Elektroniska signaturer
- säker identifiering?

Kandidatuppsats, 10 poäng, inom Informationssystem programmet
Institutionen för Programvaruteknik och Datavetenskap
Blekinge Tekniska Högskola
Maj 2001
Handledare: Guohua Bai
Författare: Ewonne Lennartsson
Ligia Correia Brandao

SAMMANFATTNING

Titel: Elektroniska signaturer – säker identifiering?

Författare: Ewonne Lennartsson
Ligia Correia Brandao

Handledare: Guohua Bai, Institutionen för Programvaruteknik och Datavetenskap

Problem: I dag finns det ett stort behov av säkra identifierings metoder på Internet. Traditionellt sätt är en handskriven namnteckning en form av identifiering och vad som behövs är en elektronisk motsvarighet.
Vi kommer i vår uppsats att undersöka en identifierings metod som kallas för elektroniska signaturer för att se ifall detta är en lösning till dagens identifieringsproblem.

Hypotes: ”Elektroniska signaturer leder till ökad integritet och säkerhet vid identifiering på Internet”

Syfte: Målet och syftet med denna uppsats är att studera och analysera huruvida elektroniska signaturer kommer att bidra till ökad integritet och säkerhet vid identifiering på Internet.

Metod: Primärdata har insamlats via intervjuer med relevanta personer inom ämnet. Sekundärdatan har samlats in via aktuell litteratur på ämnet, det vill säga genom böcker, tidningsartiklar och Internet.

Slutsats: Genom att jämföra praktiska erfarenheter (fallstudie) och teoretiska kriterier kunde vi analysera oss fram till att vår hypotes är sann.

Nyckelord: Elektroniska signaturer, digital identifiering, kryptering

ABSTRACT

Title: Electronic signatures – secure identification?

Authors: Ewonne Lennartsson
Ligia Correia Brandao

Tutor: Guohua Bai, The Dept. of Software Engineering & Computer Science

Problem: Today there is a great need form safe identification methods on the Internet. Traditionally a hand written signature is a form of identification and a digital counterpart is needed. With our thesis, we are going to investigate an identification method called electronic signatures, to se if this method can solve the identification problems today

Hypothesis: ”Electronic signature contributes to increased privacy and security while identifying oneself over the Internet”

Purpose: The purpose of this thesis is to, with the help of our goal driven questions, achieve our goal - proving our hypothesis.

Method: Data was gathered via interviews with relevant people within the subject and by other materials, such as books, articles and the Internet.

Conclusion: The goal and purpose of this thesis is to study and analyse if and in that case how electronic signatures will contribute to increased privacy and security while identifying oneself over the Internet.

Keywords: Electronic signatures, digital identification, cryptography

FÖRORD

Denna uppsatsen skulle inte vara möjlig att genomföra utan andras åsikter och kritik. Vår handledare Guohua Bai, vår seminariegrupp och de oss nära har gett oss detta.

Annie Stahel på Copenhagen Business School, har ställt upp som sakkunnig och hjälpt oss mycket, både praktiskt och teoretiskt.

Ett stort tack till Er alla.

Ligia och Ewonne

INNEHÅLLSFÖRTECKNING

1 INLEDNING

Tanken med detta inledande kapitel är att ge läsaren grundläggande förståelse kring det problemområde som skall undersökas, förklara uppsatsens mål och syfte samt påvisa vilka avgränsningar som gjorts.

1.1 BAKGRUND

I alla tider har det funnits ett behov att kunna styrka sin identitet, för att kunna vinna andra människors tilltro och tillit. Med nya teknologiska innoveringar förändras sättet vi kommunicerar och utbyter information på. Fram tills idag har avtal och transaktioner undertecknats med handskrivna namnteckningar. Denna signering har då identifierat parterna och verifierat transaktionens innehåll. Till fördel av den ”digitala revolutionen” har det tillkommit nya utmaningar för säkerheten, slutna kommunikationer och informationstransaktioner över öppna nätverket. Dessa utmaningar har lett till att säkerhetsmekanismerna av traditionella pappersbaserade kommunikationer blivit ersatta av bl.a. krypteringstekniker.

”*Osäkerheten av att man inte vet vem som finns i andra änden i en kommunikation som går över Internet, gör att Internetanvändaren inte upplever ett förtroende eller trygghet i sina elektroniska relationer.*”[1]

Vågar man lämna ut känslig information, t.ex. ett kreditkortsnummer? Elektronisk handel har hittills till stor del bedrivits i slutna grupper där parterna varit kända för varandra. I den kommande handeln över öppna nät, kommer parter i flertalet fall inte att vara kända för varandra. Kraven på säker identifiering av motparten liksom kraven på skydd mot insyn i meddelandena kommer därför att växa. Med hjälp av olika krypteringstekniker kan en säkrare elektronisk kommunikation uppnås. Man brukar skilja på kryptering som görs för att skydda innehållet i ett meddelande från insyn och kryptering som görs för att skapa en s.k. elektronisk signatur. Med en elektronisk signatur kan mottagaren dels konstatera om innehållet i ett meddelande förvanskats, dels knyta ett meddelande till en bestämd avsändare.[2]
Men för att denna elektroniska signering ska kunna användas krävs att den har samma juridiska status som den handskrivna motsvarigheten. Detta har möjliggjorts genom att från och med den 1 januari 2001 är elektroniska signaturer juridiskt bindande i Sverige.

1.2 HYPOTES

”Elektroniska signaturer leder till ökad integritet och säkerhet vid identifiering på Internet.”

Med denna hypotes som röd tråd i vårt arbete ska vi försöka visa hur elektroniska signaturer underlättar vid identifiering på Internet. Att kunna lita på att motparten är den han/hon utger sig för att vara är oerhört viktigt för fortsatt utveckling av elektroniska och mobila tjänster.
Elektroniska signaturer är en av lösningarna idag, men är det en säker metod och kommer den att fungera för gemene man?

Den lagliga statusen är mycket viktig för användandet av elektroniska signaturer, men minst lika viktigt är tilliten. Marknaden och användarna måste kunna och våga lita på den nya elektroniska teknologin.

1.2.1 Oberoende variabel

Den oberoende variabeln i hypotesen är den variabel som manipuleras för att komma fram till en slutsats efter teorier och fallstudier. Den oberoende variabeln i vår hypotes är *elektroniska signaturer*.

1.2.2 Beroende variabler

När den oberoende variabeln manipuleras är det variablerna *integritet och säkerhet* som påverkas, de är våra beroende variablerna.

1.3 MÅL OCH SYFTE

Målet och syftet med denna uppsats är att studera och analysera huruvida elektroniska signaturer kommer att bidra till ökad integritet och säkerhet vid identifiering på Internet.
För att nå målet, att se om vår hypotes stämmer, besvarar vi följande frågor:

1. Vad finns det för problem med att identifiera sig över öppna nätverk i dag?
2. Vad är elektroniska signaturer och hur fungerar de rent tekniskt?
3. Hur används elektroniska signaturer i praktiken?
4. Är elektroniska signaturer en bra lösning till dagens identifieringsproblem?

1.4 AVGRÄNSNINGAR

Vi kommer att studera och analysera om elektroniska signaturer är en bra lösning till de identifierings problem som finns på Internet idag. Vi kommer inte att utföra några jämförelser med andra metoder för att ta reda på huruvida elektroniska signaturer är den bästa lösningen eller inte. Detta eftersom vi varken har kunskaperna eller möjligheterna att utföra dessa jämförelser. Vi kommer däremot att göra en jämförelse mellan vad teorierna säger om elektroniska signaturer och hur de fungerar i praktiken.

Elektroniska signaturer kan skapas av symmetriska och asymmetriska krypteringsmetoder. Vi kommer endast att ta upp elektroniska signaturer som använder sig utav digitala signaturer, det vill säga asymmetrisk kryptering. Den tekniska delen är inte djupgående och vi går endast in på krypteringsmetoder och de olika tekniska lösningarna. Detta för att läsaren ska få en övergripande bild och förståelse av hur elektroniska signaturer och tillhörande tekniker fungerar.
Eftersom teorier rörande hur elektroniska signaturer fungerar i praktiken är begränsade kommer vår analys av empiriska data ske utifrån existerande teorier om identifiering, tillit/tilltro och datasäkerhet. Vår fallstudie utförs på Köpenhamns Handelshögskola.

1.5 MÅLGRUPP

Denna uppsats riktar sig till alla som är intresserade av datasäkerhet, men med vissa förkunskaper inom datavetenskap ser vi ökade möjligheterna att kunna tillgodogöra sig ett mervärde av uppsatsen.

1.6 DEFINITIONER

Nedan förklarar vi de olika begrepp som berör elektroniska signaturer, för att klargöra innebörden i de begrepp vi valt att använda genomgående i uppsatsen.
Man måste kunna lita på att ingen utnyttjar någon annans personliga uppgifter eller har ändrat de data som en part sänder till en annan, att datan är oförändrad. Dessa typer av integritet kallas för ***personlig och dataintegritet***.

Personlig integritet är när känslig information endast kan läsas av behöriga. Med dataintegritet menar vi att datan endast kan bli modifierad av auktoriserade användare. I detta sammanhang inkluderas även skriva, ändra, ändra status, radera och skapa i begreppet modifiera.[3]
En ***signatur*** är en egenhändigt skriven namnteckning, särskilt använd för att intyga tillförlitligheten eller äktheten av dokumentet. För att kunna säkra integriteten, datans såväl som den personliga, kan ***elektroniska signaturer*** användas. Dessa signaturer är data i elektronisk form som är fogade till eller logiskt knutna till en elektronisk handling och som används för att kontrollera om innehållet härrör från den som framstår som undertecknare. Den teknologi som används för gör detta möjligt är digitala signaturer. ***Digital signatur*** är beteckningen på den teknologin som används inom många olika områden allt ifrån elektroniska signaturer till metoder för nätverkssäkerhet. Begreppet innefattar även den teknik som innebär att man har två sammanhörande krypteringsnycklar som användas för identifikation, kryptering och signering.[4]
Grundstenarna i en elektronisk signatur är identifikation, signering och kryptering. Med hjälp av ***identifikation*** kan t.ex. säljande och köpande parter i en affärssituation, vara säkra på att de kan identifiera varandra. Köparen vill veta att han betalar till den riktige säljaren och inte till en bedragare. Säljaren vill på samma sätt känna sig säker på vem han gör affärer med. Köparen kan ju efter genomfört köp hävda att han varken har beställt eller tagit emot vara eller tjänst.
Signering är själva skapandet av en elektronisk signatur för att säkerställa att elektroniskt överförd information inte har förändrats. Slutligen ***kryptering*** som är kodning av information för att dölja dess verkliga mening för obehöriga. Där finns två typer av krypteringsmetoder, ***symmetrisk och asymmetrisk.*** Symmetrisk kryptering är då avsändare och mottagare har tillgång till samma nyckel för kryptering och dekryptering. Asymmetrisk kryptering betyder att en av krypteringsnycklarna är känd, medan den andra hålls privat, dvs. är okänd för andra än ägaren.
Som plattform till dessa grundstenar ligger ***PKI (Public Key Infrastructure)*** och kombinerat ger de oss t.ex. säker e-handel. PKI är ett ramverk bestående av flera produkter som används för två huvuduppgifter: Den ena är verifiering av användare och den andra krypteringen av trafik. Grunden till dessa funktioner är så kallad ***digitala certifikat*** som är ett dokument som kopplar ihop en person, ett program eller en tjänst med en given publik krypteringsnyckel.

1.7 DISPOSITION

Denna uppsats är indelad i åtta kapitel och en referensförteckning.
Nedan följer en beskrivning över hur kapitlen är strukturerade och en kort förklaring av dess innehåll.

Kapitel 1 - Inledning
Detta inledande kapitel ger en bakgrundsbild i ämnet, en grundläggande förståelse kring det problemområde som skall undersökas (hypotesen) och här förklaras mål och syfte med uppsatsen samt de avgränsningar vi gjort.

Kapitel 2 - Metod
Det andra kapitlet är uppsatsens metodavsnitt och här förklaras val av metod och material samt käll- och metodkritik.

Kapitel 3 - Identifiering
I detta kapitel förklaras de olika grundbegreppen som identifiering, signering samt integritet och säkerhet.

