
- Direktör Berne Landgren, VD för Telia Megacom AB.
- Projektledare Jerker Sjögren, Stockholms stad.
- Ambassadör Magnus Faxén, UD, och regeringens utredare av en svensk krypteringspolicy.

Utfrågning av Britta Johansson, Statskontoret

Britta Johansson är organisationsdirektör vid Statskontoret.

- **Hur snabbt är det möjligt att rulla ut detta i stor skala genom bl a den upphandling som du arbetar med inom Statskontoret och Toppledarforum?**

Det är svårt att svara på. Vi gör ett försök att genom upphandlingen att åstadkomma en del av förutsättningarna. Men det är inte den enda delen. Sedan måste man i de olika organisationerna hitta var de viktiga tillämpningarna är, alltså var man ska börja någonstans. Det rår inte vi över helt och hållet.

Detta är en stegvis process där man rycker fram på en front. Har vi gjort upphandling av korten får man hitta i vilka situationer det är lämpligt att driva fram en fram en ändring av regelverket och var man behöver utveckla tillämpningar. Så stegar man sig framåt. Hur lång tid det kommer att ta är svårt att sia om. Förmodligen skyndas det på, om man från högre instanser sätter upp mål av typen "att nu ska ni se till att rationalisera genom att använda tekniska lösningar inom si och så lång tid". Det driver processen framåt.

- **Om det är raketfart som är målet (och det låter så när man hör alla olika signaler) och om regeringen och alla på den politiska fronten gör vad de kan – hur den offentliga sektorn gå fram om man vill?**

För att kunna svara på den frågan måste man ju veta: Gå framåt – vart? Det är inte farten som är målet, utan det är ju att komma någonstans. Det sönderfaller i en massa olika frågeställningar. Digitala signaturer finns t ex redan för Tullverket. Om man i alla sammanhang där man idag har manuell hantering, ska komma över i elektronisk form och därtill med all lagstiftning på plats – det kommer att ta ganska lång tid. Vissa saker går att lösa inom det närmaste året. Sedan finns hela skalan däremellan. Det går inte att säga mera.

- **Det blir alltså en utdragen införandeprocess?**

  Ja, det blir det.

- **Vilka är de största hindren för ett snabbt införande inom den offentliga sektorn?**

  Då måste man ju fortfarande fråga sig: I vilket sammanhang då? Vi har inom offentlig sektor t ex avgränsat frågan kring elektronisk handel. Där finns avtal, leverantörer och planer på att förse de handlande parterna med kort för signaturbruk. Det är på god väg.

  Övriga tillämpningar arbetet håller vi på med och det är inte lika långt kommet. Inom t ex landstingsvärlden finns planer på att ska använda kort för vissa tillämpningar i journalhantering och annat.

  Digitala signaturer kommer på en tillämpning i taget, tror jag. Det blir alltså inte så att plötsligt är digitala signaturer införda i alla tillämpningar och alla tänkbara situationer i offentlig verksamhet. Så kommer det inte alls att gå till. Regelverket är olika. Behoven är olika. Mognaden, trycket och förväntningarna är också olika.

- **Men under nästa år kommer det att finnas tillräckligt underlag för att genomföra upphandlingen?**

  Om vi inte finner att det finns ett underlag, kommer vi inte att göra någon upphandling.

- **Sett ur Statskontorets perspektiv har ni ännu inte svaren på om underlaget finns för att gå fram så snabbt som man har talat om?**

  Vi har inte svaret. Men vi arbetar på att få fram det nu. Å andra sidan jag inte arbetat med dessa frågor särskilt länge.

- **Får vi tolka det som att substansen för att driva en snabb utvecklingen ännu inte är på plats?**

  Det är möjligt att den är. Men jag har den inte listad på papper. Det kanske jag har om två månader och då fattar vi beslut om vi har underlag för upphandling eller inte.

- **SEIS har ett upplägg för hur man ska införa identifiering och identitet i digitala miljöer. Finns förutsättningar att det upplägget ska kunna vinna både i Sverige och i andra länder?**

  Till att börja med, för att man ska kunna referera till SEIS-standarder måste de vara färdiga och ha befunnits möjliga att genomföra. Där finns idag brister såvitt jag kan se.

  Om man får fram en helhetslösning som fungerar och börjar använda den – även i en liten ö som i Sverige – och visar att vi faktiskt har klarat av hela kedjan, tror jag att vi har bra på fötterna.

  Visar det sig sedan att internationella krafter och marknadskrafter drar iväg någon annanstans, är inte det värre än att vi får följa efter. Det är ju ingen 20-årig livslängd på sådana här saker, utan de går att förändra. Det är bättre att vi här i Sverige arbetar på, än att vi väntar på att allt ska lösas internationellt.

- **Så Sverige kan gå före?**

Ja, det finns mycket i Sverige att bygga på. Vi har en bra mognad som gör att vi är väl lämpade för sådana här lösningar. Det finns acceptans för tanken med identitetskort. Vi har personnummer. Vi har ganska många beståndsdelar som är viktiga.

- **Ytterst är det naturligtvis ekonomiska fördelar som driver fram utvecklingen i företag som Ericsson. Även inom den offentliga sektorn är effektivare metoder knutna till ekonomiska fördelar. Finns någon bedömning av hur stora vinster som det går att göra genom att föra in tekniken?**

Det har jag ingen som helst ambition på att försöka svara på.

Utfrågning av Anne-Marie Eklund-Löwinder, SNUS

Anne-Marie Eklund-Löwinder är IT-utredare vid Statskontoret och verksam inom Swedish Network Users Society (SNUS)[5]

- **Hur snabbt utifrån Internet-perspektivet är det är möjligt att rulla ut de nya tjänsterna med identifiering och identitet i digitala miljöer.**

Vi måste tänka på att digitala signaturer och säker identifiering också är absolut nödvändigt för att säkerställa själva näten. Styrinformationen för Internet t ex i Sverige har också behov av funktionerna kryptering, digital signatur och säker identifiering. Det finns belyst i Internet-utredningen från Statskontoret.

T ex informationen i domännamnsservrar DNS (som översätter mellan IP-adresser och domänadresser) måste säkerställas och signeras. Det arbetet påbörjades under november genom användning av ett protokoll som heter DNS-Sec.

När det gäller hur snabbt vi kan införa tjänsterna, är det inte svårt när det gäller branschspecifika eller företagsspecifika tillämpningar. Det går att göra i stort sett omgående.

Problemet uppstår när vi börjar tala om globala tillämpningar, globala i meningen Sverige, att vi alla ska kunna nå varandra på detta sättet och vara säkra på vem den andra är, vara säkra på den andra signaturen o s v – där är vi ännu inte. Dit är det långt.

Ofta brukar man tala om denna typen av lösningar som teknikdrivna och att teknikerna går på och skapar lösningar som inte har någon grund, etc. Nu säger man från olika håll att tekniken är klar, att den är färdig att införa. Det hävdar jag är fel. Den finns inte på plats när man talar i det globala perspektivet. Däremot finns tekniken för tillämpningar inom en organisation eller en bransch.

- **Så hur lång tid tar det rimligtvis att rulla dessa tjänster så att allmänheten och småföretagen omfattas och även trafiken mellan företag?**

Mellan tummen och pekfingret dröjer det 4–5 år innan det blir volymer. Det ska finnas kortläsare överallt vart du än går. Det ska finnas program som kan hantera en kortlösning. Vi ska övertala Microsoft att ha det med i sina produkter eller att vi hittar på sätt som löser det. Det finns en massa saker som man måste lösa. Det tar tid.

- **Vilka är de största hindren?**

Det vore om vi fick en oerhört restriktiv syn på användningen av kryptering och krypteringsteknik. Det skulle vara ett stort hinder naturligtvis eftersom allt bygger på kryptoteknik. Det är en politisk boll.

Ett annat hinder är att om inte kommer fram regler som gäller för utfärdaren av det certifikat med vilket jag signerar min deklaration som sedan ska skickas in till Riksskatteverket i Sverige. Men det behöver inte nödvändigtvis vara en lagstiftning.

[5] SNUS är en ideell förening för svenska nätanvändare vars syfte är att höja kunskapen om nät och användning av nät, primärt Internet. Antalet medlemmar är cirka hundra. Det var SNUS som bidrog till att utveckla det första kommersiella IP-nätet, Swipnet.

- **Vilka möjligheter har SEIS upplägg att göra sig gällande i andra länder?**

Snus har sett att det finns en del poänger med det som SEIS gör. Vi behöver någonting som SEIS, det är alldeles uppenbart. Men det kanske borde genomföras på hemmaplan först, d v s det ska finns någonting mera innan vi börjar sälja lösningen internationellt. Det måste vara mer färdigt. Vi ska alltså inte sälja skinnet innan björnen är skjuten.

