

*Sammenfattende evaluering af
Forskningsministeriets
pilotprojekter om*

Digital Signatur

September 2000

Sammenfattende evaluering.....	5
Konklusion.....	5
Digital signatur hos offentlige myndigheder	6
Konkrete resultater af pilotprojekter	6
1. Indledning.....	7
Formålet med pilotprojekterne	7
Rapportens indhold.....	7
Kryptering og digital signatur	8
<i>Public-key kryptering</i>	9
<i>Certifikater</i>	11
<i>Betroet tredjepart og nøglecentre</i>	12
<i>Digital underskrift</i>	13
<i>Digitalt signeret dokument</i>	15
<i>Public-key Infrastructure</i>	16
Kryptering og digital signatur i praksis	17
<i>Nøglelængde</i>	17
<i>Kryptering og SSL</i>	18
<i>Digital signatur og elektronisk post</i>	20
<i>Secure Electronic Transactions</i>	21
<i>Software- eller smart card baserede løsninger</i>	22
Digital signatur og offentlige myndigheder	23
<i>Lov om elektronisk signatur</i>	24
<i>Offentlige initiativer omkring digital signatur</i>	24
2. Pilotprojekterne	25
Erhvervs- og Selskabsstyrelsen.....	25
<i>Projektets formål</i>	25
<i>Anvendelsen af digital signatur</i>	27
<i>Status</i>	28
<i>Opnåede resultater</i>	28
<i>Projektets videre forløb</i>	28
EU-direktoratet	29
<i>Projektets formål</i>	29
<i>Anvendelsen af digital signatur</i>	30
<i>Status</i>	31
<i>Opnåede resultater</i>	31
<i>Projektets videre forløb</i>	31
SU-styrelsen.....	32
<i>Projektets formål</i>	32
<i>Anvendelsen af digital signatur</i>	33
<i>Status</i>	35
<i>Opnåede resultater</i>	35
<i>Projektets videre forløb</i>	35
Handelshøjskolen	36
<i>Projektets formål</i>	36
<i>Anvendelsen af digital signatur</i>	37
<i>Status</i>	38
<i>Opnåede resultater</i>	38
<i>Projektets videre forløb</i>	39
Næstved Kommune	39

<i>Projektets formål</i>	39
<i>Anvendelsen af digital signatur</i>	41
<i>Status</i>	42
<i>Opnåede resultater</i>	43
<i>Projektets videre forløb</i>	43
Ringsted Kommune.....	43
<i>Projektets formål</i>	43
<i>Anvendelsen af digital signatur</i>	45
<i>Status</i>	46
<i>Opnåede resultater</i>	47
<i>Projektets videre forløb</i>	47
Vordingborg Kommune	47
<i>Projektets formål</i>	47
<i>Anvendelsen af digital signatur</i>	49
<i>Status</i>	49
<i>Opnåede resultater</i>	50
<i>Projektets videre forløb</i>	50
Århus Amt	50
<i>Projektets formål</i>	51
<i>Anvendelsen af digital signatur</i>	51
<i>Status</i>	52
<i>Opnåede resultater</i>	52
<i>Projektets videre forløb</i>	52
3. Sammenfattende evaluering	53
Forskningsministeriets formål med pilotprojekterne.....	53
Målgruppe og løsningstype	53
<i>Målgruppe</i>	54
<i>Løsningstype</i>	54
<i>Serviceforbedringer og rationaliseringsgevinster</i>	56
<i>Løsningens opbygning</i>	57
Løsningens omfang	58
<i>Antal pilotbrugere</i>	58
<i>Pilotperiode</i>	59
<i>Generelle brugervurderinger</i>	60
<i>Årsag til brugerfrafald</i>	60
Udvikling og drift.....	61
<i>Udviklingserfaringer</i>	61
<i>Installations- og driftserfaringer</i>	62
Teknologi og standarder.....	64
<i>Anvendte teknologier</i>	64
<i>Standarder</i>	66
<i>Certifikater og deres anvendelser</i>	66
Løsningernes fremtidige anvendelse.....	67
<i>Løsningens fortsatte eksistens</i>	67
<i>Forudsætning for udbredelse af digital signatur</i>	69
<i>Robusthed for teknologisk udvikling</i>	69
4. Resultater, erfaringer og problemstillinger	71
Formål med pilotprojekter	71
<i>Brug af digital signatur hos offentlige myndigheder</i>	71
<i>Udvikling af produkter og tjenester</i>	72
<i>Udvikling af standarder og protokoller</i>	73
<i>Delkonklusion</i>	73