Kapitel 4 - Teknisk introduktion
Kapitel fyra ger en teknisk introduktion till de tekniker som används vid skapandet av elektroniska signaturer.

Kapitel 5 - Elektroniska signaturer
Kapitel fem förklarar vad elektroniska signaturer är och hur det fungerar. Biometri beskrivs kort som en kompletterande metod. I detta kapitel tas även de juridiska aspekterna upp.

Kapitel 6 – Fallstudier
I kapitel sju redogörs för vår empiriska undersökning, vilken insamlats med hjälp av intervjuer i kombination med observationer. Även egna erfarenheter redovisas.

Kapitel 7 - Analys.
I detta kapitel redovisas vår analys av den teoretiska och empiriska delen. Kapitlet avslutas med en redovisning av våra slutsatser

Kapitel 8 - Slutdiskussion.
Detta avslutande kapitel syftar till att summera våra erfarenheter samt att delge rekommendationer för fortsatt forskning.

2 METOD

I detta kapitel beskrivs vårt vetenskapliga synsätt och vår teoretiska referensram för uppsatsen. Slutligen förs en diskussion kring käll- och metodkritik.

2.1 VAL AV ÄMNE

Anledningen till att vi valde just elektroniska signaturer, och inte någon av de andra säkerhetsfrågorna eller alternativen, var att vi tycke att elektroniska signaturer är den säkerhetsfråga som är mest spännande och som kommer att ha stor inverkan på utvecklingen inom elektroniska och mobila tjänster. Det talas mycket om säkerhet på Internet och vid e-handel och en mycket viktig punkt är att kunna lita på sina samarbetspartners.
Eftersom elektroniska signaturer är så pass nytt, är det att intressant att undersöka ifall användningen av elektroniska signaturer gör möjligheten att identifiera sig över Internet bättre.
Elektroniska signaturer är den lösning som ska kunna vara en digital ersättning för en juridiskt bindande namnteckning t.ex. på ett kontrakt eller annan avtalshandling.[4] Denna utveckling verkar väldigt intressant och vi kände att det var något som vi ville undersöka mer ingående.
Lagen om elektroniska signaturer har nyligen trätt i kraft i Sverige, så det kommer att bli spännande att se ifall resultatet av vår undersökning stämmer överens med den framtida utvecklingen bland företag och privatpersoner.

2.2 VAL AV METOD

Syftet med en uppsats är ofta avgörande för vilken metod man väljer att arbeta. En undersökning som söker svaret på frågan ”hur många” bör baseras på en kvantitativ studie. Är syftet istället att skapa en överblick och förståelse, samt få svar på frågan ”varför” är kvalitativa studier att föredra.[5]
För att komma in i ett forskningsområde och precisera vad det är man vill göra är litteraturstudier en viktig del av uppsatsarbetet. Det finns dock ett antal problem förknippade med litteraturstudier. Dels kan det vara svårt att hitta relevant litteratur, dels kan det vara svårt att välja ut lämpliga delar ur litteraturen.[5] För att finna relevant litteratur har vi bland annat studerat de källor som tidigare uppsatser, vilka behandlar närliggande områden, baserats på. Vi har även tagit kontakt med i ämnet insatta personer, som har givit oss litteraturtips.
Detta för att få en överblick över befintlig och användbar litteratur.

Vi behövde skapa någon form av överblick och förståelse för vad integritet och säkrare transaktioner innebär. Eftersom vi inte såg kvantitativa studier som någon lösning (då denna metod utmynnar i numeriska observationer eller låter sig omvandlas till sådana.) valde vi att göra en kvalitativ studie av elektroniska signaturer.
Eftersom teorier rörande hur elektroniska signaturer fungerar i praktiken är begränsade har vår analys av empiriska data främst skett utifrån existerande teorier om identifiering, tillit och datasäkerhet.

Vi har använt oss av både direkt och indirekt datainsamling.

”Med direkt informationsinsamling avses att man med egna ögon och öron iakttar ett skeende. Indirekt innebär att man försöker ta del av iakttagelser som redan gjorts av någon annan.” [6]

Direkt så till vida att vi har installerat en egen elektronisk signatur och sedan provat oss fram till olika användningsområden. Vår indirekta informationssamling kommer från diskussioner och intervjuer.
Användandet av elektroniska signaturer är relativt begränsat än så länge, men det finns några organisationer som har börjat använda dem, såsom Copenhagen Business School, i Köpenhamn. Vi har undersökt denna organisation för att se hur elektroniska signaturer fungerar och vilka roller de har i praktiken. Intervjuerna genomfördes i ostrukturerad form, vilket innebär att intervjun är av samtalskaraktär. Några frågor förbereddes inte, men vi försökte i viss mån styra intervjun i önskad riktning för att kunna fokusera på problemområdet.

2.3 VAL AV MATERIAL

För att kunna sätta oss in i ämnet om elektroniska signaturer som möjligt, har var vi tvungna att hitta relevant material. Böcker, uppsatser och artiklar om just elektroniska och digitala signaturer studerades, men även relaterade ämnen såsom Internetsäkerhet, kryptering, EU-direktiv, biometri osv. har vi tagit del av, för att kunna skapa oss en helhets bild om signering.

2.3.1 Val av sekundärdata

När det gäller sekundärdata finns det en stor risk att information hinner bli inaktuellt, så vi har försökt att hela tiden vara uppdaterade. För att kunna hitta ny och uppdaterade artiklar som belyser vårt ämne har vi att använt oss av olika tidskrifter och artiklar. Internet har varit en källa och för att finna relevant information har vi framförallt använt oss av sökmotorn, Google. Även flera facktidskrifter som vi studerat finns idag i elektronisk form på Internet.

Vårt ämne har medfört att vi har främst sökt litteratur inom domänen för datasäkerhet. Den författare vår litteraturdel grundas på är framförallt Pfleeger (2000). Anledningen till att vi har valt Pfleegers (2000) ” Security in computing” är att den ger en övergripande och djupgående genomgång av datasäkerhetsområdet. Även Elektroniska Signaturer.(2000) av Halvarsson och Morin, har studerats mycket.

2.3.2 Val av primärdata

En av våra empiriska studier utfördes på Copenhagen Business School, CBS, i Köpenhamn. Som komplement till litteraturstudien genomfördes samtal och diskussioner med Annie Stahel som var projektledare för pilotprojektet med införandet av elektroniska signaturer vid CBS. Vi har även experimenterat med en egen elektronisk signatur och på så sätt fått information och erfarenheter av hur de fungerar.
De samtal och observationer som har gjorts är som tidigare sagts främst avsedda som ett komplement till litteraturstudien eftersom uppsatsen i huvudsak är teoretiskt uppbyggd.

2.4 KÄLL- OCH METODKRITIK

Att uppsatsen till största del bygger på litteraturstudier kan vara en nackdel eftersom all data är andrahandsinformation och det kan dessutom vara svårt att avgöra tillförlitligheten hos dessa källor. Detta problem ökar när Internetkällor används eftersom dessa inte är beständiga och det kan vara svårt att i efterhand hitta ursprungskällan. Därför har vi i första hand använt Internet som ett sökverktyg och strävat efter att söka upp den skriftliga ursprungskällan. Eftersom utvecklingen inom vårt problemområde går snabbt kan skriftliga källor dock snabbt bli inaktuella och i detta sammanhang kan en Internetkälla vara befogad om ingen aktuell litteratur finns att tillgå.

Vi anser att det inte är möjligt att göra objektiva urval i det material som insamlats. Det finns en risk att urvalet omedvetet påverkas av våra egna värderingar som från början skapar en föreställning om slutsatserna. Eftersom vi är två författare till denna uppsats kan det uppstå meningsskiljaktigheter och åsiktskollisioner. Vi har därför genom diskussioner enats om ett gemensamt förhållningssätt som vi båda kan stå för.

3 PROBLEMOMRÅDEN PÅ INTERNET

I detta kapitel ges en teoretisk genomgång av grundbegreppen i vår hypotes. Signering, integritet, säkerhet och identifiering. Såväl på Internet som i det vardagliga livet.

3.1 INTEGRITET

Vad är integritet? Det finns olika typer av integritet, men de vi kommer att beröra är personlig och dataintegritet.
Personlig integritet är skydd av information om personen från olovlig och eventuell olaglig tillgång. Här ingår skydd från identitets stöld, som begås då en person försöker och/eller lyckas använda en annan persons identitet för egen vinst, och skydd mot att känslig information inte läses av obehöriga. Inom t.ex. sjukvården är det ett självklart krav att patientinformation skyddas mot insyn dvs. att patienters personliga integritet skyddas.
Dessa skydd av personlig integritet är en av de viktigaste frågorna på Internet idag. Även enskilda personer har rätt till integritet och har behov av att skydda sitt privatliv. Dessa rättigheter och behov finns också vid överföring av e-post eller annan användning av Internet Flera Internetsiter samlar personlig information från användaren genom online registrering, undersökningar eller blanketter. Det är som användare idag svårt att kontrollera att obehöriga inte får tillgång denna personliga information. För att främja den elektroniska handeln är det viktigt att användarna kan känna tillit till systemen, inte minst när det gäller skydd mot intrång i den personliga integriteten.[2]

Man måste kunna lita på att ingen annan har ändrat den data som en part sänder till en annan. Detta blir ett stort problem när data sänds över öppna nätverk t.ex. Internet. Dataintegritet är skydd mot att data inte kan bli modifierad av obehöriga användaren. I detta sammanhang inkluderas även skriva, ändra, ändra status, radera och skapa i begreppet modifiera.[3]

Många företag är geografiskt spridda, såväl nationellt som internationellt, och behöver överföra information till spridda enheter. För att företagen ska kunna använda Internet till olika ändamål måste informationen kunna skyddas mot insyn och manipulation. För att såväl företag, myndigheter och andra organisationer som enskilda personer skall ha förtroende för att utnyttja alla de möjligheter Internet erbjuder och kommer att erbjuda, krävs det att information skyddas.[7]

3.2 IDENTIFIERING

Traditionellt kommunicerar vi genom att fysiskt befinna oss på samma plats, via handskrivna brev eller genom att tala i telefon. Vi identifierar andra människor genom att se dem framför oss eller känna igen deras handstilar och röster. Varje dag sker identifiering i den fysiska världen, t.ex. när du kommer utomlands visar du upp ditt pass och vid passkontrollen görs en jämförelse mellan fotot i passet och dig. På Internet är identifiering grundläggande. Ett problem idag är att en visuell identifiering inte är gångbart.[4]
Istället har många människor i dagsläget en identitet som på Internet bedöms genom deras e-postadress. Denna identifikation kan fungera som användarnamn, oftast kombinerat med ett lösenord, och som signatur vid e-postkorrespondens.[8] Enligt Ann Beeson[9] , såväl som många andra, så kan ett e-post lätt spåras och lagras av andra och kan därför inte anses vara en säker identitetsform. Som vi tidigare nämnt, är det viktigt att användarna kan känna tillit till Internet och få skydd mot intrång i den personliga integriteten. De tre olika anledningarna till att fastställa en persons identitet är:

- ***Identifiering,***
  En identifiering är till för att ta reda på vem någon är. Det finns ingen utsago om personens identitet.

- ***Verifiering***
  En person hävdar att han är en viss individ. Det krävs något för att verifiera detta påstående: en PIN-kod, ett lösenord eller ett tumavtryck.

- ***Auktorisering***
  Innebär att en behörighetskontroll görs. Denna kontroll säkerställer att personen i fråga är behörig till önskad information eller hårdvara.

Ovanstående kontroller fungerar bra i den fysiska världen. Nu finns det ett stort behov av att hitta tillfredsställande mobila och elektroniska motsvarigheter, eftersom Internetanvändaren inte upplever något reellt förtroende eller trygghet i sina elektroniska relationer.[1]

3.3 SIGNERING

Den vanligaste individuella identifieringen sker via din fysiska underskrift, t.ex när du signerar ett kontrakt. På samma sätt som vi kan använda denna namnteckning för olika ändamål behöver vi generella lösningar för elektronisk identifiering. Standarder som ger bekräftelser som inte kräver speciell teknik och separata juridiska överenskommelser med varje ny part som man skall göra affärer eller ha annat utbyte med.[10]

För det stora flertalet människor borde företeelsen att skriva sitt namn på ett papper betraktas som okomplicerat. Det är ofta redan av sammanhanget uppenbart när en namnteckning förväntas och vilka följder detta får.