- **Men Snus måste ju sälja in detta inom Internet-världen, så att det där finns en beredskap att lyssna på de erfarenheter som går att vinna i Sverige?**

Där finns ett kulturellt problem genom att det allmänt inom Internet-världen råder en stor misstro mot kort och korttillämpningar. Det är något som måste överbryggas på sikt.

Men allt är inte bara elektroniska identitetskort. Det finns många andra typer av användningsområden, t ex där tillämpningar ska tala med varandra eller där datorer ska tala med varandra. Det finns många sådana fall där det inte är möjligt att ha kortlösningar, men där det ändå måste kryptering, säker identifiering och signering.

- **Vilka är de största vinsterna för Internet-världen med att införa system för identifiering?**

De största vinsterna är ett säkrare, mer tillgängligt och robust Internet.

Men vi måste förstå att i ett införande på global nivå, kommer det att uppstå oväntade problem. Det kommer att kräva tålamod, uthållighet och flexibilitet av oss. Vi får inte låsa oss i förhand till en given lösning, utan detta måste växa fram. Vi får inte sträva efter perfektionism från starten, utan det måste provas.

Utfrågning av Göran Ribbegård, Spri

Göran Ribbegård är utredare inom Spri, Hälso- och sjukvårdens utvecklingsinstitut, Stockholm.

- **Vårdens förhållande till IT är lite mer grannlaga än många andra genom t ex integriteten. Kraven är höga när det gäller hantering av journaler och annat. I det perspektivet, hur snabb kan utvecklingen inom detta område blir inom sjukvården?**

Problemet är vilken utveckling som avses. IT-användningen inom sjukvården är väldigt diversifierad. Det finns alla möjliga olika system och behov på många olika områden. Men fortfarande finns det till stora delar inte bra tillämpningar för delar inom sjukvården.

Därför är frågan svår att besvara.

Om det handlar om meddelandehantering eller remisshantering (som vi kallar det), så är det i gång och det kommer mer under 1998 i sådana tillämpningar.

Om det handlar om avancerad journalhantering i vårdflöden och vårdprocesser, dröjer det säkerligen fem år. Men detta styrs mycket också av tillämpningsutvecklingen.

- **Ni tror på en gemensam teknisk lösning av det slag som SEIS har skissat på?**

Ja, Spri är mycket positiv till SEIS. Vi arbetar i SEIS. Det är viktigt med en nationell samordning.

Men vi bevakar också intensivt den internationella marknaden. Det beror på att sjukvården i Sverige är för liten för en egen programvarumarknad, åtminstone inom sjukhussidan. De övriga delarna av vården är idag redan långt datoriserade. Sverige har cirka 100 sjukhus och det är ingen marknad. Därför måste vi hela tiden känna av vad som händer t ex på Europafronten och internationellt. Det är klart, att om det kommer stora produkter på den nivån som löser frågorna på ett annat sätt, kommer vi naturligtvis att noga överväga det. Men idag vi är mycket inriktade på att se vilka möjligheter som finns med de lösningar som SEIS för fram.

- **Vore det möjligt att få SEIS upplägg accepterat i resten av Europa?**

Ja.

- **Vilka signaler finns i det avseendet från sjukvårdens människor i andra länder?**

Spri arbetar mycket i EU-projekt, bl a i Trust Health-projekten. Där har vi kontakt med ett antal sjukvårdsorganisationer i andra länder inom EU. Där är SEIS-modellen utgångspunkt för bl a kortfrågorna. Det är en bra signal.

- **Andra länder kanske väntar på att SEIS-modellen ska införas i Sverige, för att den sedan ska kunna rullas ut i resten av Europa?**

Ja, inom sjukvårdsorganisationer är man nog ganska intresserade av att någon kommer i gång med någonting och man skulle nog gärna se att en SEIS-modell startas.

- **Vilka är de största hinder för att införa SEIS-modellen?**

Hindren på sjukvårdens område är egentligen avsaknaden av lämpliga tillämpningsprogramvaror, d v s att ha någonting att säkra. Det känns lite övermaga att tala om säkerhetslösningar, när man inte har någonting att säkra.

Det som är viktigt är att få i gång tillämpningsutvecklingen och en bra fungerande marknad. Sedan är det naturligtvis kritiskt och intressant att se hur den marknaden kommer att välja väg.

Idag kan man med intresse se att det bildas en förening i USA kring sjukvårdens användning av Microsoft-produkter. Sådant kan ge tyngd på området. Det finns också andra områden där man arbetar med sjukvårds-IT-tillämpningar kopplade till företagsprodukter. Utvecklingen beror mycket på hur marknaden för sjukvårdsprodukter kommer att se ut.

- **När går det att se vilket vägval som går att göra?**

Det beror på vilket område det handlar om. Det är ett så brett område med många olika produkter. Och det växer fram olika inom olika områden. Det kommer ingen slutgiltig lösning eller någon riktigt tydlig bild inom det närmaste femårsperspektivet.

- **Det kan alltså bli andra kortlösningar [än SEIS] som kommer fram inom sjukvården?**

Ja, det tror jag definitivt. Detta kommer ju att utvecklas. Det är inte ett område som slutar med SEIS-specifikationen.

- **Och det går inte att göra SEIS-specifikationen så bra, att den kan konkurrera ut allt annat?**

I evig tid, nej.

- **Har SEIS en chans att dominera under de närmaste fem åren?**

Fem år är väldigt lång tid i branschen. Vi lever med treårsperspektiv – och redan detta känns som evigheter. Jag vill därför inte svara vidare på den frågan.

- **Ambitionen och tron att Sverige ska kunna gå före och visa vägen, bygger ju också på en bedömning av de samlade konkurrerande alternativen för dagen?**

En förutsättning när man arbetar med detta, är att gå in för öppna system. Man söker standarder. En viktig faktor hos öppna system och standarder är att man kan byta ut komponenter. Det betyder att en ny kortlösning, kan leda till att den pusselbiten byts.

Det blir alltså inte ett färdigt pussel, utan det blir något som består av många bitar där vi kommer att få se olika bitar bytas efterhand. Men trots det hänger pusslet ihop. Detta måste vara den rätta inriktningen och det är definitivt den inriktningen som Spri har; att söka standarder och försöka bygga ett öppet system.

- **Vilka vinster går att nå inom sjukvården?**

Som Lars Ingelstam sa: "Tillit, vad är det för någonting? Jo, det är att dina intressen blir beaktade även när du inte själv är i någon position att försvara dem." Detta är som en definition av sjukvård. Tillit är grunden i sjukvård.

Vinsten som vi kan få med detta, är att vi verkligen kan sälja in tillit i sjukvården – det är det viktigaste.

- **Samtidigt är sjukvården i en process där man letar efter IT-lösningar som sparar pengar?**

Javisst. När sjukvården letar efter IT-lösningar som sparar pengar, tittar sjukvården väldigt mycket på processorientering, d v s att försöka fördela arbetet. Då tas nya delar av samhället in. Kommunerna håller i dagens läge på att involveras mer och mer i sjukvård. Det blir mer och mer kommunikation som blir viktig. Därmed blir frågorna säker kommunikation ännu viktigare.

Vi får en specialistsjukvård som handlar om att kunna nå specialister över hela landet och därmed kunna utnyttja specialistkunskapen på bredare front. Återigen detta att veta vad det är för specialist som svarar – vad är han specialist på? – och att sedan få honom att signera ett specialistutlåtande så att man kan gå tillbaka och säga: "Du sa ju ..." Det går hand i hand. Ju mer vi försöker söka lösningar på vårt sjukvårdsproblem genom att användning av IT, desto mer av frågorna kring system för identifiering och identitet i digitala miljöer behöver vi lösa.

Utfrågning av Stefan Bernhard, Lagerlöf & Leman samt ICC

Stefan Bernhard är advokat vid Lagerlöf & Leman Advokatbyrå, Stockholm, och representant för ICC[6].

- **ICC har nyligen publicerat ett förslag till regelverk för detta område och det är tydligt att det pågår en internationell process. Med den bakgrunden, hur snabbt kan det vara möjligt att rulla ut tjänster för identifiering och identitet i digitala miljöer i Sverige?**

Frågan är för generellt ställd. Det beror på vilka ambitioner man har. Om det ska vara ett totalt genomförande, d v s att om en var människa ska ha sitt identitetskort och kunna göra affärer kommer det att ta väldigt lång tid.