Erfaringer fra pilotprojekterne.....	74
<i>Integration af systemer.....</i>	74
<i>Organisatorisk implementering</i>	74
<i>Lovmæssige aspekter.....</i>	75
Åbne problemstillinger.....	76
<i>Interoperabilitet</i>	76
<i>Tekniske barrierer.....</i>	79
<i>Behov for yderligere standarder</i>	80
<i>Finansiering af løsninger med digital signatur.....</i>	80
<i>Flere ydelser med digital signatur</i>	81
<i>Problemstilling ved mistet privat nøgle til kryptering.....</i>	82
5. Digital signatur i fremtiden.....	83
Tendenser og udvikling for digital signatur.....	83
<i>Analyser og forudsigelser</i>	83
<i>Anvendelse af digital signatur i andre sektorer</i>	83
<i>Andre lande.....</i>	84
<i>Standardiseringsarbejde.....</i>	84
Indsatsområder	86
<i>Sikker datakommunikation mellem offentlige myndigheder.....</i>	86
<i>Offentlige initiativer.....</i>	87
<i>Fortsættelse af pilotprojekter.....</i>	87
<i>Informationskampagne</i>	88
<i>Finansiering af løsninger til offentlige myndigheder.....</i>	88
<i>Fortsættelse af standardiseringsarbejde.....</i>	89
Bilag 1: Indkaldelse af forslag til projekter.....	90
Udkast til indkaldelse af pilotprojekter.....	90
Krav om standarder	92
Bilag 2: Høring om digital signatur.....	99
Sikring af interoperabilitet i løsninger.....	99
Finansiering af digital signatur	99
Transaktionsmængde.....	100
Teknik.....	100

Sammenfattende evaluering

Forskningsministeriet igangsatte pilotprojekter om digital signatur i 1998 på et tidspunkt, hvor offentlige myndigheder ikke havde erfaringer med brugen af digital signatur, og antallet af produkter og tjenester i markedet var lille. Formålet med projekterne var, at:

- Udbrede brugen af digital signatur hos offentlige myndigheder.
- Stimulere udviklingen af produkter og tjenester i markedet.
- Udarbejde nødvendige standarder og protokoller.

Som det belyses i de efterfølgende afsnit, er alle disse formål blevet opfyldt.

Konklusion

Da pilotprojekterne startede, var teknologien forholdsvis ny og der eksisterede kun få praktiske erfaringer med anvendelse af digital signatur hos offentlige myndigheder.

Pilotprojekterne har tilvejebragt en stor mængde praktisk viden og klart demonstreret, at anvendelse af digital signatur hos offentlige myndigheder er mulig.

Brugernes tilfredshed med de udviklede løsninger har generelt været stor. Brugen af digital signatur muliggør udbydelse af en række serviceydelser via Internettet som ellers ikke ville være mulig.

De fleste brugere mener, at Internettet som adgangskanal til offentlige myndigheder er en væsentlig servicegevinst.

Pilotprojekterne har dog også vist, at der stadig eksisterer en række barrierer som skal overvindes, før digital signatur kan anvendes bredt. De væsentligste problemer har været manglende kendskab til digital signatur og tekniske vanskeligheder ved installation og konfiguration af løsningerne.

Den teknologiske udvikling vil mindske omfanget af tekniske problemer, og informationskampagner kan oplyse befolkningen om sikkerhed og brug af digital signatur.

Erfaringerne fra de deltagende offentlige myndigheder har generelt været gode. Alle deltagere har identificeret mulighed for rationaliseringsgevinster og serviceforbedringer. Projekterne viser dog også, at indførelse af løsninger med digital signatur på Internettet er kompliceret og kræver spidskompetence.