Genom att signera ett dokument uppnås två saker: autencitet och förfalskningsskydd, alltså verifiering och skydd mot förfalskning av signatur. I praktiken litar vi ofta på t ex en signatur som återges i ett mottaget faxmeddelande, trots att det är enkelt att, med stöd av en dator och en scanner, kopiera den elektroniska bilden av underskriften och sedan tillfoga den till vilket dokument som helst. På motsvarande sätt kan mottagaren läsa faxet direkt på sin datorskärm och endast besvara det elektroniskt. Vid en sådan kommunikation behöver det alltså inte finnas något pappersbaserat original. För att ersätta dessa lättmanipulerade rutiner har säkra tekniska motsvarigheter till underskrifter skapats, baserade på kryptering. Underskriften identifierar den som undertecknar och ger tillit till att viss text omanipulerat härrör från den som framstår som utställare.[11] Det blir allt vanligare att det inte finns några fysiska dokument att signera och signeringen görs då istället digitalt. Målsättningen är dock densamma; att säkerställa vem som är avsändare av ett meddelande.

3.4 SÄKERHET

Internet är en anonym värld, där traditionella metoder att identifiera individer och organisationer inte fungerar. Tilltro och förtroende är ett viktigt begrepp när man diskuterar säkerhet. En pålitlig säkerhet är fundamental när man ska skicka känslig och kommersiell information på Internet, oavsett om det är mellan privatpersoner, företag, anställda och arbetsgivare, säljare eller köpare. En säker överföring av meddelanden kan ges följande egenskaper: [12]

- **Konfidentialitet**
  Konfidentialitet innebär att andra inte kan "avlyssna" meddelandet. I dag finns detta i allmänhet inte på Internet.

- **Dataintegritet**
  Detta innebär att de meddelanden som mottags är de samma som de som avsänds.
  Som vi tidigare nämnt passerar meddelanden över ett öppet nät (Internet) som har miljoner datorer anslutna och där finns ingen garanti för integritet.

- **Autencitet**
  Autencitet innebär att man vet vem man kommunicerar med. På Internet finns inget av det som vanligtvis ger autencitet - signatur, röst eller ansikte.

- **Icke-förnekbarhet**
  Icke-förnekbarhet innebär att de som kommunicerat inte kan förneka detta. Eftersom man inte erhåller någon kvittens kan mottagaren påstå att han/hon inte erhållit meddelandet, och om avsändaren ångrar sig kan denne påstå att han/hon inte sänt meddelandet.

Internets infrastruktur måste därför skyddas mot intrång, förvanskning av data (att data-integritet bibehålls) eller andra ingrepp. Säkerhetsmodellen[13]för elektroniska transaktioner tar upp sex tänkbara scenarier med hotbilder som företag kan gradera sig mot. I modellen ingår följande sex säkerhetsfunktioner

1. ***Förvanskningsskydd (Message content integrity)***
   Innebär skydd mot förändring av ett meddelande

2. ***Äkthetsbevis (Message origin authentication)***
   Innebär skydd mot att den som skickar ett meddelande inte är någon annan än den han uppger sig vara, dvs. avsändaren är äkta.

3. ***Skydd mot förnekande av ursprung (Non-repudiation of origin)***
   Innebär skydd mot att den som skickar ett meddelande inte vid ett senare tillfälle kan neka till att denne har skickat meddelandet.

4. ***Skydd mot förnekande av mottagning (None-repudiation of receipt)***
   Innebär skydd mot att den som mottagit ett meddelande inte vid ett senare tillfälle kan neka till att ha tagit emot det.

5. ***Sekvensskydd (Message sequence integrity)***
   Innebär skydd mot att meddelandet dubbleras eller försenas, att delar av meddelandet blir kopierat eller försvinner och mot att inget tillägg görs.

6. ***Insynsskydd (Confidentiality of content)***
   Innebär skydd mot att ett meddelande läses av obehöriga.

Internet är till sin natur ett osäkrat nät. Det finns ingen som är ytterst ansvarig för Internet, därmed ingen att vända sig till för att få garantier. Det som behövs är en garanti som säkrar datatrafiken, vilken i sin tur skapar förtroende som bl.a. bereder väg för elektronisk handel i stor skala.

4 TEKNISK INTRODUKTION

Här beskriver vi den tekniska bakgrunden och plattformen för elektroniska signaturer. Detta sker genom en grundläggande genomgång av symmetrisk och asymmetrisk kryptering, PKI samt certifikat.

4.1 KRYPTOLOGI

”Att skicka meddelande över öppna nätverk är riskfyllt. Ett meddelande kan avlyssnas (tappas), återanvändas och få innehållet och/eller användaren ändrad. För att förhindra förvanskning av ett meddelande används olika kryptografiska metoder. Kryptering används när hela meddelanden måste krypteras. Innehållet är då så känsligt att obehöriga inte kan tillåtas läsa det. Om ett meddelande däremot kan tillåtas läsas av utomstående parter, så länge innehållets och avsändarens äkthet kan garanteras, används digitala signaturer. Metoderna används alltså för att säkra sekretessen, det vill säga konfidentialiteten hos ett meddelande samt för att garantera avsändarens och innehållets äkthet.”[14]

Kryptering betyder gömd skrift, metoden som används för att dölja text. En av de tidigaste krypteringsmetoderna är ”Ceasars cipher”, den form av kryptering som Julius Ceasar använde sig av. Metoden går ut på att varje bokstav omvandlas till bokstav som befinner sig längre fram i alfabetet. Använder man sig av siffran 3 innebär detta att bokstaven A ersätts med D. När mottagaren sedan ska tyda meddelandet krävs att denne vet att D ska räknas tillbaka 3 steg för att få den ursprungliga bokstaven.[3]
Kryptering har alltså traditionellt sett använts för att skydda datamängder mot insyn, för att skapa konfidentialitet. På senare tid har nya krypteringsmetoder utvecklats som gör det möjligt att även skapa ett upphovs- och förändringsskydd. Dessa senare metoder har bland annat öppnat vägen för digitala signaturer.
Trots att krypteringstekniken har förändrats sedan Julius Ceasars tid kan all kryptering beskrivas utifrån att information i sin normala form, *klartext*, förvrängs till oigenkännlighet, *kryptotext*. För att kunna läsa en kryptotext måste den först dekrypteras tillbaka till klartext. Omformningen från klartext till kryptotext och vice versa sker med hjälp av en matematisk algoritm. Kryptografins styrka beror på den algoritm och de nycklar som används. Antalet bitar i nyckeln bestämmer hur lång krypteringsnyckeln är och därmed hur stark och säker krypteringen blir.[15] För varje tillkommande bit i nyckeln fördubblad antalet möjliga kombinationer av nycklar. Det innebär att varje ytterligare bit i nyckeln gör att det tar dubbelt så lång tid för en inkräktare att pröva sig fram till rätt nyckel. För nycklar i digitala signaturer använder man 512-bitars eller 1024-bitars nycklar.
Det finns två typer av krypteringsalgoritmer, symmetriska och asymmetriska. Vid symmetrisk kryptering används samma nyckel för både kryptering och dekryptering. Asymmetrisk kryptering, karakteriseras av att två olika nycklar används vid kryptering och dekryptering.

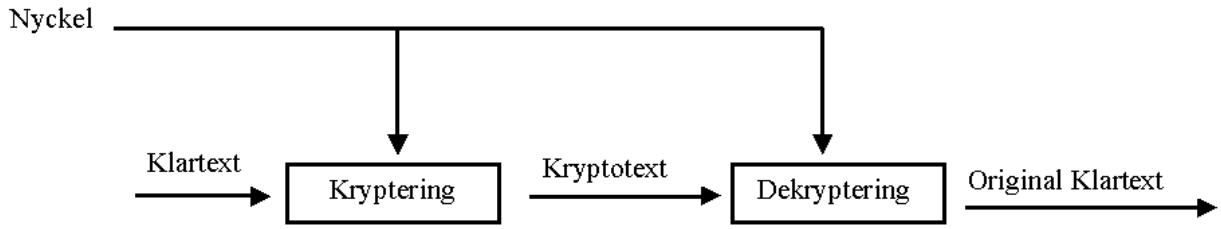
Det finns ett par av samhörande krypteringsnycklar, där den ena offentliggörs, den publika nyckeln och den andra, den privata nyckeln, förblir hemlig och endast känd av användaren. [15]. Symmetrisk och asymmetrisk kryptering skyddar meddelanden mot avlyssning.

Ett meddelande ska dock inte bara skyddas mot avlyssning, det är bara en av säkerhetsriskerna. Andra är att ingen manipulerat meddelandet på vägen, eller att avsändaren är den han utger sig för att vara. För att veta att detta inte har inträffat används en grupp av algoritmer som använder hashing, dvs. räknar ut en kontrollsumma* ett så kallat hashvärde.[16] Med hjälp av hashing går det att åstadkomma ett integritetsskydd för filer. Utgående från informationen i filen beräknas en kontrollsumma, ett fingeravtryck med hjälp av en algoritm. Filen kan ha vilken storlek som helst medan kontrollsumman har en fix längd. Kontrollsumman lagras på ett säkert ställe där den inte kan modifieras. För att sedan kontrollera att filen inte har ändrats beräknas kontrollsumman ytterligare en gång och jämförs med den lagrade varianten. Om de två är lika är det ytterst osannolikt att filen har ändrats, eftersom hashalgoritmen har egenskapen att i princip varje ändring i filen medför att hash-värdet ändras.[14]

* En kontrollsumma är ett tal som beräknas ur en datamängd med en känd formel. Avsändaren räknar ut ett tal med formeln och skickar data och kontrollsumma. Mottagare av data beräknar med samma formel ett tal och jämför med det tal som kom från avsändaren. Om dessa två tal är olika, har inte korrekt information mottagits. Kallas också hashvärde.

4.1.1 Symmetrisk kryptering

Den symmetriska krypteringstekniken är den äldsta och mest beprövade tekniken. Tekniken baseras på att sändare och mottagare använder samma (gemensamma) nyckel för både kryptering och dekryptering.[10] Då krypterings- och dekrypteringsnycklarna är identiska krävs att nyckeln hålls hemlig för de parter som inte ska få tillgång till meddelandet och därmed dess information.[17]



Figur 4:1 Symmetriskt kryptosystem

En sändare och mottagare kommer överens om vilken nyckel som skall användas för att kommunicera med varandra, denna nyckel hålls hemlig. Nyckeln måste på något sätt föras över mellan parterna. Om de nu vill kommunicera med en tredje part så krävs ytterligare en annan nyckel då dessa parter kommunicerar med varandra. Detta innebär att för varje ny part skall en ny nyckel skapas och om antalet kommunicerade parter blir för stor krävs det en omfattande nyckeladministration, vilket kan så småningom bli ohållbar.[4]

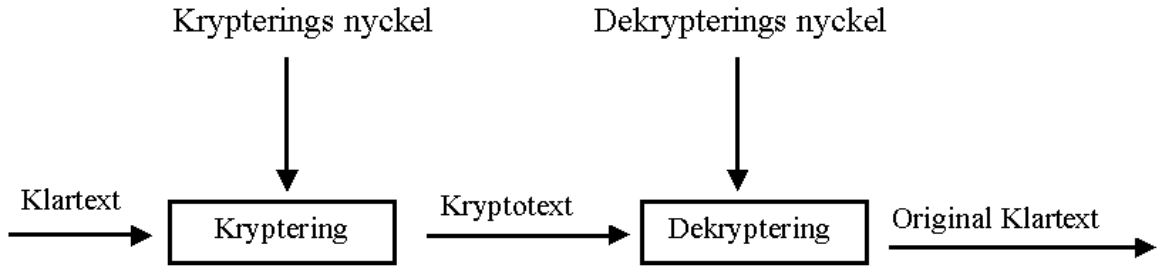
Symmetrisk kryptering har den fördelen att det är en väl beprövad teknik och att krypteringsalgoritmerna kan begränsas i sin komplexitet, vilket innebär att tekniken är relativt snabb.
” Svårigheten med symmetrisk kryptering ligger i att mottagaren av ett meddelande måste få kännedom om den hemliga nyckeln utan att någon obehörig får det.” [2]

Den stora nackdelen med symmetrisk kryptering rör alltså distributionen av nycklar. Alla som ska läsa ett krypterat meddelande måste ha tillgång till samma nyckel. IDEA* och DES** är exempel på vanliga symmetriska krypteringsalgoritmer varav DES är den mest använda.[2]

* International Data Ecryption Standard
** Data Encryption Standard

4.1.2 Asymmetrisk kryptering

Asymmetrisk kryptering är en förhållandevis ny teknik som utnyttjar två skilda nycklar vid kryptering respektive dekryptering. [10]
Till skillnad från symmetrisk kryptering använder sig asymmetrisk kryptering av två skilda nycklar, nämligen en *publik* och en *privat*. Varje användare har en publik/öppen och en privat nyckel, vilka tillsammans utgör ett unikt par. Varje användare har två olika nycklar (nyckelpar). Den ena nyckeln är den publika och den andra är privat och hålls hemlig.
En av nycklarna används för att kryptera informationen och den andra för att dekryptera den. När data krypteras med den publika nyckeln kan det bara avkodas med den privata nyckeln, och tvärtom, när data krypteras med den privata nyckeln kan den avkodas med den publika nyckeln.