Snabbheten beror också på vilka problem som man har på olika sektorer. Det finns en viss skillnad mellan de offentliga organen och näringslivet.

De offentliga organens behov och krav på säkerhet och verifierbarhet präglas av det hela tiden är en rättslig process. Skattemyndigheterna t ex vill vara säkra på att de kan bevisa att jag har skatteförfalskat i min deklaration. Finns inga regler på den punkten går det inte att bli fälld heller.

I näringslivet och i enskilda förhållanden är det en annan syn på tillvaron. Där finns inte samma krav på säkerhet.

- **För näringslivet är det uppenbart viktigt att snarast kunna använda säker kommunikation med leverantörer och kunder (för att bl a säkert kunna hantera stora pengar) – hur snabbt är det möjligt att införa de möjligheterna för svenska företag?**

Det beror på. Det som händer nu är att väldigt många banker satsar, så det börjar och slutar med pengarna.

När man gör avtal på EDI-sidan mellan organisationer, i en bransch eller i en grupp av företag som arbetar ihop på kontraktuell basis, går det att lösa många av frågorna i kontrakt.

Men det är den öppna hanteringen – utan kontrakt – som är problemet. Där är det nödvändigt att behöva vänta ytterligare tills det finns regler för hur certifieringsprocesser ska gå till och hur man i övrigt ska hantera den typen av frågor.

Det är i det ljuset som ICC levererat sin Guidec som är internationellt utarbetat utkast till vilka best practises som en Certification Authority ska använda. I vårt perspektiv finns det många saker att diskutera i det steget. Det dokumentet kommer också att förändras med tiden, men det är ett första steg internationellt sett på detta området.

- **Handlar det om ett 4–5-årigt perspektiv för ett allmänt införande i Sverige?**

På vissa områden och vissa tillämpningar kommer det säkert att gå fortare. Andra tillämpningar kommer att ta mycket längre tid. Vissa tillämpningar kommer aldrig att realiseras.

[6] ICC (International Chamber of Commerce) är en framträdande internationell frivillig sammanslutning av större företag som arbetar för att underlätta den globala handeln.

- **Så vi ska inte tro för mycket på att detta kan lösa alla problem?**

  Näringslivet och bankerna kommer att ha goda förutsättningar att kunna genomföra mycket inom området. Hindren finns på lagstiftningsområdet. Tekniskt finns lösningarna.

- **Behövs en starkare signal än den som regeringen redan har fått för att skynda på?**

  Frågan är kanske inte styrkan på signalen, utan om mottagaren förstår signalen.

- **Du är inte övertygad om att regeringen har förstått signalen ännu?**

  Jag är sedan tidigare starkt kritisk mot att t ex datastraffrättsutredningen från 1992 ännu inte har genomförts och att en ny utredning är tillsatt. Vi måste veta i vilken utsträckning som en manipulering av en digital representation är straffbart. Det är inte med säkerhet straffbart idag i alla situationer. Denna typ av frågor är viktiga, men jag har en känsla av att de nedprioriteras istället för att upprioriteras.

- **Är SEIS-ambitionen att sprida sitt upplägg i världen en realistisk ambition?**

  Det är säkert en realistisk ambition om andra länders medborgare eller näringslivsföreträdare finner att detta är någonting som de också kan ta. Då vill man gärna ta färdiga lösningar. Varför göra om arbetet?

  Men generellt är det svårt att uttala sig om möjligheterna. Vad som är gångbart i USA och England, är kanske inte alls gångbart i Frankrike och Italien. T ex i Italien vill man inte ens handla med vanliga kontokort utan där betalar man kontant – det finns där inga traditioner för kortaffärer.

- **Kan en samlad teknisk lösning uppbackad med ett regelverk få global räckvidd?**

  Ska detta fungera måste det bygga på att datorer kan kommunicera och att människor bakom datorer kan kommunicera. Det handlar mycket om etablerade standarder och öppna och verifierbara säkra lösningar. I den meningen tror jag på en sådan utveckling, under förutsättning att det inte finns mycket inslag av underrättelsetjänst och nationell säkerhet.

  Om man analyserar frågeställningen från underrättelsetjänst- och nationellt säkerhetsperspektiv är svaret givet. Det blir ett annat svar om säkerheten för individen är det primära före underrättelsetjänst och nationell säkerhet. Det är utgångspunkten för analysen som är avgörande.

  Ett typexempel på det är DGXIIIs senaste Communication, som är ett uttalat handelsvänligt och från den utgångspunkten mycket bra dokument. Inom EU har vi sett andra reaktioner tidigare och såväl EU-kommissionen som de flesta länderna är starkt kluvna i vilka anspråk som ska väga tyngst i detta avseendet.

- **Om näringslivets vinster och fördelar kan bli väldigt stora genom att införa system för identifiering och identitet i digitala miljöer, kan det innebära att många av de multinationella företagen inom ICC lägger ökande tryck mot sina hemländers regeringar för att bredda vägen? Kommer just de ekonomiska fördelarna i den pågående globaliseringen att ha en utslagsgivande betydelse för en relativt snabb utveckling bland de företag som vill ha det?**

Det är ingen tvekan på den punkten. Det tycker amerikanerna själva också. Ett amerikanskt undersökningsinstitut lade för något år sedan fram en stor rapport till senaten som konstaterade att *national security interests* kommer inte att klara att stå emot denna utveckling. Det förfarande som vi nu ser är egentligen den brända jordens taktik, att hålla uppe exportkontrollerna och exportreglerna när det gäller kryptering o s v så länge som möjligt.

Det är inte vinster som är det avgörande, utan mera mätt i termer av effektivitet och konkurrenskraft. Det handlar om att integrera leveranskedjor och att dela information för att eliminera mycket av det som tar tid idag. Anledningen till att ICC började med EDI redan på 1980-talet var att man konstaterade att godset kom fram före papperen när man fraktade över Atlanten. Det är mycket dyrt med en otillfredsställande pappershantering.

Utfrågning av Berne Landgren, Telia Megacom AB

Berne Landgren är VD för Telia Megacom AB, Stockholm.

- **Telia visar intresse för många nya tillämpningar där digital identifiering och signatur är en grundbult. Det förefaller som att Telia, precis som Posten, kommer att lansera något av detta under 1998. Hur snabbt är det möjligt att i stor omfattning föra in tekniken utifrån Telias perspektiv?**

Det beror på vad man menar med stor omfattning. För Telia är detta egentligen ett sätt att gradera upp telenätet. Idag måste du i vissa sammanhang träffa en person fysiskt för att vara säker på vem vederbörande är och för att genomföra vissa handlingar. Imorgon kan det ske över telenätet. Det är en hisnande möjlighet. Inte bara för Telia, utan för oss alla.

Därför är Telia inriktat på arbeta mycket med SEIS-standarden och det öppna förhållningssättet. Det är fundamentalt med tilliten och det kräver öppenhet. Det går att byta pusselbit efter pusselbit i systemet för att få det långsiktigt hållbart. Telia arbetar med många sådana tillämpningar idag med många olika intressenter.

Nordbanken är först ute med kortläsare och elektroniskt identitetskort i sin nya Internetbank. Det gör hanteringen mycket enklare än att, som många gör idag, använda säkerhetsdosa för att visa behörighet för att komma in i banksystemet. Med en sådan säkerhetsdosa är det tidsödande, besvärligt och arbetsamt för att uppnå en säkerhet.

Telia kommer också använda samma teknik i settopboxen för kabel-TV. Det är starten på en mycket stor framtidsutveckling där telenätet graderas upp för bredbandig kommunikation. Det kommer att flöda mycket mer värdefull information genom ledningarna och det innebär högre säkerhetsrisker. Därmed finns behovet av säker identifiering.

- **Därmed når Telia ut till hushållen[7] i mycket stor utsträckning. Kommer med andra ord SEIS-konceptet att finnas tillgängligt för huvuddelen av abonnenterna inom några år?**

Det hänger på den kommersiella fortsättningen. Tillämpningarna måste till. Innehållet måste till för att det ska finnas tillräckligt intresse. Det går inte att säga i förväg. Vi försöker vara konsekventa. I allt vi gör, bygger vi in denna säkerhetslösning. Vi bygger in det i bredbandsaccesserna. Vi bygger in det i våra interna system för att vi ska nå våra egna lokala nät inom Telia. Vi bygger in det i tillämpningarna till våra kunder.

Vi arbetar med många tillämpningar och projekt i bankbranschen, både mot bankernas kunder och internt inom bankvärlden. Andra områden är försäkringar, elektronisk handel, hotell och vi diskuterar med t ex Bilregistret så att det kommer att vara möjligt att säkert fjärrgenomföra bilbyte istället för med dagens omständliga procedur.