På tre områder har pilotprojekterne ikke helt levet op til forventningerne. Antallet af pilotbrugere har ikke været så højt som planlagt tillige med, at pilotperioden for flere projekter har været kort, og projekterne har kun i ringe omfang afprøvet interoperabilitet mellem løsningerne.

Der er dog intet, der indikerer, at de fundne resultater og erfaringer ville have været anderledes, hvis antallet af pilotbrugere havde været større. Der er stadig åbne problemstillinger omkring interoperabilitet af løsningerne og PKI.

Digital signatur hos offentlige myndigheder

Forskningsministeriet har med pilotprojekterne igangsat brugen af digital signatur i Danmark. Løsningerne i Næstved Kommune, Ringsted Kommune, Vordingborg Kommune, i Århus Amt og hos Erhvervs- og Selskabsstyrelsen er i permanent drift. Nogle løsninger er endda ved at udvide brugergruppen. Dette er eksempelvis tilfældet med løsningen udviklet i Århus Amt.

Samtidigt har pilotprojekter medvirket til, at der nu eksisterer et antal produkter og tjenester til PKI på det danske marked.

Ved at igangsætte en række nye initiativer de kommende år, kan udbredelsen og anvendelsen af digital signatur fortsat stimuleres. Udvikling af disse initiativer kan drage stor nytte af de erfaringer, som pilotprojekterne har tilvejebragt.

Konkrete resultater af pilotprojekter

Sammenfattende har pilotprojekterne resulteret i følgende:

- Der er udviklet et antal produkter og løsninger, der nu er tilgængelige på det danske marked.
- Der er etableret et antal nøglecentre på det danske marked.
- Der er fastlagt et antal standarder for brug af digital signatur i offentlige forvaltninger.
- Flere offentlige myndigheder har implementeret og udbyder tjenester, der anvender digital signatur.
- Der er oparbejdet en væsentlig viden og kompetence omkring brug af digital signatur hos offentlige og private organisationer i Danmark.

1. Indledning

Forskningsministeriet igangsatte i 1998 ni projekter om digital signatur hos offentlige myndigheder i Danmark. De otte projekter er nu afsluttet. Nærværende rapport er en sammenfattende evaluering af disse otte projekter.

Formålet med pilotprojekterne

I 1998 opfordrede Forskningsministeriet offentlige myndigheder i Danmark til at indgive forslag til pilotprojekter om digital signatur. Situationen i Danmark var på det tidspunkt, at Forskningsministeriet ønskede at igangsætte og stimulere brugen af digital signatur i den offentlige forvaltning, men at der ikke eksisterede produkter eller tjenester på det danske marked. Ved hjælp af pilotprojekterne ønskede Forskningsministeriet at "kick-starte" brugen af digital signatur.

Forskningsministeriets generelle formål med pilotprojekterne var:

- At fremme opbygningen af et universelt Public Key Infrastruktur, herunder
 - Etablering af konkurrencedygtige nøglecentre
 - Udvikling af et marked for sikre produkter til generering og verifikation af digital signatur
 - Fastlæggelse af nødvendige tekniske standarder og protokoller
- At få det offentlige i gang med at bruge digital signatur i den elektroniske betjening af borgere og virksomheder
- At indhøste erfaringer til brug for lovgivningsarbejdet omkring elektronisk signatur.

Forskningsministeriet valgte at medfinansiere pilotprojekterne med 15 mio. kr., hvoraf otte er blevet gennemført. Et projekt blev ikke afsluttet af grunde, der ikke kan tilskrives forhold omkring anvendelsen af digital signatur.

Sideløbende med pilotprojekternes gennemførelse er der udarbejdet et antal konkrete forslag til standarder og protokoller. Dette arbejde er primært gennemført i Forum for Digital Signatur.

Pilotprojekterne og standarder for digital signatur er beskrevet på Forskningsministeriets hjemmeside på adressen http://www.fsk.dk/cgi-bin/theme-list.cgi?theme_id=7471.