Figur 4:2 Asymmetriskt kryptosystem

Därigenom kan säkerheten bevaras samtidigt som man får en snabb och enkel distribution av nycklarna. Viktigast är att de två nycklarna endast kan användas tillsammans, alltså att då informationen krypteras med den ena nyckeln i nyckelparet så kan informationen endast dekrypteras till sin ursprungliga form med den andra nyckeln i nyckelparet.
Med detta nyckelsystem så kan avsändaren alltid vara säker på att den enda som dekrypterar avsändarens meddelande är mottagaren. Om man vill identifiera sig själv kan man kryptera en text med sin privata nyckel. Den kan av den som vill kolla identiteten dekrypteras med den öppna nyckeln, som alla har tillgång till. Om värdet som kommer fram överensstämmer med det värde som från början krypterades kan mottagaren vara säker på att avsändaren verkligen är korrekt avsändare, eftersom ett värde som korrekt kan dekrypteras med den offentliga nyckeln bara kan ha krypterats med rätt privata nyckel.

När krypteringen utförs av datorer kan den också knäckas med datorer. Därför är nyckelns längd avgörande. Ju längre nyckellängd, desto längre tid tar det att knäcka. För symmetrisk kryptering används idag 40-bitar medan asymmetrisk kryptering använder sig ofta av nycklar med 1024 bitar. Asymmetrisk kryptering av hela meddelandet är en tidskrävande algoritm.[3]
Om meddelanden inte måste hållas hemliga utan endast skyddas från manipulation används därför digitala signaturer.

Det är denna funktion som används när digitala signaturer skapas. Asymmetrisk kryptering är alltså en förutsättning för digitala signaturer, där sändaren skapar signaturen med sin privata nyckel och mottagaren verifierar med den korresponderande publika.
Även om det finns ett antal olika asymmetriska krypteringsalgoritmer har RSA utvecklats till att bli en de facto-standard.[1] RSA utvecklades 1978 av Rivest, Shamir och Adleman och fick sitt namn från deras initialer.

4.1.2.1 Nyckelhantering och förvaring

En viktig fråga är hur den privata nyckel som korresponderar med den publika skall kunna skyddas. Den privata nyckeln får, varken när den genereras eller senare när den förvaras av användaren, komma till någon obehörigs kännedom. Det finns olika sätt att spara och lagra den privata nyckeln. Några exempel är

- **Personlig ”nyckel”**
  Liten sak som bäras på en vanlig nyckelring, och som sätts in i en port direkt i dator. I nyckeln finns ett chips som är unikt och identifierar bäraren.
- **Mobiltelefon**
  I alla mobiltelefoner finns redan ett SIM-kort som håller reda på vad abonnemangets telefonnummer. Det kortet kan också användas för digitala signaturer.
- **Koddosor**
  Används sedan länge av kunder hos Internetbankerna. De nuvarande dosorna omfattas dock inte av den nya lagen, utan bygger på avtal mellan banken och kunden.
- **Mjuka certifikat**
  Ett program som lagras på datorn och identifierar användaren.
- **Smarta kort**
  Ser ut som ett vanligt id-kort förutom att det också har ett chips. För att kunna använda kortet krävs en kortläsare till datorn. Många förordar att nyckeln ska förvaras i ett chips på ett traditionellt ID-kort.

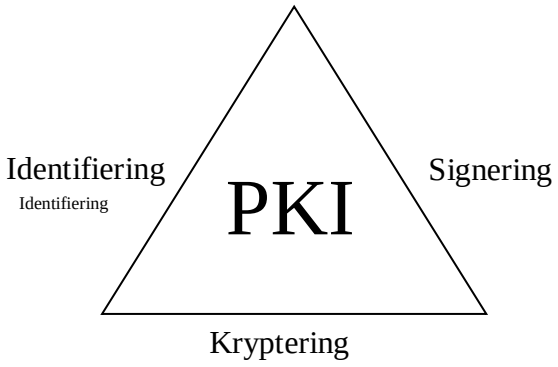
Oavsett vilken av dessa förvaringsmetoder man använder måste den vara oanvändbar utan individens närvaro, annars är det inte en personlig signatur. För att tillgodose detta krav utformas kortet så att det är blockerat tills individen har visat sin närvaro. Att visa individens närvaro kan vara svårt och det finns flera olika sätt att använda. Den vanligaste metoden är att ha en kort hemlig siffersekvens, en PIN-kod, på samma sätt som till bankomatkort. För närvarande används PIN-kod för att skydda kortet, eller den elektroniska identiteten, från missbruk. Om koden exponeras kan den missbrukas. Till skillnad från andra system krävs dock att missbrukaren, utöver koden, måste ha fysisk tillgång till kortet. Koden används endast för att starta den förbestämda processen i kortet. Koden har ingenting med framställningen av den digitala signaturen att göra. PIN-koden kommer förhoppningsvis att kunna ersättas med biometriska rutiner.

4.2 PUBLIC KEY INFRASTRUCTURE

För att säkerhetsställa att den grundläggande uppgiften, om vem ett nyckelpar tillhör, behövs en helt ny infrastruktur för publika nyckelsystem, med en engelsk term Public Key Infrastructure (PKI), där certifikat utgör en viktig pusselbit.
PKI, är samlingsnamnet för lösningar där man med hjälp av en speciell krypteringsteknologi skapar system för identifiering, kryptering och integritetskontroll. Det är system som både består av avancerad säkerhetsteknik och olika regelverk, anpassade för specifika användningsområden. Som exempelvis, elektroniska signaturer för olika typer av avtal, säkra elektroniska transaktioner mellan företag, identifiering av användare, säker e-post och olika typer av säker kommunikation över publika nätverk.[18] I en PKI ingår en rad olika funktioner, t.ex.:

- Certifiering, skapande av certifikat
- Verifiering, kontroll av certifikat
- Revokering, återtagande av certifikat

PKI-tekniken bygger på förtroendet för certifikatutfärdaren. Denne utfärdar certifikaten och de organisationer som utnyttjar dem förlitar sig på dem. Det gör att tekniken är lämpad för relationer en-till-många, ett certifikat kan alltså användas i flera sammanhang, medan t.ex. engångslösenord förutsätter en en-till-en relation.[19]
En certifikatbaserad PKI kan erbjuda en teknik för att etablera tilltro och erhålla säkra tjänster. Denna tilltro kan sträcka sig över organisatoriska och även landsgränser, även om parterna tidigare var okända för varandra. Detta gör att PKI är en grundläggande faktor för elektroniska signaturer.



Figur 4:3 Grundstenar i en elektronisk signatur.[4]

4.3 CERTIFIKAT

Ett digitalt certifikat är ett dokument som kopplar ihop en person, ett program eller en tjänst med en given publik krypteringsnyckel. Ett certifikat skapas genom att någon betrodd person eller organisation, en s.k. CA (Certification Authority). I Sverige är dessa organisationer Telia och Post & Telestyrelsen. Certifikaten är för det mesta definierade i ISO-standarden X.509v3, men det finns också andra format.[1] Digitala certifikat innehåller information om:

- certifikatinnehavarens namn och adress, e-postadress och ev. ytterligare uppgifter
- certifikatutfärdarens namn och adress, e-postadress, webbadress och andra relevanta uppgifter om hur man kan få kontakt med certifikatutfärdaren
- certifikatets giltighetstid. Certifikaten är tidsbegränsade. När certifikattiden gått ut måste användaren byta ut sina krypteringsnycklar och få dessa certifierade igen.
- vilka ev. andra certifikatutfärdare som i sin tur kan intyga certifikatutfärdarens egen identitet.

Certifikatet signeras med certifikatutfärdarens eget nyckelpar , dvs. den privata respektive den publika nyckeln. Ett digitalt certifikat kan spridas fritt och utgör en koppling mellan certifikatet och en viss fysisk eller juridisk person. Det digitala certifikatet kan användas för skyddad e-post (förhindra obehörig åtkomst) och elektronisk signering.
I alla dessa metoder måste man dock skilja på tekniken och det system av förtroenden och rutiner som vilar på tekniken. Tekniken i sig skapar inte säkerhet. Någonstans i varje PKI finns rutiner som kopplar samman företag, organisationer och personer med krypteringsnycklar i certifikat. Den rutinen utförs av en trovärdig part, en s.k. Certification Authority(CA) även kallad Certification Service Provider (CSP), som lämnar vissa uppgifter i elektronisk form om individen och signerar dessa. Förtroendet för nycklar i ett visst nyckelsystem beror på hur mycket man litar på en CA: s rutiner för att kontrollera att en person eller ett företag verkligen hör ihop med en öppen nyckel.
Detta kan jämföras med hur informationen i en fysisk ID-handling säkras genom att den framställs på ett svårförfalskat sätt. Syftet är att aktörerna ska kunna lita på att en viss privat nyckel verkligen innehas av den som påstås vara innehavaren.
Enligt regeringskansliets referensgrupp[14] kan man skilja på hårda och mjuka certifikat. Det är de fysiska bärarna av de privata nycklarna som avgör typen. Med hårda certifikat avses sådana som där nycklarna förvaras i någon form av hårdvara, t.ex. i ett aktivt kort eller annan utrustning som är avsedd för ändamålet.
Att säkerheten är lägre i de mjuka certifikaten beror på att de privata nycklarna lagras i en vanlig datafil. Filen överförs vanligtvis till en diskett eller till en hårddisk och skyddas genom exempelvis lösenord eller genom förvaring i ett låst kassaskåp. En CA kan antingen vara intern för ett företag (se kapitel 6 om Copenhagen Business School) eller erbjuda sina tjänster till allmänheten. En CA som erbjuder sina tjänster till allmänheten uppträder som en betrodd tredje part, även kallad ”Trusted Third Party”.[14]

5 ELEKTRONISKA SIGNATURER

Detta kapitel är en ingående förklaring till identifieringsmetoden, elektroniska signaturer. Även kompletterande metoder beskrivs kort. Slutligen redogörs för den juridiska aspekten.

5.1 VAD ÄR ELEKTRONISKA SIGNATURER?

Elektroniska signaturer ska betraktas som en motsvarighet till en handskriven signatur på ett pappersdokument fast med mer funktioner och större säkerhet.[13] Syftet är att mottagaren av ett elektroniskt meddelande som är signerat med säkerhet vet att avsändaren är äkta, dvs. är den som personen eller systemet utger sig för att vara.

Elektroniska signaturer är data i elektronisk form som är fogade till eller logiskt knutna till en elektronisk handling och som används för att kontrollera om innehållet härrör från den som framstår som undertecknare. Den teknologi som används för att gör detta möjligt är digitala signaturer. Begreppet innefattar även den teknik som innebär att man har två sammanhörande krypteringsnycklar som användas för identifikation, kryptering och signering.[4]
Dessa tre element är grundstenarna i en elektronisk signatur. Som plattform ligger PKI. Dessa delar i kombination ger oss bl.a. säker e-handel. PKI-teknik är för närvarande den bästa metoden att åstadkomma en elektronisk signatur. Användning av den tekniska metod som brukar betecknas digital signatur innebär förutom identifiering av nyckel- och certifikatinnehavaren också att data skyddas mot oupptäckt förvanskning. Detta ger fördelar jämfört med metoder som enbart erbjuder identifiering såsom t.ex. symmetrisk kryptering, engångslösenord eller PIN-koder.
Det är endast signaturer som är baserade på asymmetriska nyckelsystem som betecknas ”digital” signatur, medan begreppet ”elektronisk” signatur brukar anses inrymma alla tänkbara varianter, från de mest avancerade kryptografiska skydden till att på tangentbordet skriva sitt namn under en ordbehandlingstext.[20] Elektroniska signaturer och elektronisk identifiering kan idag användas inom flera olika områden och för olika ändamål[21],

- Attestering av fakturor
- Kryptering av e-post
- Signering av avtal elektroniskt
- Godkänna dokument
- Lämna offert elektroniskt
- Upprättande av säker förbindelse för kommunikation

Elektroniska signaturer bygger på förtroende[11]. Så för att ovanstående uppgifter ska kunna underlättas och effektiviseras, är det viktigt att kunna försäkra sig om att avsändaren är den rätta och att programmet resp. dokumentet inte har blivit förändrat.