- **Vilka är de största hindren för att genomföra Telias planer?**

Det största hindret är hönan-och-ägget-problematiken. För att man ska bygga infrastruktur, krävs det nytta och tillämpningar. För att nytta och tillämpningar ska byggas, krävs infrastruktur. Telia försöker att bygga infrastruktur så mycket och så konsekvent som möjligt – i samtalsautomater, i PCar, i telefoner o s v.

[7] Telia Kabel-TV har 1,3 miljoner anslutna hushåll och några hundratusen med settopboxar.

- **I vilken utsträckning behövs ändrad lagstiftning?**

  Det ena hindret är hönan och ägget. Det vore mycket bra om Statskontoret tar initiativ till att handla upp tekniken. Det kommer att driva på utvecklingen.

  Det andra hindret är lagstiftningen. Tilliten och förtroendet kräver att det finns ett lagstöd och att det kommer snabbt.

- **Är det realistiskt att SEIS-konceptet kan rullas ut i resten av världen?**

  I resten av världen är säkert att ta i. Men vi har ett försprång på delar av detta. Vi har kunskap och vi har också en tradition av samverkan. Det som vi har gjort i Sverige är ganska unikt, genom att vi faktiskt samlar banker, operatörer, Posten och ett antal andra intressenter och samsas om en viss standard. Det ska vi ta vara på.

- **Är det realistiskt att SEIS-konceptet går att rulla ut i Europa?**

  Delvis i alla fall. I norra Europa har vi en bra chans. Vi arbetar ju över hela Norden och Östersjöområdet, vilket gör att med rimliga gemensamma ansträngningar borde vi kunna få finnar, norrmän och danskar med oss. Vi kommer ju att göra egna lösningar i det som vi håller på med runt Östersjön och Norden. Alliansen som Telia har tillsammans med holländare och schweizare och AT&T är ett annat sådant exempel, där vi kan arbeta från vårt håll. Men det krävs ju att det är många som är med och drar i denna utveckling.

- **Vilka ekonomiska möjligheter ligger i SEIS-konceptet? Är det främst ökad tjänsteförsäljning?**

  Det är egentligen ekonomiska möjligheter överallt – för oss alla. Det är oerhört många tillämpningar och på alla olika områden finns det möjligheter som öppnar sig genom SEIS-konceptet.

- **Istället för SEIS lösning skulle Telia väl kunna välja en egen teknisk lösning som presterar i stort sett samma sak – vilken är fördelen med att välja den gemensamma lösningen?**

  Därför att den är en öppen lösning. Det betyder att vi kan göra ett antal saker som också våra konkurrenter kan göra som stöder samma infrastruktur. Infrastrukturen kostar pengar att bygga. Ju fler som är med och betalar, desto bättre och snabbare går det.

Utfrågning av Jerker Sjögren, Stockholms stad

Jerker Sjögren är projektledare för Medborgarinformationsprojektet i Stockholms stad.

- **Stockholms stad är en av de kommuner som satsar kraftigt på ny IT. Varför är det intressant att införa system för identifiering och identitet i Stockholm?**

Det är intressant utifrån både de interna och externa behoven. Det finns 12 000 persondatorer idag i Stockholms stad som används från morgon till kväll. För att de ska kunnas användas ännu mer effektivt behövs denna typ av lösning kopplat till satsning på intranät o s v. Därtill kommer kontakten med medborgarna. Fullmäktige har beslutat om en plattform för kommunikation mellan staden och dess medborgare. Det är tre kanaler: telefoni, de fysiska medborgarkontoren som nu växer upp och Internet. För att det ska bli mer än bara enkla informationstjänster – det ska bli riktiga, interaktiva tjänster – måste man ha denna typ av säkerhetslösning.

Hur snabbt det kan ske beror helt på hur vi lyckas samla oss i Sverige och i vilken mån vi kan dra nytta av det som vi ser i andra länder. Men klart är att vi måste få till den typ av lösning som Toppledarforum har beskrivit. Vi behöver ha kortsiktiga lösningar snabbt. Vi kan inte lösa alla problem på en gång. För då kommer vi inte framåt.

Det är viktigt att se säkerhetslösningen som en del av den nya infrastrukturen som håller på att växa fram. Problemet är detta med hönan och ägget, att det är lätt att fastna i ett moment 22 – inget händer därför att man inte kommer i gång. Samhället har ett ansvar för att bygga infrastrukturer. Om man får ett bra samspel mellan samhället och marknaden, i form av både leverantörer och användare både på den privata och offentliga sidan, kan det börja hända saker redan under nästa år.

- **Vilka är de största hindren?**

Till de största hindren hör framför allt bristen på relevant lagstiftning. Oklarheterna skapar en osäkerhet på den privata sidan där man inte vill ta affärsrisker. På den offentliga sidan finns en osäkerhet i form av att man inte vill riskera att "trampa ut i det moras[8]" som regelverket eller trakterna utanför regelverket innebär. Alla kommuner är ju inte lika uppkäftiga som Gällivare.

- **Har Stockholms stad studerat internationella alternativ till SEIS? Eller nöjer ni er med signalerna från Toppledarforum och SEIS?**

Jag har haft förmånen att via SEIS träffa eldsjälar, företrädare för motsvarande organ i Holland, Finland och några andra länder. Samstämmigheten är stor om att det är bråttom och att man ska se till att dra nytta av varandras erfarenheter i arbetet.

I den finska handlingsplanen finns klart och tydligt utskrivet att man ska dra nytta av SEIS-specifikationen. De har lusläst specifikationerna och kommit med konkreta synpunkter på sådant som behöver förändras. Samarbete är den rätta vägen att gå. Det handlar alltså inte om att sälja detta till andra länder eller "invadera världen" med hjälp av SEIS. Det handlar om samspel och samarbete

[8] Moras = träskartat område, kärr.

- **Gör samarbete kring SEIS-plattformen att den sprids i förbättrad form till andra länder?**

  Ja. I olika grupperingar har vi som nämnts kontakter med Finland, Holland m fl. Så med samarbete i Norden och norra Europa, kanske det går att få med Kanada för att sedan rulla upp USA bakvägen.

- **Vilka vinster – utöver förbättrad kommunikation till invånarna – går det att göra med en bra säkerhetslösning?**

  Man måste se på detta som en investering i infrastruktur. Som med alla sådana investeringar gäller att vinsterna inte kommer omedelbart. Dessutom dyker de ofta upp någon annanstans än hos den som gör investeringen. Men säkerhet måste vi ha. Utan säkerhet kommer vi inte vidare med tillämpningsutveckling, d v s verksamhetsutveckling i praktiken. Vi kan heller inte få genombrott för t ex självbetjäning i stora delar av den offentliga servicen med hjälp av informationskiosker ute på gator och torg. Det är alltså nödvändigt att skaffa denna typ av lösning.

  Vinsterna kommer är jag övertygad om, bl a i form av kortare handläggningstider. Många tjänstemän hos kommuner och statliga myndigheter (som idag går på knäna och får Yrkesinspektionen att rycka ut) får möjlighet att ägna sig åt mer kvalificerade arbetsuppgifter, om det går att få undan en del av ärendehanteringen genom att jag som medborgare exempelvis levererar in halvfabrikat i form av deklarationer och annat.

Utfrågning av Magnus Faxén, UD

Ambassadör Magnus Faxén, UD, är regeringens utredare av en svensk krypteringspolicy.

- **Grytan kokar på många ställen internationellt kring dessa frågor. Hur snabbt är det realistiskt att tekniken kan slå igenom i de avancerade industriländerna? Är det ett perspektiv på 4–5 år eller kanske tio år?**

Det lätta svaret är att det är omöjligt att svara på. Den riktiga svaret är att olika frågor kommer att ta olika lång tid. Ett område där det finns chans att kunna finna gångbara lösningar internationellt är att skapa förutsättningar för elektronisk handel, d v s att börja med de digitala signaturerna. Det är visserligen inte helt enkelt, men ändå det enklaste i hela komplexet.

En fråga är om man kan skilja på hanteringen av digitala signaturer och kryptering i vidare bemärkelse, d v s hemlighållandet av innehållet i meddelandena. Svaret är ja. För ett par år sedan fanns i många länder en väldigt rigid inställning kring kryptering eftersom underrättelseorganen då var mycket dominanta. Nu har stämningarna svängt. Nu är det möjligt att klart skilja på hanteringen av kryptering och de digitala signaturerna. I Tyskland finns redan en lagstiftning om digitala signaturer. Nu kan de börja utveckla tillämpningarna. Men när det gäller krypteringsdelen råder oenighet i Tyskland och den frågan kommer inte att hanteras förrän efter 1998 års val.