Rapportens indhold

Denne rapport er udarbejdet af Andersen Consulting for Forskningsministeriet i perioden 15. maj 2000 til 30. juni 2000.

Evalueringen er primært baseret på de enkelte projekters slutrapporter. Den 8. juni 2000 afholdte Forskningsministeriet en fælles høring med deltagelse af alle pilotprojekter, leverandører og andre interessenter. På høringen blev resultaterne fra de enkelte pilotprojekter præsenteret og diskuteret. Høringen indeholdt også en diskussion, hvor en række centrale spørgsmål blev debatteret.

Indholdet af rapporten er som følger. Kapitel 1 introducerer digital signatur og den bagvedliggende teknologi. I kapitel 2 præsenteres de 8 pilotprojekter kort med beskrivelse af projektets formål, brug af digital signatur og opnåede resultater. I kapitel 3 gives en sammenfattende fremstilling af pilotprojekterne og væsentlige ligheder og forskelle fremhæves. I kapitel 4 vurderes projekternes resultater i forhold til Forskningsministeriets formål med igangsættelse af projekterne. I kapitel 5 angives på baggrund af pilotprojekternes erfaringer og resultater et antal strategiske indsatsområder.

Kryptering og digital signatur

Internettet er essentielt et åbent netværk, hvor dokumenter normalt sendes som klar tekst. Dette har som konsekvens, at når to personer udveksler information, så kan tredjepart principielt opsnappe indholdet. Tredjepart kan også udgive sig for at være den ene af de to kommunikerende parter, og sende "falsk" information til den anden part.

Hvis for eksempel en person sender en elektronisk post til sin bank med en anmodning om at overføre et beløb fra en bankkonto til en anden, så kan tredjepart ændre den elektroniske post og derved få banken til at overføre pengene til bedragerens bankkonto. Ikke alene risikerer bankkunden, at tredjepart kan se fortrolige oplysninger (eksempelvis kontonummer) men også banken løber en risiko ved transaktionen. Banken kan nemlig ikke være sikker på, at den elektroniske post virkelig kommer fra den person, som tilsyneladende er afsender og banken kan heller ikke være sikker på, at posten ikke er blevet ændret undervejs på Internettet.

Løsningen på disse to problemer er *kryptering* og *digital signatur*.

Ved kryptering af et dokument gøres teksten ulæselig for tredjepart. Ved dekryptering af dokumentet gøres teksten læsbar igen.

En digital signatur er ækvivalent til en håndskreven underskrift på et papir og sikrer:

- *Autenticitet*: Den digital signatur autentificerer underskriveren, eksempelvis ved navn og adresse.
- *Uafviselighed*: Den digitale underskrift gør, at underskriveren ikke kan afvise dokumentets oprindelse.
- *Integritet*: Den digitale underskrift garanterer modtageren af

dokumentet, at teksten ikke er blevet ændret undervejs fra afsender til modtager.

I den offentlige debat anvendes begreberne "elektronisk signatur" og "digital signatur" ofte i flæng. Elektronisk signatur er en generel betegnelse for en metode eller algoritme til elektronisk underskrivelse af et dokument. Digital signatur refererer til en specifik metode baseret på "public-key"-kryptering.