Hanteringen av elektroniska signaturer kan bli förtroendeingivande genom: [22]

- att framställningen av den privata, nyckeln sker under användarens kontroll.
- att privata och publika nycklar är skyddade.
- att program alltid skiljer på inloggning (autentisering) och underskrift (signering).
- att program alltid visar dokument som ska skrivas under.
- att elektroniska signaturer är oberoende av operativsystemet.
- att leverantörer av certifikat, program och utrustning lämnar garantier för funktionen.

Elektroniska signaturer tillför meddelande ”autencitet”, dataintegritet och ”non-repudation”.[3] Med andra ord gör elektroniska signaturer det möjligt att ingå i bindande transaktioner, så som fakturabetalning och lägenhetsköp.

5.2 HUR FUNGERAR DIGITALA SIGNATURER?

En digital signatur är en funktion som garanterar innehållet och äktheten hos en elektronisk handling. Funktionen uppnås genom en kombination av asymmetrisk krypteringsteknik och hashing.
För att skapa en digital signatur på ett meddelande använder man sig av en *hashfunktion*. Genom en beräkning av det aktuella meddelandets innehåll skapas en kontrollsumma, ett så kallat *hashvärde.* Denna kontrollsumma av meddelandets innehåll, krypteras med avsändarens privata nyckel. Den krypterade kontrollsumman utgör den digitala signaturen och tillförs meddelandet. Signaturen och meddelandet kan sedan säkert skickas över ett öppet nätverk till mottagaren. Signaturen är alltid kopplad till en informationsmängd. Att signera något behöver inte betyda att informationen döljs, att den krypteras. Signering innebär endast att man kan identifiera avsändaren samt att man kan avgöra att informationen inte är förändrad på vägen från avsändaren.
Signaturen kan inte förhindra att någon utomstående ändrar meddelandet eftersom meddelandet skickas i klartext. Eventuell manipulation upptäcks dock när mottagaren dekrypterar kontrollsumman med avsändarens publika nyckel, samt använder samma hashfunktion som avsändaren för att göra ett eget kontrollvärde av det i klartext skickade meddelandet. För att sedan få veta om det skickade meddelandet är äkta behöver mottagaren bara jämföra det egna kontrollvärdet med det skickade. Överensstämmer de båda värdena har ingen manipulation gjorts. Hur det går till när en digital signatur skapas kan beskrivas med följande scenario:

1. **Avsändaren beräknar kontrollsumma**
   En programvara beräknar, med en känd formel, en kontrollsumma (hashvärdet) utifrån den information som ska signeras. Det fungerar ungefär på samma sätt som sista siffran i personnumret, som är framräknad utifrån de nio första. Samma metod använder postgirot och banker för att enkelt kunna avgöra om kontonumret är ett korrekt nummer.

2. **Avsändaren krypterar kontrollsumman med privat nyckel**
   Kontrollsumman krypteras sedan med avsändarens privata, hemliga, nyckel. Den krypterade informationen, kontrollsumman, bifogas originalinformationen som inte är krypterad. Denna bilaga är en digital signatur.

3. **Information och signatur publiceras eller överförs**
   Nu kan informationen och signaturen distribueras tillsammans. De kan skickas som e-post, publiceras som webbsajt eller utgöra en programvara som distribueras över ett nätverk.

4. **Mottagaren dekrypterar bilagan med kontrollsumman**
   En mottagare som vill säkerställa informationen kan dekryptera bilagan med avsändarens publika nyckel. Då får man fram en kontrollsumma.

5. **Mottagaren beräknar ny kontrollsumma**
   Mottagaren (eller troligare: mottagarens programvara) beräknar en ny kontrollsumma utifrån informationen, med samma formel som avsändaren använde.

6. **Kontrollsumman jämförs**
   Den nya kontrollsumman jämförs med den man fått fram genom att dekryptera bilagan till informationen. Om dessa två värden stämmer överens har man kommit fram till två slutsatser. Den första är att avsändaren är den man tror det är (förutsatt att man kan lita på att den nyckel man använt är rätt nyckel) och att informationen inte förändrats. Om värdena inte stämmer överens är informationen inte att lita på.

7. **Båda sidor måste följa samma standard**
   För att det här ska fungera måste både sändare och mottagare följa samma standard. Det gäller både hur kryptering ska ske, hur nycklar kan kontrolleras och hur kontrollsumma beräknas.

Syftet med en digital signatur är att användaren skall kunna ta ansvar för sin signering av ett digitalt dokument. Utöver de tekniska krav som redovisats ovan måste användaren förstå när och var signeringssituationen uppstår. Denna funktion benämns i detta sammanhang ”upplysningsfunktionen”. För att tillgodose detta krav skall användaren kunna ”se” de data som skall ingå i den beräkning av kontrollsumman som föregår signeringen. Denna hashrutin kopplas normalt till en lösenordshantering, dvs. användaren måste ange PIN-koden till sitt aktiva kort eller ett lösenord för att komma åt signeringsnyckeln om den ligger på hårddisk eller diskett. På så sätt uppnås dels upplysningsfunktionen, dels skyddet mot att signeringsnyckeln används utan användarens uttryckliga önskan.[10]

5.2.1 EID-kort

Rent tekniskt kan underskrifterna göras på flera sätt, till exempel via den typ av koddosor som kunder hos Internetbankerna använder. ”Den teknik som har fått mest uppmärksamhet är dock elektroniska ID-kort, som man sticker i en kortläsare kopplad till datorn.”[23]
Det elektroniska ID-kortet, ett EID-kort, innehåller elektroniska ID handlingar i form av digitala certifikat. Utsidan av EID-kortet kan då fungera som ett vanligt ID-kort med bild på innehavaren.
EID-kort är baserade på så kallades smarta kort, ett plastkort försett med ett mikroprocessor chips.
Mikroprocessorn har ”manipulationssäkert” minne, som innehåller privata nycklar och digitala certifikat tillhörande dessa nycklar. Det gör att de privata nycklarna bara kan användas i operationer och uträkningar som sker inne i mikroprocessorn. I dessa fall används chips av en typ som medger dels att lagrade nycklar kan skyddas mot exponering, dels att signeringsprocessen kan ske skyddat. Fördelen med detta, ur säkerhets synpunkt, är att nycklarna aldrig kan visas utanför kortet. Tekniken för att skapa digitala signaturer i ett chips är den i dag bäst kända tekniken. Utöver den tekniska kvaliteten på skyddet tillkommer de sociala aspekterna. Förpackningen, dvs. att montera chippet på ett ID-kort av traditionellt slag, innebär att innehavaren har en större möjlighet att ta ansvar för den fysiska hanteringen av sin ”digitala identitet”. [1]
För att nu förhindra att andra än den rätta användaren använder sig av kortet, måste man använda en PIN-kod (Personal Identity Number) för att aktivera EID-kortet. Precis som vid användandet av vanliga magnetkort (bankkort) är det viktigt att PIN-koden hålls hemlig. Men det är en stor skillnad vid aktiveringen av ett EID-kort m h a en PIN-kod och använda ett magnetkort vid t.ex. ett bankomatuttag. I det senare fallet skickas PIN-koden till ett avlägset datasystem för validering, medan i fallet med EID-kortet, skickas koden bara till kortet för kontroll. Detta gör det möjligt för EID-kort att stödja två grundläggande tjänster:

- Att styrka användarens ”äkthet”
- Kryptera konfidentiella meddelanden med hemligt innehåll

Då en CA (Certification Authority) i detta fall har möjlighet att ta ansvar för hela processen fram till utfärdandet av ID-kortet, skapas förutsättningar för en certifiering med mycket hög trovärdighet. Det är denna situation som ligger till grund för SEIS Policy (S7)[24] för utfärdande av kombinerade elektroniska ID-kort enligt SIS-standard.[23]

5.3 KOMPLETTERANDE METODER

Istället för att använda sig av en PIN-kod för att identifiera ägaren av en elektronisk signatur, kan man använda sig av någon form av biometri, såsom fingeravtryck eller scanning av ögats iris.
Detta är mycket säkra metoder och idag är det omöjligt att förfalska en iris, vilket gör att kombinationen med elektroniska signaturer och iris-scanning är helt säker.

För oss människor är den vanligaste formen av identifiering av en individ att se på ansiktet. Man känner direkt igen en person på dragen. De tekniska förutsättningarna är datorisera visuell identifiering är goda. Det som krävs är en bild. Problemet är komplexiteten i ett ansikte. Tekniken bygger på att en mjukvara lokaliserar nyckelpunkter i ansiktet och mäter avstånd. Ögon och näsa är relativt fasta punkter, medan mun och hårfästet kan variera.
System av denna art är dock känsliga för hur bilden tas. Dessutom kan smink, en ny frisyr och grimaser förstöra möjligheterna för korrekt verifiering. Ansiktsigenkänning är mest lämpade för miljöer, där man redan vet vilka som finns på plats och där säkerhetskraven inte är så höga. För att öka säkerheten kan man istället använda sig av fingeravtryck eller ögonscanning.
Fingeravtrycket är unikt för varje individ, till och med enäggstvillingar har olika fingeravtryck. Samma sak gäller irisavläsning. Mönstret i ögat, såväl iris som retina är unikt och är en säker metod att identifiera en individ. Speciellt retina, ögats inre del som ljuset faller in på, är idag omöjlig att kopiera. Iris, den färgade delen runt pupillen, kan störas med kontaktlinser. Ögonvitan används inte för biometriska system idag.

Det finns ett sätt att helt säkert kontrollera en individs identitet. Genom dess DNA. Det går ej att förfalska eller att stjäla vilket gör DNA-teknik till en helt säker metod. Tekniken är dock alldeles för dyr och komplicerad.
System baserade på biometriska metoder kommer troligen att bli vanliga. Idag ser tekniken med verifiering med hjälp av fingeravtryck ut att bli dominerande. Metoden är mycket säker, kostnaderna är låga och det är enkelt för individen Det är dock bara en del av säkerhetssystemet. Fortfarande kommer krypterad information, låsta dörrar och brandväggarna i datorsystem, att vara nödvändiga.

5.4 JURIDISK ASPEKT

Historiskt sett har en namnteckning och fingeravtryck på papper varit det enda sätt att juridiskt binda en individ till t ex ett beslut, en identifiering eller ett godkännande. Tillkomsten av elektroniska media ställer helt nya krav.
Elektroniska signaturer har länge diskuterats i internetsäkerhetskretsar och blivit allmänt accepterade som pålitliga.[25] Men utan en lag som gäller i alla EU:s medlemsstater är risken stor att många olika tillämpningar växer fram, och detta gör att man kan ifrågasätta den rättsliga giltigheten i signaturerna.
En korrekt användning av elektroniska signaturer eliminerar ett av de viktigaste hindren för att elektronisk handel skall bli allmänt accepterat. Utan tillförlitliga signaturer har man ju egentligen ingen aning om vem som sitter på andra sidan av nätverket, och därmed ingen aning om med vem man gör affärer med, eller vilka befogenheter denne har. Här spelar lagen en viktig roll, där en elektronisk signatur rättsligt kommer att likställas med en handskriven.

Lagar för digitala signaturer är ett mycket viktigt och intressant område. Det pågår ett stort arbete inom EU-kommissionen på detta område.[23] EU kommissionen har sett till att elektroniska signaturer får samma juridiska status som namnunderskrifter. Inte minst den offentliga sektorn är beroende av att få använda elektroniska signaturer. Det uttalade målet är att 25 procent av all offentlig upphandling i Europa ska ske elektroniskt senast år 2003.