- **Kan det bli en snabb utveckling på området?**

Utvecklingen kommer att gå stegvis. Vad vi än gör i Sverige när det gäller digitala signaturer, måste vi se till att vi gör det i takt med utvecklingen hos våra viktigaste handelsparter, t ex Tyskland. Därför måste vi noga studerar hur den tyska lagen kommer att verka.

En del säger att den tyska lagen inte är smidig och bra, att den har brister o s v. Men det är den som finns och den som tyskarna kommer att följa. Ska tyskarna godta våra certifierade digitala signaturer, måste Sverige ha en lagstiftning som är någorlunda samstämmig med den tyska.

- **Innebär det att eftersom tyskarna redan har en lag, kan den svenska lagen komma fram snabbt?**

Det vet jag inte. Men detta är av det viktigaste som regeringen måste ta itu med omedelbart. Justitiedepartementet, Näringsdepartementet och andra funderar över detta och det ska så snabbt som möjligt komma i gång ett samordningsarbete inom regeringskansliet eftersom det berör flera departement.

Det är oerhört bråttom att få i gång arbetet med att ta fram en lagstiftning för digitala signaturer, så att de får en verkan och kan användas praktiskt.

- **Vem som har den starkaste positionen – är det polisen och rättsväsendet eller är det näringslivet och affärsintressena? Har affärsfolket har tagit hem spelet nu?**

Den slutsatsen är något förhastad. Det inte är frågan om vem som är starkast, utan att man tar hänsyn och försöker finna en balanserad lösning. Det låter enkelt. Alla länder talar också om att så ska man göra. Det är nödvändigt att försöka balansera intressena. Det är givet att det är ett allmänintresse, även ett statens intresse, att se till att näringslivet har tillgång till den bästa tänkbara tekniken. Att man har ett bästa tänkbara skydd är i allas intresse. Men det är också naturligtvis ett intresse hos individer och näringsliv att inte denna underbara teknik tas om hand av gangsters, maffiosos och terrorister. Det är ett faktum att det finns allvarliga hot och stora risker i användningen av dessa system.

Ett exempel är Japan där lagstiftningen skyddar individernas rätt på ett avancerat sätt. Den påtvingades Japan av amerikanerna efter nederlaget i andra världskriget. Det ironiska är att amerikanarna nu driver på att även Japan borde ta i med hårdhandskarna för att skydda sig mot terrorister. Opinionen har svängt efter terrordådet i Tokyos tunnelbana, när man upptäckte att planeringen av dådet hade skett med hjälp av kryptering. Så kan det gå.

Från svensk sida finns ett krav på – precis som rättsväsendet redan har via bokföringslag, skattelagar o s v – viss insyn i affärer. Det måste rimligen ordnas så att det passar in i användningen i ny teknik. Vissa hänsyn måste tas. Hur det ska gå till är en annan fråga.

- **I Sverige anser vi oss vara tidigt ute i utvecklingen på detta område – har vi möjlighet att göra oss gällande internationellt?**

Jag är övertygad om det. Det finns redan ett väl etablerat samarbete med vissa länder. Sverige har ett högt anseende på flera sätt, t ex när det gäller den tekniska nivån och samhälleliga strukturer som fungerar väl. Det har bl a lett till att vi har bjudits in i arbetsgrupper inom EU. Vi har också blivit indragna i diskussionsarbete om teknikens interoperabilitet och om exportkontrollen. De åtta länder som är med i dessa resonemang är fem EU-länder, Förenta staterna, Kanada och Japan. Det är alltså frågan om att försöka finna enighet och gemensamma uppfattningar som utgångspunkt för lösningar.

- **De tunga spelarna kommer överens om någonting som sedan kan slå igenom i resten av världen?**

Ja. Och Sverige är med f n. Respekten är stor bl a för den teknik som Sverige har presterat.

- **När det gäller krypteringssidan i stort – blir det någon obligatorisk deposition av nycklar?**

Det är inte aktuellt när man hanterar digitala signaturer. Men när det gäller frågan om krypterade meddelanden och möjligheterna för rättsvårdande myndigheter att komma åt vad misstänkta brottslingar har haft för sig, föreslår vi att det inte ska finnas krav på en obligatorisk deposition av nycklar i Sverige. Men som det ser ut idag i vissa länder som vi har trafik med, kan andra länder komma att ställa krav på att internationell trafik ska kunna genomföras först när man har deponerat nycklar.

Den amerikanska administrationen driver hårt linjen att amerikanska företag som vill sälja maskin- eller programvara med krypto till Sverige, beviljas inte detta om inte mottagaren först har ordnat med nyckeldeposition. Eftersom vi inte har någon nyckeldeposition i Sverige, innebär det att man blir tvungen att lägga nycklarna i USA. Det är läget. Om det blir en förlängning efter 1998 återstår att se. I Frankrike är det lag på att om man ska kommunicera digitalt ska man ha nyckel deponerad hos en fransk nyckeldepositör.

Strategisk diskussion: Vem gör vad, när och hur?

Inledning

Detta avsnitt belyser vad som behöver göras för att i Sverige införa system för digital identifiering och digital signatur.

Medverkande

Thomas Falk (Industriförbundet), Ulf Jonströmer (AU-System AB) och Peter Seipel, (Stockholms universitet). Ordförande: Gunnar Hedborg (IT-kommissionen).

- **Att införa system för digital identifiering och identitet förefaller vara en komplex uppgift. För att nu komma framåt är frågan – vad ska göras och vem ska göra det?**

Thomas Falk, Industriförbundet: Ska någon göra något? Detta kommer att ta tid. Ett femårigt perspektiv är rimligt. Vi debatterade inte ens denna fråga för tre år sedan. Internet som kommersiell företeelse begränsar sig till i stort sett de senaste två åren och har utvecklats utan påhejningar av vare sig lagstiftare eller andra. Det har skett organiskt. Därmed inte sagt att det inte finns problem i användningen av Internet framöver. Det gäller framför allt problem som rör affärskultur – att vi kan lita på varandra helt enkelt, känna tillit.

När det allmänt gäller utvecklingen av affärskulturen sätter naturligtvis lagstiftningen vissa gränser. Ofta har lagstiftningen kommit till i vissa lägen för att justera skevheter o s v. Men trots allt förutsätter en tillitspräglad affärskultur att det är parterna på marknaden som på olika sätt är överens.

Det är alltså parterna som vill använda denna teknik på marknaden som måste driva frågan. Jag tror inte att vi *snackar upp ett tält* genom att i förväg säkerställa en lagstiftning eller liknande för att skapa en ansad gräsplan där vi sedan kan börja spela fotboll eller krocket. Är det inte så att vi ofta börjar spela även om planen inte är så jämn från början? Efterhand kan det finnas skäl oss att hyfsa ekvationen.

Ulf Jonströmer, AU-System AB: Min syn är densamma. Är detta så märkvärdigt? För ett trettiotal år sedan införde banker, Posten och några till ett gemensamt identitetskort. Inte talade man då om behovet av ny lagstiftning. De kom överens och genomförde det.

Idag diskuterar vi hur många nivåer av certifiering mellan Certification Authorities som vi behöver för att verkligen lita på de nya identitetskorten o s v. Men vi har redan identitetskort där ingen garanterar någonting. Vi litar på det i alla fall.

Vi ska inte göra detta så väldigt komplicerat! Vi borde försöka finna praktiska lösningar på ett akut och aktuellt problem, nämligen identifiering och bekräftelse i en elektronisk värld.

Visst kan vi använda samma teknik för att bygga upp ett nytt elektroniskt samhälle. Där kommer vi säkert att behöva en ny lagstiftning, m m. Men det är i ett längre perspektiv – om 4–5 år och längre fram. I dagens läge är vi många som behöver lösningar för behovet av identifiering och bekräftelse. Väljer vi inte lösningarna med smarta kort och SEIS, är vi hänvisade till våra säkerhetsdosor eller andra än värre lösningar.

Det finns idag en överenskommelse, en teknik och ett regelverk som tillräckligt väl reglerar detta för att det ska vara möjligt att få i gång en lösning för en bank. Nordbanken riskerar inte sitt namn på en säkerhetslösning som inte fungerar.

Vi bör idag vara mycket pragmatiska. Vi ska se vad som går att göra på kort sikt. Parallellt med det kan vi diskutera om vad som ska hända om 4–5 år. Då kanske det behövs annat i form av regelverk, lagstiftning o s v.