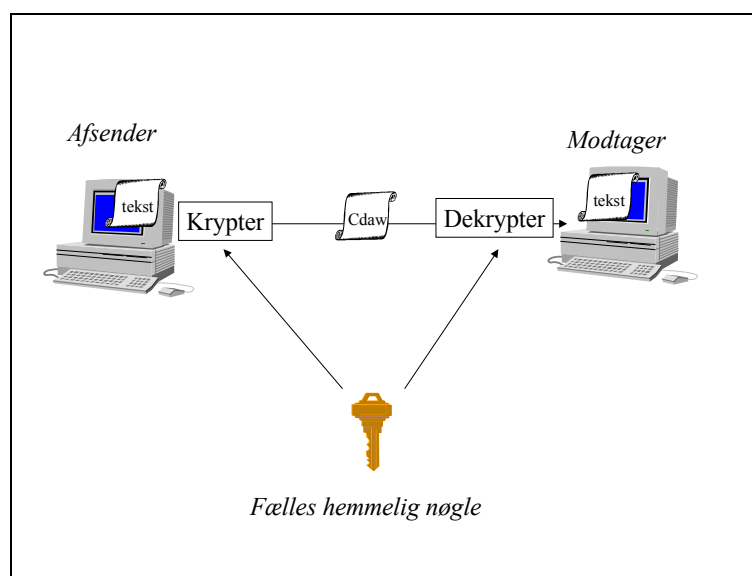
Digital signatur og kryptering af et dokumentets indhold opfattes tit som relaterede, men dette behøver ikke at være tilfældet. Der er intet i vejen for, at dokumenter forsynes med en digital signatur uden at være i krypteret form. Herved kan en eventuel tredjepart læse indholdet af dokumentet, men modtageren kan stadig være sikker på, at dokumentet virkelig stammer fra den påståede afsender, og at dokumentet ikke er blevet ændret undervejs fra afsenderen til modtageren.

Public-key kryptering

Når to personer skal udveksle et hemmeligt dokument over et åbent netværk, er det nødvendigt at kryptere dokumentet, så indholdet ikke kan læses af uvedkommende. Kryptering implementeres ved hjælp af en krypteringsalgoritme der specificerer, hvordan teksten gøres ikke-læsbar (krypteres) og læsbar igen (dekrypteres).

Krypteringsalgoritmer kan opdeles i to hovedkategorier: Algoritmer baseret på en *fælles hemmelig nøgle* (secret-key), og algoritmer baseret på *offentlig/privat nøgle* (public-key).

Når to personer udveksler et dokument, som er krypteret med en fælles hemmelig nøgle, sker det som vist i figuren nedenfor.



Kryptering med fælles hemmelig nøgle

Fremgangsmåden er:

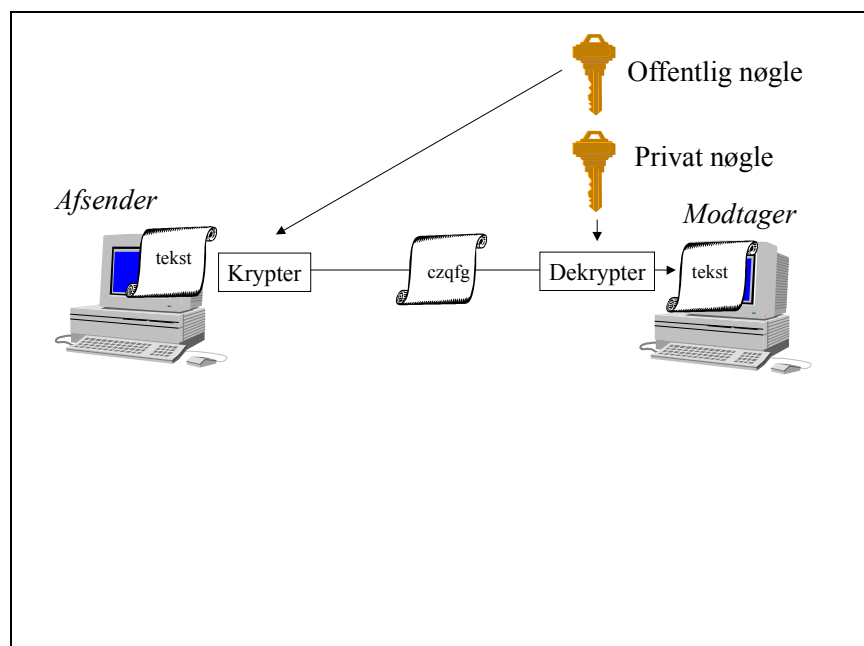
1. Afsenderen bruger den fælles hemmelige nøgle til at kryptere dokumentet.
2. Det krypterede dokument sendes via Internettet til modtageren. Teksten er ulæselig for alle, som ikke kender den fælles hemmelige nøgle.
3. Modtageren dekrypterer dokumentet ved hjælp af den fælles hemmelige nøgle.