Den 13 december 1999 fastställde EU-kommissionen ett EU-direktiv (399L0093) för elektroniska signaturer.[26]
Syftet är att underlätta och främja användningen av elektroniska signaturer vid t.ex. elektronisk handel. En elektronisk signatur kan användas för att säkerställa att elektroniskt överförd information inte har förändrats, att informationens avsändare är den som uppges samt att avsändaren inte senare förnekar att han eller hon sänt informationen.[18]
I direktivet anges att en elektronisk signatur under vissa förutsättningar ska kunna jämställas med en underskrift.
Direktivet innehåller, utöver bestämmelser om vissa elektroniska signaturer, föreskrifter om certifikat för elektroniska signaturer och säkra anordningar för signaturframställning samt om utfärdande av s.k. kvalificerade certifikat. Till detta kommer anknytande bestämmelser om skadeståndsskyldighet för certifikatutfärdare, behandling av personuppgifter, tillsyn och avgifter för tillsynen.

Direktivet innehåller även följande definitioner och en bestämmelse om "rättslig verkan" för elektroniska signaturer:

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

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

- **avancerad elektronisk signatur:** en elektronisk signatur som
  a) är knuten uteslutande till undertecknaren,
  b)undertecknaren kan identifieras genom,
  c)är skapad med hjälpmedel som endast undertecknaren kontrollerar, och
  d)är knuten till en elektronisk handling på ett sådant sätt att alla efterföljande ändringar av den elektroniska handlingen kan upptäckas,

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

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

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

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

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

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

- **certifikatutfärdare:** den som utfärdar certifikat.

***”1 §** Syftet med denna lag är att underlätta användningen av elektroniska signaturer, genom bestämmelser om säkra anordningar för signaturframställning, om kvalificerade certifikat för elektroniska signaturer och om utfärdande av sådana certifikat. Lagen gäller sådana certifikatutfärdare som är etablerade i Sverige och som utfärdar kvalificerade certifikat till allmänheten.”*

Lag (2000:832) om kvalificerade elektroniska signaturer

I Sverige gäller sedan den första januari 2001, den nya lag (se ovan) där kvalificerade elektroniska signaturer likställs med pappersbaserade signaturer. Lagen, har kommit till för att avhjälpa den anonymitet som råder på Internet och innebär i stort sett två saker:

– Det ska nu gå att identifiera sig på Internet, att bevisa att man verkligen är den man utger sig för att vara.
– Denna underskrift är bindande – precis som en vanlig namnteckning.

Den nya lagen ska genomföra EU-direktivet om ett gemensamt ramverk för elektroniska signaturer. Lagförslaget skapar regler för de elektroniska signaturer som uppfyller vissa krav, så kallade kvalificerade signaturer. Detta ger en ökad tillit till elektroniska signaturer och skapar förutsättningar för en ökad användning av elektronisk kommunikation i samhället. För att en signatur ska vara kvalificerad måste den baseras på ett kvalificerat certifikat och vara skapad på ett säkert sätt, till exempel genom ett smart kort. I det kvalificerade certifikatet ska det bland annat anges vem som utfärdat certifikatet och hur länge det är giltigt. De nya kvalificerade elektroniska signaturerna ska accepteras inom EU, då samtliga medlemsstater kommer att ha en liknande lagstiftning baserad på samma EU-direktiv.

Denna lag, och det bakomliggande EU-direktivet, kommer att kompletteras med europeiska standarder. Utvecklingen av dessa standarder pågår och kommer att beröra regelverk för certifikatutfärdare, certifikatformat, godkänd utrustning för signering i användarens dator med mera. Ett kvalificerat certifikat kräver att de tillhörande privata nycklarna förvaras under användarens fullständiga kontroll. Detta kommer med mycket stor sannolikhet att innebära att det krävs ett säkert operativsystem, eller någon form av hårdvara, t.ex. ett aktivt kort för nyckelförvaring. S.k. mjuka certifikat kommer inte att uppfylla kraven.[19]

6 FALLSTUDIER

Vi kommer i detta kapitel beskriva hur elektroniska signaturer kan fungera i praktiken. Både genom att beskriva hur elektronisk signering används på Copenhagen Business School i Köpenhamn och hur vi själva har signerat och krypterat information. Det är alltså detta kapitel som är vår praktiska referensram för uppsatsen.

6.1 COPENHAGEN BUSINESS SCHOOL

Copenhagen Business School, CBS, i Köpenhamn CBS är Danmarks näst största utbildningsanstalt med över 14 000 studenter, 1 000 forskare och anställda samt 1 500 externa lärare. Under de senaste åren har skolan satsat hårt på att profilera sig inom IT. Studenter, forskare och lärare på CBS har tillgång till egna digitala signaturer. Tanken är att skolans studenter och personal nu ska kunna kommunicera säkert via Internet. Därmed är också CBS mycket tidigt ute med att integrera digitala signaturer i både studier och administration.

6.1.1 Pilotprojektet

CBS var en av de offentliga institutionerna som 1998 ingick i ett pilotprojekt med digitala signaturer, med stöd av det danska forskningsministeriet.
De generella bakomliggande målen för CBS elektroniska IT- lösningar var:

- En bättre och effektivare service.
- En markant högre grad av säkerhet.
- Rationalisering såväl tidsmässig som ekonomisk.
- En frigörelse från ”tid och plats”.
- En automatisering av tidigare manuella rutiner.

Dessa målsättningar skulle kunna infrias genom att införa elektroniska signaturer i arbetsvardagen för studerande, lärare, forskare och den administrativa staben. Syftet med pilotprojektet var att ge ut mjukvara och dela ut certifikat till en vald grupp studenter, som skulle skicka in sina kandidatuppsatser till CBS via e-post, förseglade med sina digitala signaturer. Syftet var således inte att utföra ett försök, utan att genomföra den ordinarie inlämningen av kandidatuppsatser genom att använda digitala signaturer. Det förekom således inte någon ”dubbel-inlämning”. Målen specifika för pilotprojektet var:

- Införandet av ett multifunktionellt studiekort (plastkort) med chips till certifikat, digitala signaturer och en betalnings funktion, som skulle fungera som studentens ID-kort.
- Inskickandet av examensuppsatser från studenterna till administrationen.
- Högre grad av säkerhet och användning av webbtjänster för självbetjäning
- Högre grad av säker elektronisk sakbehandling i administrationen och bland forskarna.

Skolans PKI-lösning hade som sagt sin utgångspunkt i smarta kort och ambitionen var att man skulle kunna införa ett multifunktionellt studiekort, som skulle rymma alla administrativa funktioner inklusive e-handel och digitala certifikat.

Det visade sig emellertid att de tekniska möjligheterna för ett multifunktionellt studiekort med ett inbyggt chips(smart kort), som utöver den digitala signaturen exempelvis kan innehålla e-handelsfunktioner, ännu inte är möjligt. Smarta kort var inte och skulle inte komma att bli den bärande delen av PKI-lösningen, utan var snarare att betrakta som ett appendix. Ett verktyg som ger PKI användarfördelar, snarare än en helomfattande lösning. Visionen med ”allt på ett kort” var med andra ord lite längre fram än verkligheten. Därför/därav reducerades målen till:

- Multifunktionella studiekort som ett självständigt projekt
- Digitala signaturer som ett självständigt projekt:
  - Inskickandet av examensuppgifter med elektroniska signaturer från studenterna
  - Säker e-post

CBS valde att koncentrera krafterna på att uppnå kraven på PKI-lösningens säkerhets och funktionella egenskaper. Det var inte bara CBS egna krav på säkerhet som skulle tillgodo ses utan även de krav forskningsministeriet hade satt upp, för att de skulle stödja projektet.
Forskningsministeriets bidrog finansiellt till projektet under förutsättningarna att den valda lösningen skulle uppfylla en rad krav och standarder för säkerheten i strukturen; en digital signatur med RSA och 1024 bits till signering, kryptering med 128 bitars nyckellängd, standardmässig överlåtelse av X-509 v 3 certifikat (ISO standard) och användandet av smarta kort. Alternativet till smarta kort var att förvara certifikatet på en diskett. Rent användarmässigt var det även viktigt att krypteringen och signering skulle fungera på de vanligaste filtyperna: Wordfiler, Excelfiler, textfiler och pdf.filer.

Med dessa krav som riktlinjer letade CBS efter ett digitalt signatursystem i en PKI-struktur, som skulle kunna integreras i både ”kontorsautomation” och webbmiljöer. Lösningen skulle kunna fungera tillsammans med existerande system på CBS. De bestod av Oracle databaser, Oracle Financial, både Microsoft och Netscape e-postklienter, NT och Unixservrar, Scanjour journalsystem och Firewall-1 från Checkpoint. Valet av PKI-system föll på Entrust, en kanadensisk produkt, som i Danmark representeras av Protect Data A/S, som därmed även blev en samarbetspartner såväl som ett bollplank i projektet.
CBS ställde från början ett krav, som inte ska frångås. Den digitala signaturen skulle också kunna användas av användarna, som fysiskt befinner sig utanför skolans lokaler. Det skulle vara möjligt för en student att fungera i studiemiljön, lämna in uppsatser, anmäla och avanmäla sig till tentamina osv. från sitt sommarhus på landet, från ett Internetkafé eller bara från det privata skrivbordet. Denna mobilitet och geografiska oberoende var en av de bärande delarna i konstruktionen och en av de saker som man från CBS sida ville kunna erbjuda sina studenter.

CBS hade från början intentionen att skapa en välkonstruerad intern infrastruktur, med hänsyn till säkerhetsnivå, kompetens, mjukvaror och personal.
Det bestod i praktiken av att man snabbt beslutade att uppnå en kompetens och säkerhetsnivå, som möjliggjorde installation och drift av en egen CA för att utfärda certifikat.
Det framstod vid uppstarten som den enda möjligheten, både administrativt och ekonomiskt, för att inarbeta digitala signaturer i CBS vardag.

Var och en av studenterna fick vid en föreläsning varsin CD med program och installationsvägledning på.(Vid utdelandet av CD:n kontrollerades varje students identitet).
Utöver CD fanns stöd och vägledning att få på skolans webbplats, www.adm.cbs.dk, med handledning över hur digitala signaturer fungerar och används. Utförliga instruktioner över hur själva inlämnandet går till, telefonnummer till en akut hjälplinje osv. Själva ”chipskorten” och kortläsarna för dessa smarta kort, valdes bort redan innan genomförandet. Det hade upplevts som ostabilt att använda dem och studenterna blev istället uppmanade att förvara sina krypteringsnycklar och profiluppgifter på sin dator eller om nödvändigt transportera dem på en diskett. Utöver den CD som studenterna fick för installationen av PKI-programmen på sin privata dator, installerades ett användarrum på skolan, där datorerna hade den nödvändiga mjukvaran. De berörda lärarna fick på samma sätt mjukvaran samt chipskort med tillhörande kortläsare.
PKI-lösningen testades i praktiken året därpå. Den 29 oktober 1999 skickade de 64 studenterna, i grupper om 2-3 st, in sina uppsatser, på maximalt 50 sidor plus bilagor. Endast en grupp kunde av tekniska skäl inte skicka in sin uppsats via e-post (de satt på en arbetsplats med en restriktiv brandvägg).

Uppsatserna var försedda med digitala signaturer och skickades via e-post till en för ändamålet upprättad e-postadress hos CBS sekretariat. Härifrån blev de, fortfarande försedda med digitala signaturer, dirigerade vidare till en databas för arkivering, där materialet lagrades, låst, utan att kunna ändras. Detta säkrade såväl tids och datumstämplingen som fungerade som en garanti för uppsatsens autencitetticitet om det av någon anledning skulle uppstå en tvist angående detta.
Hela ovanstående process är helautomatiserad och skedde utan något mänskligt ingripande.
Till studenterna skickades en kvittering på att uppsatsen blivit mottagit av signaturkontot. Kontot hade med andra ord fått ett eget certifikat med privata och offentliga nycklar. Denna kvittens sköttes dock manuellt av en av de anställda på skolans dataavdelning. Det undersöktes om det var möjligt att generera en automatisk svarsfunktion på ingående e-post(reply-funktionen), men det var inte omedelbart möjligt att kunna koppla på kontots signatur automatiskt

Uppsatsen blev sedan utskriven i ett exemplar, för att användas av studentens lärare.
Efter att läraren hade läst och utvärderat uppsatsen, fyllde denne i ett elektroniskt betygsblad, som med en digital signatur blev skickat till sekretariatet. Där skrevs sedan betyget in i en studentdatabas.