Peter Seipel, Stockholms universitet: Min syn är en variation på samma tema. Det finns ur lagstiftningssynvinkel såväl hårda som mjuka frågor av olika svårighetsgrad:

	Hård fråga		
Lätt att lösa	Exempel: digital signatur		
		Exempel: tillit	Svår att lösa
		Mjuk fråga	

En hård och enkel fråga är rimligtvis den digitala signaturen. Om det underlättar skeendet och utvecklingen borde det vara möjligt att snabbt göra en reglering.

Bland frågor som är mjuka och svåra finns t ex allmänhetens tilltro och tillit o s v som är väsentliga komponenter på detta område. Där är det oerhört mycket svårare att se vad man kan göra nu och här och vem som är ansvarig. Dessa frågor kan vi försiktigt skjuta in i framtiden.

Allmänt sett måste fantasin få spela mera för att hitta lösningar. Ta t ex problemet med deponering av nycklar – varför inte tänka i termer av tidlås? Om det är så att information är känslig endast under kort tid går det att sätta tidlås på den, så att det inte är möjligt att öppna förrän om ett eller två år när domstolen behöver det.

Eller sätt elektroniska bojor, så att de som tidigare har betett sig illa måste tyvärr deponera nycklar. Medan alla andra är värda förtroendet att använda fullt krypteringsskydd. Det kan vara antingen ett förtroende som man förvärvar eller som man har från början. Mer fantasi i de tekniskt organisatoriskt juridiska lösningarna!

Ulf Jonströmer, AU-System AB: Jag har full respekt för de juridiska frågorna, men i det korta perspektivet är allmänheten mer betjänt av en diskussion om skillnaden mellan ett smart kort (med nycklar och identitet) och det som ligger på en hårddisk. Det borde vi förklara på ett vettigt sätt. Då går det att skapa mycket större tillit till de lösningar som finns, än om vi har tjusiga regler för certifiering m m.

- **Det vi diskuterar om att införa för digitala miljöer är egentligen en oändligt mycket högre säkerhetsnivå än i befintliga system. En namnteckning är ganska enkel att förfalska o s v. Överdriver vi kraven på säkerhet?**

Thomas Falk, Industriförbundet: Vi överdriver inte säkerhetstänkandet för affärstransaktioner i generell mening. Men redan idag är det en mycket osäkrare hantering att lämna ifrån sig ett vanligt kreditkort på en restaurang än att använda ett smartkort-system. Men affärsidkare som bryter mot affärskulturen och missbrukar förtroendet med kort, kan bara göra det en gång. I den elektroniska världen är det lättare att gömma sig. Men det är förhållandevis ett litet problem att lösa hur vi ska kunna bedriva handel på nätet som når slutkonsumenten.

Den stora frågan är den civilrättsliga delen som gäller utbytande av affärsdokument i generell mening: offerter, kontrakt och annat där en namnteckning idag gäller juridiskt. Detta handlar om elektronisk affärskommunikation som inkluderar allt, alltså inte enbart kommers eller handel som resonemangen vanligtvis fokuserar på.

Ulf Jonströmer, AU-System AB: Det finns idag lösningar som tycks räcka för att klara av mina transaktioner med S-E-Banken (med en säkerhetsdosa) och då kan man undra: Behöver jag någonting mer? Ja, det behövs något mer. I det större perspektivet med elektronisk handel, vill jag kunna använda samma PC för många olika tjänster. Det är praktiskt omöjligt att ha 15 olika säkerhetsdosor.

Framgent vill vi alltså kunna använda samma grundteknik mot många olika system. Då är kraven som ställs av SEIS helt naturliga och nödvändiga.

Dessutom är vissa typer av tillämpningar överhuvudtaget inte möjliga om vi inte höjer nivån. Riksskatteverket testar möjligheten att göra deklarationer via Internet. Där behövs en säkrare identifiering än ett vanligt engångslösenord.

Peter Seipel, Stockholms universitet: Det kommer att behövas viss lagstiftning i efterhand. När det gäller de hårda enkla frågorna (se matrisen tidigare) är det onödigt att ha osäkerhet som består i att man inte har satt namn på saker och ting juridiskt. Just de enkla operationerna bör man i största möjliga utsträckning genomföra, så att man vet vad man umgås med och vet vilka helt konventionella rättsliga konsekvenser det ena och det andra tillvägagångssättet har. Sedan blir det naturligtvis större allvar av detta när det leder över i straffrättsliga resonemang, om att människor ska eller inte ska hållas ansvariga för det ena eller andra tillvägagångssättet.

Här borde lagstiftningsarbetet accelerera – jag kan inte se det på annat sätt. I stor utsträckning kommer det att handla om konsumentfrågor. Industrin ger sitt perspektiv, men jag ser det också ur ett mer vardagligt enkelt konsumentperspektiv. Rätten är inte bara maktens redskap, utan också vanmaktens stöd.

Thomas Falk, Industriförbundet: Handeln på nätet mellan företag idag är nog betydligt större än den mellan företag och slutkonsument. Det bekymmersamma är att vi behöver komma överens om var svensk immaterialrätt slutar och var tysk och fransk börjar. Hur fungerar internationella kontrakt, etc?

Det är viktigt att börja klassificera affärshändelser. Vi får nya typer av affärslösningar som vi tidigare inte har haft. Då är det viktigt att vara överens om innebörden av dem. Om det sedan nödvändigtvis i alla lägen måste följas av lagstiftning är något som går att diskutera – men vi ska veta vad vi talar om.

Exempel: Om jag gör en elektronisk överföring av pengar idag digitalt till min dotter i London kan jag faktiskt med denna teknik ordna det så att hon inte kan brukar pengarna var som helst, t ex på puben. Det är två operaföretag i London plus fyra av mig förutbestämda bokhandlare som gäller, that is it. Så kommer vi att ha det. Vi kan alltså tänka oss en värld som är ofantligt mycket mer säker för konsumenten. Nu unnar jag min dotter att gå på puben och lägger mig egentligen inte i hur hon använder sina pengar.

Om vi leker med tanken, inser vi att vi är på väg in i en ny struktur och att vi måste ha mycket mer fantasi för att förstå hur de olika affärslösningarna kommer att se ut. Därför måste vi börja försöka beskriva de olika affärshändelserna – en taxonomi helt enkelt.

Ulf Jonströmer, AU-System AB: Industrin välkomnar i hög grad den dag som vi har en lagstiftning om digitala signaturer, etc. Men de användare som vi ser nu, och de företag och banker som satsar på detta, klarar sig under en relativt lång tid framöver på avtal.

De inom statsförvaltningen som blir försedda med elektroniska tjänstekort, kommer inte att ha svårt att skriva på ett avtal med S-E-Banken, Handelsbanken eller Nordbanken om att det kortet också går att använda i banken. Rimligtvis behövs ingen särskild juridik för det.

I Nordbankens planer är det självklart att genom att vara tidigt ute kan man vinna affärsfördelar, genom att kunna erbjuda sitt kort till ett antal andra köpställen som gör att kunden kommer att uppleva det mer värdefullt att ha Nordbankens lösning för identifiering och säkerhet, än säg en säkerhetsdosa från S-E-Banken.

- **Det framskymtar en bristande kunskap och insikt om denna utveckling hos politikerna. Är det så?**

Ulf Jonströmer, AU-System AB: Bristen på insikt finns inte bara hos politiker. Detta är ett komplext område och det är inte lätt att skilja agnar från vetet. Vi för själva en lite förvirrad debatt om dagens problem och morgondagens jättelösningar och därför förstår jag om politiker har svårt att fatta beslut i dessa frågor.

Vi i branschen och andra intressenter måste via SEIS eller på annat sätt vara mycket mer konkreta om vad vi förväntar oss av politikerna. Det finns en klar öppenhet i dagens läge att gäller att få råd och dåd i hur man ska agera i bl a dessa frågor.

Peter Seipel, Stockholms universitet: Politik är svårt. Den erfarne lagstiftaren Karl-Axel Petri har sagt att det i lagstiftningssammanhang finns en mystisk faktor som heter "Tiden är mogen" eller "Tiden är inte mogen". Det är svårt att förklara när den faktorn slår till i ena eller andra riktningen.

Men det ligger mycket i att det måste bli politik av det för att det ska tända. Frågan är om identifiering och identitet i digitala miljöer uppfattas på det viset eller som andra- eller tredjerangsfrågor. Detta är inte rationellt till fullo. Persondatafrågorna t ex är politik, de är synliga och de får medieuppmärksamhet.

Detta med kryptering och digitala signaturer fanns redan på 1970-talet och tidigare. Då fanns koncepten, tekniskt och juridiskt. Men det var ett fullkomligt ickeproblem på den tiden och har varit länge. Det är en irrationell och mystisk faktor.