Udveksling af en fælles hemmelig nøgle er problematisk på et åbent net, så som Internettet. Afsenderen kan eksempelvis ikke blot sende den hemmelige fælles nøgle til modtageren som elektronisk post, da en tredjepart derved kan opsnappe nøglen.

Ved at bruge en krypteringsalgoritme baseret på en offentlig/privat-nøgle, behøver afsender og modtager ikke udveksle en fælles hemmelig nøgle.

Et offentlig/privat-nøglepar har den egenskab, at et dokument krypteret med en offentlig nøgle kun kan dekrypteres med den tilsvarende private nøgle - og omvendt. Hver person har således to nøgler, hvoraf den private nøgle kun er ejermænden bekendt, mens den offentlige nøgle gerne må kendes af alle, og kan publiceres via Internettet i en nøgle-adressebog.

Udveksling af et dokument med kryptering baseret på offentlig/privat nøgler er illustreret i figuren nedenfor.



Kryptering med offentlig/privat nøgle

Fremgangsmåden er:

1. Afsenderen krypterer dokumentet med modtagerens offentlige nøgle.
2. Det krypterede dokument sendes via Internettet til modtageren.
Teksten er ulæselig for alle, som ikke kender den private nøgle, der hører til den offentlige nøgle – og det gør kun modtageren.
3. Modtageren dekrypterer dokumentet med sin private nøgle.

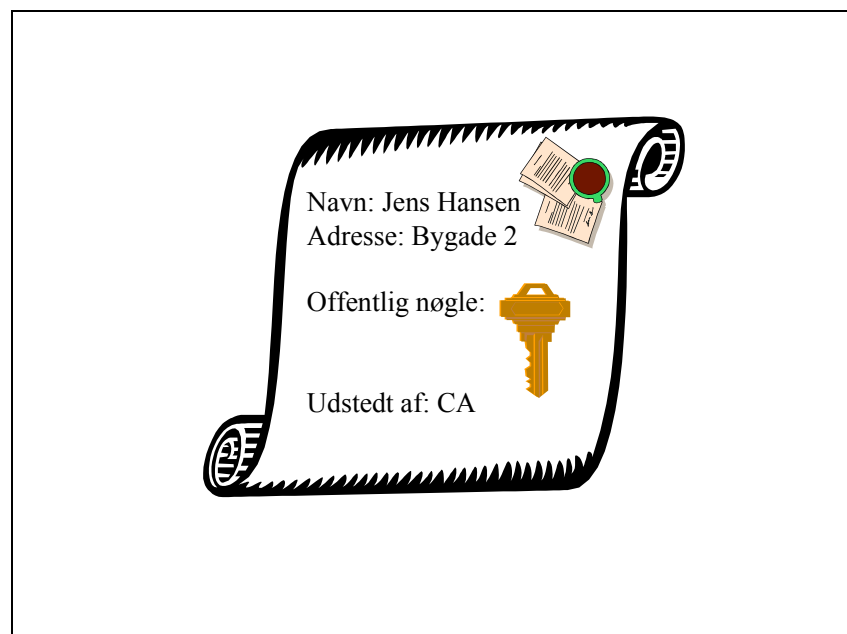
Parterne kan være sikre på, at kun modtageren kan læse dokumentet, idet kun modtagerens private nøgle kan dekryptere beskedens indhold.

En forudsætning for metoden er naturligvis at afsenderen er sikker på, at det virkelig er modtagerens offentlige nøgle, som han anvender ved krypteringen. Hvis en bedrager kan få "overbevist" afsenderen om at anvende sin nøgle, i stedet for modtagerens offentlige nøgle, så kan bedrageren dekryptere beskeden (med sin private nøgle), mens den tænkte modtager ikke kan læse beskeden (hvis han overhovedet får den).

Afsenderen skal altså på en eller anden måde kunne overbevise sig om, at det virkelig er modtagerens offentlige nøgle, som afsenderen anvender ved krypteringen. Dette kan ske ved at offentlige nøgler knyttes til certifikater, der entydigt identificerer ejeren af en offentlig nøgle.