Reaktionen från studenterna var bra, men med vissa förbehåll, det var ju ett pilotprojekt.
Några menade att mjukvaran och lösningen hade blivit omodern, andra att det var en stressfaktor att lämna in sin examensuppsats på ett helt nytt sätt.
Men detta till trots, var det stora flertalet studenter nöjda och tyckte att de administrativa förbättringarna var bra, tack vare den digitala möjligheten att lämna in sin uppsats. Att de inte behövde skriva ut och posta eller lämna in uppsatsen på en speciell plats utan kunde sitta och skriva till sista minuten. Det visade sig även att många studenter lämnade in sina uppsatser fram på småtimmarna innan deadline.

6.1.2 Idag

Genomförandet av pilotprojektet på CBS medförde först och främst en inblick i de möjligheterna, att underlätta det administrativa arbetet, som uppnås genom att lägga ut en rad tjänster på nätverket, som tidigare endast kunde hanteras manuellt. Dels för att den nya digitala arbetsgången involverar färre mänskliga händer, dels för att arbetsgången går snabbar utan mänsklig inblandning. För studenterna del innebar det bl.a. att de inte behövde skriva ut och kopiera uppsatserna i flera exemplar.

Dessutom framhäver CBS att det är en pedagogisk aspekt på pilotprojektet och införandet av elektroniska signaturer i organisationen. Det har gett studenterna en bra introduktion till morgondagens teknik, som förr eller senare kommer att vara en standard i en eller annan form. Efter att pilotprojektet var avslutat började man diskutera hur man skulle gå tillväga för att utöka användandet av elektroniska signaturer. Man beslutade att det inte skulle bli någon utökning av möjligheten att lämna in sin examensuppsats elektroniskt. Anledningen var att det är en omöjlig lösning att låta skolans administration sköta utskrifterna av uppsatserna. Lärarna vill kunna läsa uppsatserna på papper och opponenterna vill kunna göra anteckningar. En eventuellt framtida lösning på problemet är att ”outsourca” utskrifterna, dvs. lägga ut dem på entreprenad, så att administrationen inte behöver skriva ut tusentals uppsatser varje termin.

Utvidgningen är istället inriktad på att effektivisera den administrativa delen för studenterna och skolans administration.
För studenternas del innebär det att göra skolans webbplats mer interaktiv. Det ska bland annat bli möjligt att anmäla sig till kurser och ändra sina uppgifter från webbapplikationen. Detta löses med en studentportal på skolans nuvarande webbplats. Härifrån kan studenterna få information om sina poäng och lästa kurser. Denna portal finns idag, men än så länge är det inte möjligt att ändra några privata uppgifter utan endast att läsa information, som kommer från skolans databaser. Idag loggar man in på portalen med hjälp av användarnamn och lösenord. När de elektroniska signaturerna är utdelade kommer det även vara möjligt att ändra sina personliga uppgifter och anmäla sig till kurser. Här ska även finnas virtuella klassrum och möjligheten att läsa på distans, att kunna skicka in sina uppgifter och PM säkert genom portalen.

Ett problem som man märkte tidigt i pilotprojektet var hanteringen och distributionen av de privata nycklarna. Det beslutade då att under pilotprojektet skulle dessa förvaras på studentens dator eller på en diskett. Men detta är ingen tillfredsställande lösning. Studenter och personal vill kunna använda sina signaturer oavsett var de befinner sig. Och att bära omkring på sina privata nycklar överallt är inte heller något att rekommendera.
Programtillverkaren Entrust har presenterat en lösning som de kallar Truepass. Denna lösning fungerar så att man kan komma åt sin privata nyckel oavsett var man befinner sig, förutsatt att man har tillgång till Internet. De privata nycklarna ligger lagrade på en server och via dubbel kryptering blir åtkomst möjlig oavsett var i världen användaren sitter med sin dator.

För administrationen har införandet, av elektroniska signaturer, bland annat lett till stora tidsbesparingar. Vid anställningen av ny personal, räknar CBS med att man sparar ungefär en veckans administrativt arbete, för varje anställd. När en anställning sker på CBS krävs att två olika personer från skolan vidimerar och undertecknar anställningskontraktet. Mallen för anställningskontrakt finns sedan tidigare i pdf-format. Innan fylldes kontraktet i direkt på skärmen men vid undertecknandet krävdes papperskopior. Även detta kan nu ske direkt på skärmen med hjälp av elektroniska signaturer. Varje signatur låses vid den specifika informationen vid signeringen. Detta innebär att skulle person två, lägga till information till kontraktet, syns detta eftersom det skiljer sig ifrån informationen knuten till person etts signatur. Även efter anställningen är det mycket administrativt arbete som underlättas. Skapandet av nya e-postadresser, interna utskick till de olika institutionerna o s v allt detta blir mycket enklare med den säkra digitala tekniken. Och detta är endast några exempel, för i en organisation med 15 000 människor är det administrativa flödet naturligtvis enormt.
CBS nästa stora vision är ett system, där endast ett säkert login behövs för datorn.

Anledningen till att vi inte tagit upp lärarnas aspekt av användandet av elektroniska signaturerna, är att lärarna inte använder elektronisk signering i någon större utsträckning. Än så länge är utvecklingen av elektronisk signering på CBS inriktad på att underlätta för administrationen och därmed indirekt för studenterna.

Vår egen signatur
För att lättare förstå och kunna sätta oss in i hur digitala signaturer skapas och hur den elektroniska signaturen sedan kan användas, fick vi ett eget certifikat, för att kunna skapa en signatur, från CBS (Vårt certifikat är kopplat till CBS egen CA.).

Annie Stahel lade in uppgifter om våra namn och e-postadresser, i CBS digitala signatur-system och skapade på så sätt ett certifikat som identifierar vilka vi är.
Systemet generade därefter ett referensnummer och en behörighetskod, som skulle användas vid skapandet av vår profil. För att kunna använda vår signatur fick vi, precis som studenterna i pilotprojektet, en CD-skiva med Entrust programvara och installationsvägledning.

Installationen av programvaran skedde på vår hemdator. Programvaruinstallationen genomfördes utan några problem, tack vare den medskickade installationsguiden på engelska.
För att skapa och använda vår signatur behövs en användarprofil. Vi startade upp den nyinstallerade programvaran och initierade proceduren att skapa en profil. Detta skulle göras med hjälp av det referensnummer och den behörighetskod som vi tidigare erhållit
Här blev det lite knepigare, eftersom instruktionerna var på danska och lite svåra att förstå. Efter några försök lyckades vi skapa en användarprofil.
För att vår CA (CBS) skulle kunna identifiera och verifiera vår profil, dvs. bekräfta att de inmatade uppgifterna stämde, var vi naturligtvis uppkopplade till Internet under hela proceduren.
För att kunna testa att använda vår signatur skickade vi ett e-post till Annie Stahel med en bifogad Wordfil. Innan vi bifogade filen valde vi att både signera och kryptera den. Genom att signera (dvs. kryptera kontrollsumman av innehållet i filen) med vår privata nyckel kunde Annie Stahel dekryptera kontrollsumman med vår publika nyckel (som finns i ett register, åtkomligt för alla anknutna till samma CA). Eftersom vi valde att även kryptera hela filens innehåll, använde vi oss utav Annie Stahels publika nyckel (som finns i ovanstående register). Detta innebar att endast hon kunde dekryptera filen med sin privata nyckel och på så sätt läsa filen. Annie Stahel svarade genom att skicka ett e-post, bifogat med en krypterad fil. På så sätt visade hon att vår e-post hade kommit fram och att hon kunde läsa vår krypterade fil.

Med tanke på hur säkerheten med elektroniska signaturer, var det relativt enkelt att installera och använda. Vi blev förvånade över hur snabbt det gick att installera och börja använda sig av sina egna elektroniska signaturer. Från det att vi började installationen av Entrust programvara tog det minde än en halvtimme innan vi kunde skicka och ta emot både signerade och krypterade filer.

7 ANALYS

Det här kapitlet inleds med att våra frågeställningar diskuteras och relateras till vår teoretiska och praktiska referensram. Kapitlet avslutas därefter med vår slutsats.

7.1 FRÅGESTÄLLNINGSANALYS

7.1.1 Vad finns det för problem med att identifiera sig över öppna nätverk i dag?

- E-postadresser, som kan användas som användarnamn, kan lätt spåras och lagras av andra och kan därför inte anses vara en säker identitetsform.

- Som användare är det idag svårt att kontrollera att obehöriga inte får tillgång personlig information som registrerat på olika webbplatser på Internet.

- Det finns ingen som är ytterst ansvarig för Internet, därmed ingen att vända sig till för att få garantier.

- Eftersom man inte erhåller någon kvittens kan mottagaren påstå att han/hon inte erhållit meddelandet, och om avsändaren ångrar sig kan denne påstå att han/hon inte sänt meddelandet.

- På Internet finns inget av det som vanligtvis ger autencitet som en signatur, en röst eller ett ansikte Detta leder till att det är mycket svårt att säkert veta att en person är den som han eller hon uppger sig vara.

- Ett stort problem är när data sänds över öppna nätverk t.ex. Internet som har miljoner datorer anslutna och där det inte finns någon garanti för integritet. Man kan inte lita på att någon obehörig har ändrat den data som en part sänder till en annan.

Idag är mycket av det administrativa arbetet på företag och organisationer datoriserat. Men på grund av ovanstående problem, hämmas utvecklingen och många av de arbetsuppgifter som skulle kunna förbättras genom att datoriseras och skötas elektroniskt, görs fortfarande manuellt. Copenhagen Business School, CBS, i Köpenhamn började man tidigt att överföra manuella rutiner till elektronisk form. Blanketter för olika ändamål, som anställningskontrakt, kursanmälan och adressändring lades in i elektroniska mallar(i Adobes pdf-format) som sedan kunde fyllas i direkt på datorskärmen.
På grund av den bristfälliga möjligheten att säkert identifiera avsändaren och mottagare samt risken för integritetsbrott, såväl mot den personliga informationen såväl som mot själva datan, kom inte datoriseringen längre. Följaktligen var man, för att kunna signera elektroniska blanketter, tvungen att skriva ut dem på papper och antingen posta dem eller själv lämna blanketten direkt till mottagaren.
Ett annan stort problem var utdelandet av nya e-postadresser. Även här var det den bristande möjligheten för säker identifiering och kontrollen av öppna nätverk som var den bakomliggande orsaken.

För att säkert kunna ge ut e-postadresser med tillhörande lösenord, var identifiering tvungen att ske visuellt. Studenter och lärare fick således komma till datoravdelningen och identifiera sig för att kunna få ut sina adresser och lösenord. På en arbetsplats med över 15 000 e-post-adresser, var detta givetvis en tidskrävande uppgift.

7.1.2 Vad är elektroniska signaturer och hur fungerar de rent tekniskt?

Elektroniska signaturer är data i elektronisk form som är fogade till eller logiskt knutna till ett elektronisk meddelande och som används för att kontrollera om innehållet härrör från den som framstår som undertecknare. Det bredare begreppet elektroniska signaturer, refererar till varje metod som leder till en försäkran av elektroniska meddelandens äkthet och med digitala signaturer menar man de metoder som uppfyller detta krav och baseras på asymmetrisk kryptering, där en säker verifiering kan uppnås. Asymmetrisk kryptering innebär att man använder två olika krypteringsnycklar, en publik och en privat.

De elektroniska signaturer, som vi valt att undersöka, använder sig av tekniken digitala signaturer. Syftet med en digital signatur är att användaren skall kunna ta ansvar för sin signering av ett elektroniskt dokument. För att säkerhetsställa att den grundläggande uppgiften, om vem ett nyckelpar tillhör, behövs en helt ny infrastruktur för publika nyckelsystem, med en engelsk term Public Key Infrastructure (PKI), där certifikat utgör en viktig pusselbit. Ett certifikat, utfärdat av en betrodd certifikatutfärdare (CA) styrker uppgifter om nycklarnas innehavare/ägare. En digital signatur ger uppgift om, att den som utfärdar signaturen är den som anges i certifikatet samt möjligheten att upptäcka om signerade data har förvanskats.