I IT-kommissionen är vi fullt medvetna och fokuserade på dessa problem. Vi kommer i vår slutrapportering att uppmärksamma dem bland de viktiga och angelägna bevakningsområdena.

Thomas Falk, Industriförbundet: I juli 1997 var det i Bonn en s k ministerkonferens som rörde olika inslag av IT-samhället. Framför rörde en stor del av diskussionen Internet, elektronisk handel och därmed sammanhängande frågor. Det var första gången som en grupp ministrar dryftade frågorna och också kom med ett gemensamt uttalande. Det är ett gott tecken.

En sådan konferens – på tal om att tiden är mogen – var sannolikt omöjlig bara för två år sedan. Det sker en uppföljning i Åbo och en ny ministerkonferens kommer i Kanada under 1998.

Detta är otroligt viktigt, därför att en stor del av det vi talar om, har en politisk dimension och ska ha en politisk dimension.

Men det som jag har upplevt under långa tider är ju att politiker har haft ett ganska begränsat intresse för att diskutera dessa frågor. Nu börjar de uppmärksammas på allvar och det är viktigt.

Bilaga

Information om SEIS

Secured Electronic Information in Society, SEIS, är en ideell svensk förening med ett femtiotal förvaltningar och företag som medlemmar. Föreningens syfte är att höja IT-säkerheten främst för nätanvändare som fokuserar på säker kommunikation, säkert distansarbete i nätverk och säker elektronisk handel.

SEIS-föreningens uppfattning är att målet nås genom att införa en normerad infrastruktur för elektronisk identifiering, digitala signaturer och utväxling av nycklar vid kryptering. Föreningen anser att målet nås mest effektivt om dessa funktioner realiseras på ett smartkort, vars yta också bör utformas som ett konventionellt identitetskort.

Grunden för konceptet är internationellt och en vidareutveckling av material som kommer bl a från USA och Tyskland. Före bildningen av SEIS i mars 1995 arbetade projektet "Allterminalen" och projektet "Strategisk Samverkan" med liknande koncept. Nu förvaltar SEIS resultaten från dessa projekt.

Flera medlemsorganisationerna har betydande framgångar tack vare de normer som SEIS har utarbetat. Några aktuella exempel är att

- framgångsrika installationer och tillämpningar har i Sverige gjorts genom "Allterminalen" på Danderyds Sjukhus, Riksskatteverket med flera organisationer
- Posten ger ut identitetskort av typ smartkort som har fått internationell acceptans, först bland de nordiska postverken och sedan globalt och det innebär att "det svenska konceptet" ligger till grund för ett internationellt genomförande
- Finansinspektionen har tagit fram en "Java-baserad" systemlösning för den mycket konfidentiella och obligatoriska rapportering som de finansiella institutionerna är skyldiga att göra
- den offentliga förvaltningen har genom Toppledarforum tagit ett strategiskt beslut att
  a) säkerhetslösningen för den offentliga elektroniska handeln ska följa SEIS-normer
  b) införa ett anställnings-/tjänstekort i den offentliga förvaltningen baserat på SEIS.
- Nordbanken baserar sina tjänster via Internet på SEIS-normer
- Bankgirocentralen, Handelsbanken och S-E-Banken driver ett gemensamt projekt för att införa digitala signaturer på betalningsuppdrag till Bankgirot (pilotdrift 1998)
- finska Finansdepartementet har beslutat att införa frivilliga medborgarkort på basis av SEIS-normerna
- SEIS på Statskontorets initiativ inlett samarbete med den ideella föreningen National Chipcard Platform i Holland och därför ingår även finska och holländska specialister numera i SEIS arbetsgrupper
- svenska företag har internationella framgångar med produkter som är baserade på SEIS-normer, t ex AU-System i Australien, Malaysia och Singapore samt Dynamic Software i USA.

Rapporter

IT-kommissionens arbetsprogram, SOU 1995:68
Delbetänkande om kommissionens övervägande och prioriteringar samt arbetsprogram. 34 sidor. Kan beställas hos Fritzes kundtjänst. Fax: 08-690 91 91. Telefon: 08-690 91 90

Kommunikation utan gränser - rapport från IT-kommissionen, juni 1995
Skriften är ett sammandrag av kommissionens arbetsprogram. 15 sidor. Kan beställas hos IT-kommissionen, 08-405 18 51.

Communication Without Frontiers - report by the Swedish IT-Commission, june 1995
Engelsk översättning av sammandraget. 15 sidor. Kan beställas hos IT-kommissionen, 08-405 18 51.

Så kan Sverige utveckla en framgångsrik programvaruindustri inför 2000-talet
Rapport 1/96. 25 sidor. Kan beställas hos IT-kommissionen, 08-405 18 51.

IT-mått. Hur kan IT-användning beskrivas?
Av Nils-Göran Olve & Carl-Johan Westin, CEPRO AB.
Rapport 2/96. 65sidor. Kan beställas hos IT-kommissionen, 08-405 18 51

När det regnar manna från himlen, har den fattige ingen sked Om IT och handikapp.
Rapport 3/96. 32 sidor. Kan beställas hos IT-kommissionen, 08-405 18 51.

Kvinnor och IT
Rapport 4/96. 41 sidor. Kan beställas hos IT-kommissionen, 08-405 18 51.

Rättsinformation och IT - Svårigheternas advokater eller möjligheternas ambassadörer?
Rapport 5/96. 60 sidor. Kan beställas hos IT-kommissionen, 08-405 18 51.

ERROR, När IT inte fungerar - en rapport om IT och dess användbarhet
Av Per Gustafsson på uppdrag av IT-kommissionen.
Rapport 6/96. 50 sidor. Kan beställas hos IT-kommissionen, 08-405 18 51.

IT-kommissionens hearing om infrastrukturen för information och kommunikation.
Dokumentation från IT-kommissionens hearing den 5-6 juni 1996.
Rapport 7/96. 127 sidor. Kan beställas hos IT-kommissionen, 08-405 18 51.

Affärsnyttan med Internet
Sammanfattning av det seminarium som anordnades av IT-kommissionen, Swebizz och Sveriges Tekniska Attachéer den 4 juni 1996. Rapport 8/96. Rapporten är publicerad på IT-kommissionens hemsida <http://www.itkommissionen.se>.

IT-problem inför 2000-skiftet, SOU 1997:12
Referat och slutsatser från en hearing anordnad av IT-kommissionen den 18 december 1996. Rapport 1/97. Kan beställas hos Fritzes kundtjänst. Fax: 08-690 91 91. Telefon: 08-690 91 90.

Digital demokra@ti, SOU 1997:23
Ett seminarium om Teknik, demokrati och delaktighet den 8 november 1996 anordnat av Folkomröstningsutredningen, IT-kommissionen och Kommunikationsforskningsberedningen.Rapport 2/97. Kan beställas hos Fritzes kundtjänst. Fax: 08-690 91 91. Telefon: 08-690 91 90.

Kristallkulan - 13 röster om framtiden, SOU 1997:31
Rapport 3/97. Kan beställas hos Fritzes kundtjänst. Fax: 08-690 91 91. Telefon: 08-690 91 90.

IT och miljön - en samling goda exempel, SOU 1996: 178
Rapport 4/97. Kan beställas hos Fritzes kundtjänst. Fax: 08-690 91 91. Telefon: 08-690 91 90.

Sverige inför epokskiftet, SOU 1997:63
Rapport 5/97. Kan beställas hos Fritzes kundtjänst. Fax: 08-690 91 91. Telefon: 08-690 91 90.

Sweden in the Information Society, SOU 1997:67
The Swedish IT Commission report 5/97. Kan beställas hos Fritzes kundtjänst. Fax: 08-690 91 91. Telefon: 08-690 91 90

Säker elektronisk kommunikation, SOU 1997:73
Referat från ett seminarium anordnat av IT-kommissionen, Närings- och handelsdepartementet och SEIS den 11 december 1996. Rapport 6/97. Kan beställas hos Fritzes kundtjänst. Fax: 08-690 91 91. Telefon: 08-690 91 90.

IT-kommissionens hearing om den nya medie- och programvaruindustrin, SOU 1997:124
Andrakammarsalen, Riksdagen. Rapport 7/97. Kan beställas hos Fritzes kundtjänst. Fax: 08-690 91 91. Telefon: 08-690 91 90.

IT ocg regional utveckling - 120 exempel från Sverige, SOU 1998:19
Rapport 1/98. Kan beställas hos Fritzes kundtjänst. Fax: 08-690 91 91. Telefon: 08-690 91 90.