Certifikater

Et certifikat er en relation mellem en person, medarbejder, virksomhed eller organisation og en offentlig nøgle. Et certifikat udstedes af et nøglecenter (*Certificate Authority - CA*).



Certifikat

Certifikatet indeholder blandt andet oplysninger om personens navn (i

tilfælde af et personcertifikat), tilhørssted, og gyldighedsperiode.

Certifikater til brug for public-key kryptering er standardiseret af International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) og ISO. Den første version af standarden, X.509 blev publiceret i 1988. Den nuværende version 3, X.509v3 blev frigjort i juni 1996.

Standarden specificerer indholdet af et X.509-certifikat. Certifikater skal blandt andet indeholde versionsnummer, serienummer, identifikation af anvendt krypteringsalgoritme, udsteder og den offentlige nøgle. Herudover er der et antal udvidelsesfelter, der kan anvendes efter behov. Et udvidelsesfelt kan angives til at være obligatorisk eller valgfrit. Hvis et felt er obligatorisk, skal et system, der behandler certifikatet, læse indholdet i feltet. Hvis feltet ikke er udfyldt, er certifikatet ikke gyldigt. Hvis feltet er valgfrit, kan systemet blot ignorere feltet.

Et certifikat har naturligvis kun værdi for en anvender, hvis han har tillid til certifikatets ægthed.

I den fysiske verden kan man skabe tillid til et dokument, hvis en betroet tredjepart står inde for dokumentets ægthed. Dette er til eksempel tilfældet, når vitterlighedsvidner eller en notar underskriver et dokument og derved står inde for dokumentets ægthed.

I den digitale verden kan den betroede tredjepart underskrive dokumentet digitalt – det vil sige forsyne certifikatet med en *digital signatur*.

Betroet tredjepart og nøglecentre

I den fysiske verden er der ofte behov for at kontrollere identiteten af en person, eksempelvis i forbindelse med udlevering af en pakke på posthuset. En ofte anvendt fremgangsmåde er, at postmedarbejderen kontrollerer modtagerens identitet ved hjælp af en pålidelig, betroet tredjepart. Eksempelvis kan postmedarbejderen bede modtageren om at fremvise sit pas. Hvis modtageren kan fremvise et tilsyneladende uforfalsket pas, stoler postmedarbejderen på at modtageren virkelig er den modtageren siger han er, da postmedarbejderen stoler på pasmyndighederne. Ved at undersøge passets udformning med hensyn til papir, stempel, underskrift, gravering m.m. kan postmedarbejderen overbevise sig om, at passet ikke er forfalsket.

I den digitale verden kan en betroet tredjepart – et nøglecenter - ligeledes fremstå som garant for, at en offentlig nøgle virkelig tilhører en given person, ved at "underskrive" et certifikat.

Hvis man som anvender er i tvivl om et certifikats gyldighed, kan man henvende sig til nøglecenteret (udstederen af certifikatet) og bede om status på certifikatet. Normalt vil nøglecenteret svare, at certifikatet er

gyldigt (det vil sige at nøglen på certifikatet virkelig tilhører personen, medarbejderen, virksomheden etc. som angivet på certifikatet), men undtagelsesvis kan nøglecenteret afvise gyldigheden af certifikatet. Dette kan for eksempel være tilfældet, hvis den private nøgle hørende til den offentlige nøgle på certifikatet bliver kompromitteret (og den tilsvarende offentlige nøgle derfor ikke længere må anvendes til kryptering af meddelelser), eller hvis en medarbejder ophører med at arbejde for et firma og derfor ikke længere kan underskrive på vegne af firmaet.

Ved hjælp af en betroet tredjepart og et certifikat kan man altså kryptere en besked til en anden person og føle sig sikker på, at kun denne person kan læse beskeden. Den betroede tredjepart står inde for, at den offentlige nøgle på modtagerens certifikat virkelig tilhører modtageren og det er jo kun modtagerens private nøgle, som kan dekryptere beskeden.