7.1.3 Hur används elektroniska signaturer i praktiken?

Uppenbara användningsområden för elektroniska signaturer är slutna system,
exempelvis företags lokala nät eller ett banksystem. Syftet med elektroniska signaturer är bland annat att underlätta för elektroniska handel och för dem som sänder information och andra avtalshandlingar i elektronisk form. Certifikat och elektroniska signaturer används också i auktoriseringssyften, t.ex. för att få tillgång till ett privat konto.
Elektroniska signaturer kan även användas för olika typer av säker kommunikation över publika nätverk t.ex. vid identifiering av användare eller för säker e-post. För dem som utnyttjar elektronisk signering privat handlar det i dagsläget kanske mest om att verifiera att e-post verkligen kommer från den som anges som/utger sig för att vara upphovsman. En elektronisk signatur verifierar att e-posten kommer från angiven upphovsman, eftersom signaturen är unik och kan inte replikeras. På CBS (Copenhagen Business School) är denna funktion viktig för att de administrativa uppgifterna ska kunna skötas elektroniskt. Exempelvis, om en student vill ha reda på sina betyg kan han eller hon använda sin elektroniska signatur för att få tillgång till skolans studentdatabaser.
Adobe stödjer ett antal olika standarder för digital signering i sitt format PDF (Portable Document Format). På CBS har detta underlättat t.ex. vid nyanställning genom att all administrativ behandling sker elektroniskt. Anställningskontraktet skapas som tidigare nämnts i en elektronisk mall i pdf-format.
Även signeringen kan nu ske elektroniskt innan kontraktet skickas med e-post över Internet. Kontraktet behöver på så sätt inte skrivas ut i pappersformat för att vara säkert identifierat. För att anmäla sig till skolans kurser kan studenterna laddar hem en anmälningsblankett från

skolans hemsida. Studenten kan sedan fylla i och signerar anmälan direkt på datorskärmen. Därefter skickas anmälan som en signerad bifogad fil med e-post till skolans antagningsenhet. Detta underlättar både för studenter och för skolans administration genom att registreringen och lagringen av anmälningen sker automatiskt, och sparar på så sätt både tid och pengar.

7.1.4 Är elektroniska signaturer en bra lösning till de tidigare identifierade problemen?

De fem första identifieringsproblemen kan alla lösas av enbart elektroniska signaturer.
Avlyssning av information upptäcks och möjligheten att agera i någon annans namn blir omöjlig eftersom varje person har en unik signatur som till skillnad från e-post, innehåller uppgifter om personen, exempelvis namn, personnummer och adress. När avsändaren signerar sin korrespondens med en elektronisk signatur kan mottagaren säkerställa, genom kontroll med en signerad publik nyckel, att brevet har rätt avsändare.
Elektroniska signaturer kan användas för att garantera informations ursprung. På så sätt kan alltid upphovsmannen identifieras. Denna signering gör att användaren med hjälp av en CA, kan verifiera att informationen har signerats av en specifik upphovsman. Webbläsare visar upp ett certifikat för användaren, som sedan får avgöra huruvida han eller hon litar på den här upphovsmannen och därigenom bestämma sig för att ladda ner informationen till sin dator.
Elektroniska signaturer ger alltså skydd mot flera av punkterna i säkerhetsmodellen, kapitel 3.4, alltså punkterna 1 – 4.

I många tillämpningar krävs dock att informationen skyddas mot insyn och då måste hela informationen krypteras. I de fallen används den elektroniska signaturen för att identifiera användaren och sedan krypteras informationen som överförs via nätet. Denna kombination löser ytterligare ett av identifieringsproblemen som vi tidigare nämnt och ger ett skydd mot de två avslutande punkterna i säkerhetsmodellen.

Istället för att använda sig av en PIN-kod för att identifiera ägaren av en elektronisk signatur, kan man användas sig av någon form av biometri, så som fingeravtryck eller scanning av ögats iris. För att lösa det sista av våra nämnda identifieringsproblem krävs alltså en kombination av elektroniska signaturer och biometriska lösningar.
Detta är mycket säkra metoder och idag är det omöjligt att förfalska en iris, vilket gör att kombinationen med elektroniska signaturer och iris-scanning är helt säker.

Vi tror att en utbredd användning av elektroniska signaturer för olika ändamål kommer att leda till att samhället får ett nytt sätt att skapa förtroende på, mellan såväl fysiska personer som organisationer. I och med den nya lagen om kvalificerade elektroniska signaturerna blir det nu möjligt att använda Internet till sådant man av integritets- och säkerhetsskäl tidigare inte har kunnat göra – till exempel skriva under ett lägenhetskontrakt. I takt med att användningen ökar kommer även olika verksamheters beroende av kvalificerade elektroniska signaturer att öka.
För att kunna utnyttja möjligheterna med elektronisk signering, tror vi att det är viktigt att man, som på CBS, även fokusera på de fördelar som kan skapas i form av ökad vinst, växande marknadsandelar, högre servicegrad eller minskade kostnader.

7.2 SLUTSATS

”Elektroniska signaturer leder till ökad integritet och säkerhet vid identifiering på Internet.”

Tack vare att vi har kunnat ta del av CBS (Copenhagen Business School) erfarenheter rörande elektroniska signaturer i praktiken och haft möjligheten att själva använda och se hur dessa signaturer fungerar, har vi kunna jämföra realiteten med teorierna.
Vi ser två viktiga aspekter för att elektronisk identifiering och signaturer skall fungera på ett tillfredsställande och säkert sätt. Det är för det första att måste man kunna komma åt och lita på den öppna nyckeln. Problemet, som vi ser det, ligger i om någon skulle vilja utge ge sig för att vara någon annan, för att exempelvis få tillgång till information eller kunna föra en kommunikation. Detta är nämligen i princip möjligt att göra, genom att framställa en publik nyckel på egen hand. Denna nyckel kan sedan knytas till önskvärd identitet. Lösningen till problemet, det vill säga att kunna garantera att den publika nyckeln tillhör den påstådda identiteten, är ett certifikat. Den andra aspekten är att man ska kunna lagra den privata nyckeln på ett bra och säkert sätt. För att den elektroniska signaturen ska komma till användning krävs att privata nyckeln är lättillgänglig och säker. Den bästa förvaringsmetoden anser vi att s.k. hårda certifikat utgör, framförallt EID-kort. Genom att integrera den privata nyckeln i ett redan etablerat ID-kort blir den elektroniska identiteten inte någon extra identitet skild från den fysiska utan bara ett nytt sätt att bevisa den.
Uppfylls dessa båda anser vi att identiteten kan säkerställas och därmed har vi verifierat vår hypotes. Elektroniska signaturer leder till ökad integritet och säkerhet vid identifiering på Internet.
Används elektroniska signaturer i kombination med kryptering, av information, ökar även den totala säkerheten vid transaktioner och kommunikation över öppna nätverk.

8 SLUTDISKUSSION

Det här kapitlet är en summering av våra erfarenheter. Slutligen ges förslag på framtida utredningar inom området.

Vi har arbetat med denna vetenskapliga uppsats under fem månader och det har varit en intressant och lärorik tid. Genom att skriva denna uppsats har vi fått en inblick i flera olika aspekter av både identifieringsproblematiken och Internetsäkerhet.
Slutsatsen vi kom fram till i uppsatsen var elektroniska signaturer leder till ökad integritet och säkerhet vid identifiering på Internet. Vi anser att vi har verifierat vår hypotes och besvarat vår frågeställning på ett intressant och bra sätt.

8.1 FÖRSLAG PÅ FRAMTIDA UTREDNINGAR

Elektroniska signaturer är ett väldigt stort ämne och undersökas ur andra synvinklar. Vi har ibland känt att vi skulle vilja undersöka någon del (i utkanten av vårt problemområde) ännu mer ingående men har av tid varit tvungna att begränsa oss. Några områden, skulle kunna vara, Vilken är den bästa lösningen för säkerhetsproblemen på Internet, jämföra olika metoder? Biometriska lösningar? Har användningen/utvecklingen av elektroniska signaturer ökat efter EU-direktivets ikraftträdande?

9 REFERENSFÖRTECKNING

9.1 BÖCKER

[3] Pfleeger Charles P; *Security in Computing*
Prentice Hall International Editions; 2000.

[4] Halvarsson, Andreas, Morin Tommy; *Elektroniska signaturer: e-affärer utan elände med identifiering, signering och kryptering;* Studentlitteratur; 2000.

[5] Svenning Conny, *Metodboken – samhällsvetenskaplig metod och metodutveckling*, Lorentz förlag, Höör, 1999

[6] Ekholm, Mats & Anders Fransson, *Praktisk intervjuteknik*, Norstedts Förlag, Stockholm, 1994

[7] Whitfield, Diffie & Susan Landau, *Privacy on the Line - The Politics of Wiretapping and Encryption***,** The MIT Press 1998

[11] Furberg Per; *Elektronisk dokumenthantering : en rättslig problemorientering*; Riksarkivet, 2000

[15] SIG Security, Studentlitteratur, Lund, 1999

[20] Betänkande av IT-utredningen;
Elektronisk dokumenthantering; SOU 1996:40.

Europaparlamentets och rådets direktiv 1999/93/EG, den 13 december 1999

Lag (2000:832) om kvalificerade elektroniska signaturer

9.2 ARTIKLAR OCH INTERNET

Computer Sweden, Informationweek.com och andra facktidskrifter relevanta för ämnet.

[1], *Hur skall andra kunna veta att Du är den som Du utger Dig för att vara på Internet?* http://www.polko.se/digisign.html, Leksén Bill

[2] *Elektronisk handel; Regeringens skrivelse 1997/98:190* http://naring.regeringen.se/propositioner_mm/skrivelser/pdf/EHANDE_Elektronisk_handel_9798190.pdf

[8] *Internet email, How does it work?: Check your privacy and security at the door,* http://www.reagoso.com/inet/em_secur.htm, David Hesprich

[9] *Privacy in Cyberspace: Is Your E-mail Safe/From the Boss, the SysOp, the Hackers, and the Cops?* http://www.aclu.org/issues/cyber/priv/privpap.html, Anna Beeson

[10] *Regeringsskrivelse, nr 1998:14* http://naring.regeringen.se/propositioner_mm/pdf/ds9814.pdf

[12] Internet: Risker och (o)säkerhet http://www.ida.liu.se/education/dist/it/TV6.ElPubSec.html Hjerppe Roland**,** Liblab, Inst. för Datavetenskap, Linköpings Universitet

[14] *Regeringskansliets referensgrupp för krypteringsfrågor*, Regeringskansliet, 1997/10

[16] *Hemlig brevväxling - så går den till,* White Paper - Säkerhet, Datateknik 3.0 Nr 6 november 1999, Nordling, Elias

[17] *Digitala signaturer - en teknisk och juridisk översikt* Dnr 1998/0507 Kommunikationsdepartementet

[18] *"Lag om kvalificerade elektroniska signaturer m m"* http://www.naring.regeringen.se/fragor/it/esign.htm, Regeringsproposition 1999/2000:117

[19] *Rapport 2000:15* http://www.rsv.se/skatter/rapporter/rapport20001123/samsetrapport_09_27.html#_Toc494765726 Riksskatteverket

[21] *Elektroniska signaturer och elektronisk identifiering* GEA Seminarierapport, Stockholm, 20010515

[22] *Namnteckningar är överlägsna elektroniska signaturer* Industri Standard nr 13 2001, Tunedal Per

[23] *Nu kan du skriva under papper på nätet*
http://www.aftonbladet.se/vss/it/story/0,2789,21294,00.html Aftonbladet, 20010101
Johan Furusjö

[24] SEIS, Säker Elektronisk Information i Samhället, www.seis.se

[25] *Elektroniska signaturer ingen säkerhetsgaranti - men F-Secure välkomnar Clintons nya lag,* http://www.f-secure.se/nyheter/nyhet.asp?Id=93, Hellqvist Per

[26] Europeiska gemenskapernas officiella tidning nr L 013 , 19/01/2000 s. 0012 – 0020

9.3 PERSONER

Döös Peter A, Telia Electronic Commerce, Stockholm

Stahel Annie, Copenhagen Business School, Köpenhamn

Svedin Ola, Precise Biometrics, Lund