IT-kommissionens hearing om infrastrukturen för digitala medier, SOU 1998:20
Referat från en hearing anordnad av IT-kommissionen den 24 oktober 1997. Rapport 2/98. Kan beställas hos Fritzes kundtjänst. Fax: 08-690 91 91. Telefon: 08-690 91 90.

Problem med inbäddade system inför 2000-skiftet, SOU 1998:21
Hearing anordnad av IT-kommissionen i samverkan med Industriförbundet och Statskontoret 1997-11-14. Rapport 3/98. Kan beställas hos Fritzes kundtjänst. Fax: 08-690 91 91. Telefon: 08-690 91 90.

Identifiering och identitet i digitala miljöer, SOU 1998:36
Referat från en hearing den 12 november 1997. Rapport 4/98. Kan beställas hos Fritzes kundtjänst. Fax: 08-690 91 91. Telefon: 08-690 91 90.

Rapporter utgivna på uppdrag eller i samarbete med IT-kommissionen

Data om IT i Sverige
Statitsitisk sammanställning om IT gjord av Statistiska Centralbyrån på uppdrag av IT-kommissionen. Kan beställas från SCB Förlag, 701 89 Örebro. Fax: 019-17 69 32. Telefon: 019-17 68 00.

Datorvanor 1995
Undersökning av svenska folkets datorvanor utförd av Statistiska Centralbyrån på uppdrag av IT-kommissionen. 102 sidor. Kan beställas från SCB Förlag, 701 89 Örebro. Fax: 019-17 69 32. Telefon: 019-17 68 00.

IT världen runt - Nationella initiativ
Undersökning av Sveriges Tekniska Attachéer på uppdrag av IT-kommissionen och Näringsdepartementet. Kan beställas från STATT, Box 5282, 102 46 Stockholm

IT världen runt - Regionala initiativ
Undersökning av Sveriges Tekniska Attachéer på uppdrag av IT-kommissionen och Näringsdepartementet. Stencil.

IT världen runt - Statligt stöd till mjukvaruindustrin
Undersökning av Sveriges Tekniska Attachéer på uppdrag av IT-kommissionen och Näringsdepartementet. Stencil.

Europeiska Unionen - IT, telekommunikation och nya medier
En kartläggning och analys gjord av Statskontoret på uppdrag av IT-kommissionen. 111 sidor.

Statens offentliga utredningar 1998

Kronologisk förteckning

1. Omstruktureringar och beskattning. Fi.
2. Tänder hela livet
   – nytt ersättningssystem för vuxentandvård. S.
3. Välfärdens genusansikte. A.
4. Män passar alltid? Nivå- och organisationsspecifika processer med exempel från handeln. A.
5. Vårt liv som kön. Kärlek, ekonomiska resurser och maktdiskurser. A.
6. Ty makten är din ... Myten om det rationella arbetslivet och det jämställda Sverige. A.
7. Översyn av rörelse- och tillsynsregler för kollektiva försäkringar. Fi
8. Alkoholreklam. Marknadsföring av alkoholdrycker och Systembolagets produkturval. S.
9. Integritet – Effektivitet – Skattebrott. Fi.
10. Campus för konst. U.
11. Fristående utbildningar med statlig tillsyn inom olika områden. U.
12. Självdeklaration och kontrolluppgifter
    – förenklade förfaranden. Fi.
13. Säkrare kemikaliehantering. Fö
14. E-pengar – näringsrättsliga frågor. Fi.
15. Gröna nyckeltal – Indikatorer för ett ekologiskt hållbart samhälle. M.
16. När åsikter blir handling. En kunskapsöversikt om bemötande av personer med funktionshinder. S.
17. Samordning av digital marksänd TV. Ku.
18. En gräns – en myndighet? Fi.
19. IT och regional utveckling.
    120 exempel från Sveriges län. K.
20. IT-kommisionens hearing om infrastrukturen för digitala medier. Andrakammarsalen, Riksdagen 1997-10-24. K.
21. Problem med inbäddade system inför 2000-skiftet. Hearing anordnad av IT kommissionen i samverkan med Industriförbundet och Statskontoret 1997-11-14. K.
22. Försäkringsgaranti.
    Ett garantisystem för försäkringsersättningar. Fi.
23. Staten och exportfinansieringen. N.
24. Fiskeriadministrationen i ett EU-perspektiv. Översyn av fiskeriadministrationen m.m. Jo.
25. Tre städer. En storstadspolitik för hela landet. + 4 st bilagor. S.
26. Från hembränt till Mariakliniken.
    – fakta om ungdomar och svartsprit. S.
27. Nya ledningsregler för bankaktiebolag och försäkringsbolag. Fi.
28. Läkemedel i vård och handel. Om en säker, flexibel och samordnad läkemedelsförsörjning. S.
29. 1976 års lag om immunitet och privilegier i vissa fall – en översyn. UD.
30. Utlandsstyrkan. Fö.
31. Det gäller livet. Stöd och vård till barn och ungdomar med psykiska problem. S.
32. Rättssäkerhet, vårdbehov och samhällsskydd vid psykiatrisk tvångsvård. S.
33. Historia, ekonomi och forskning.
    Fem rapporter om idrott. In.
34. Företagare med restarbetsförmåga. S.
35. Förordningar till miljöbalken. + Bilagor. M.
36. Identifiering och identitet i digitala miljöer
    – Referat från en hearing den 12 november 1997. IT-kommissionens rapport 4/98. K.

Statens offentliga utredningar 1998

Systematisk förteckning

Utrikesdepartementet
1976 års lag om immunitet och privilegier i vissa fall
– en översyn. [29]

Försvarsdepartementet
Säkrare kemikaliehantering. [13]
Utlandsstyrkan. [30]

Socialdepartementet
Tänder hela livet
– nytt ersättningssystem för vuxentandvård. [2]
Alkoholreklam. Marknadsföring av alkoholdrycker och Systembolagets produkturval. [8]
När åsikter blir handling. En kunskapsöversikt om bemötande av personer med funktionshinder. [16]
Tre städer. En storstadspolitik för hela landet.
+ 4 st bilagor. [25]
Från hembränt till Mariakliniken.
– fakta om ungdomar och svartsprit. [26]
Läkemedel i vård och handel. Om en säker, flexibel och samordnad läkemedelsförsörjning. [28]
Det gäller livet. Stöd och vård till barn och ungdomar med psykiska problem. [31]
Rättssäkerhet, vårdbehov och samhällsskydd vid psykiatrisk tvångsvård. [32]
Företagare med restarbetsförmåga. [34]

Kommunikationsdepartementet
IT och regional utveckling.
120 exempel från Sveriges län. [19]
IT-kommisionens hearing om infrastrukturen för digitala medier. Andrakammarsalen, Riksdagen 1997-10-24. [20]
Problem med inbäddade system inför 2000-skiftet. Hearing anordnad av IT kommissionen i samverkan med Industriförbundet och Statskontoret 1997-11-14. [21]
Identifiering och identitet i digitala miljöer.
– Referat från en hearing den 12 november 1997.
IT-kommissionens rapport 4/98. [36]

Finansdepartementet
Omstruktureringar och beskattning. [1]
Översyn av rörelse- och tillsynsregler för kollektiva försäkringar. [7]
Integritet – Effektivitet – Skattebrott. [9]
Självdeklaration och kontrolluppgifter
– förenklade förfaranden. [12]
E-pengar – näringsrättsliga frågor. [14]
En gräns – en myndighet? [18]
Försäkringsgaranti.
Ett garantisystem för försäkringsersättningar. [22]

Nya ledningsregler för bankaktiebolag och försäkringsbolag. [27]

Utbildningsdepartementet
Campus för konst [10]
Fristående utbildningar med statlig tillsyn inom olika områden. [11]

Jordbruksdepartementet
Fiskeriadministrationen i ett EU-perspektiv. Översyn av fiskeriadministrationen m.m. [24]

Arbetsmarknadsdepartementet
Välfärdens genusansikte. [3]
Män passar alltid? Nivå- och organisationsspecifika processer med exempel från handeln. [4]
Vårt liv som kön. Kärlek, ekonomiska resurser och maktdiskurser. [5]
Ty makten är din ... Myten om det rationella arbetslivet och det jämställda Sverige. [6]

Kulturdepartementet
Samordning av digital marksänd TV. [17]

Närings- och handelsdepartementet
Staten och exportfinansieringen. [23]

Inrikesdepartementet
Historia, ekonomi och forskning.
Fem rapporter om idrott. In. [33]

Miljödepartementet
Gröna nyckeltal – Indikatorer för ett ekologiskt hållbart samhälle. [15]
Förordningar till miljöbalken. + Bilagor. [35]