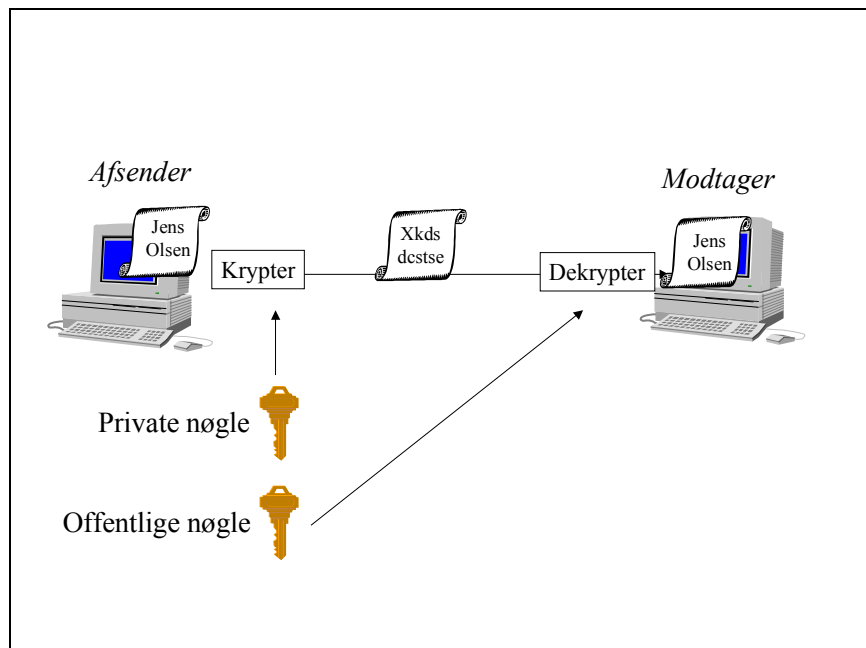
Digital underskrift

Ved brug af certifikater og en betroet tredjepart kan en afsender sende en fortrolig besked til en modtager og have tillid til, at kun modtageren kan læse beskeden.

Modtageren af en besked har dog ingen sikkerhed for, at beskeden virkelig kommer fra den påståede afsender. Alle har jo adgang til modtagerens offentlige nøgle og kan i princippet sende beskeder til modtageren i en andens navn.

I den fysiske, papirbaserede verden vil modtageren føle sig overbevist om beskedens oprindelse, såfremt beskeden er underskrevet af afsenderen. I visse tilfælde er beskedens oprindelse og indhold ligefrem bekræftet af betroet tredjepart, eksempelvis vitterlighedsvidner eller en offentlig notar. Hvis beskeden ikke ser "ændret" ud, for eksempelvis ved, at noget tekst er skrevet med en anden skrift, kan modtageren blive overbevist om, at beskeden ikke er blevet modificeret under transporten fra afsenderen til modtageren.

I den digitale verden kan en meddelelses oprindelse og integritet sikres med en digital underskrift. Hvis afsenderen krypterer noget tekst med sin private nøgle (eksempelvis sit navn), kan modtageren dekryptere "underskriften" med afsenderens offentlige nøgle og se, om navnet er det forventede.



Digital signatur

Modtageren kan nu verificere beskedens oprindelse på følgende måde:

1. Først henter modtageren den forventede afsenders certifikat. På certifikatet findes afsenderens offentlige nøgle og den betroede tredjepart står inde for, at det virkelig er den forventede afsenders offentlige nøgle.
2. Modtageren dekrypterer beskeden med den offentlige nøgle.
3. Hvis dekryptering giver den forventede tekst, er der stor sandsynlighed for, at det virkelig var afsenderen, der genererede signaturen – kun afsenderen har jo adgang til den private nøgle, som matcher den anvendte offentlige nøgle.

En bedrager kan ikke lave en falsk underskrift, med mindre han har adgang til personens private nøgle.

Modtageren kan hente afsenderens offentlige nøgle ved at henvende sig til den betroede tredjepart og anmode om afsenderens certifikat. (I praksis vil fremgangsmåden være, at afsenderen medsender sit certifikat til modtageren, der så kontrollerer certifikatets gyldighed, se nedenfor.)

Modtageren kan så være sikker på, at beskeden virkelig stammer fra afsenderen.

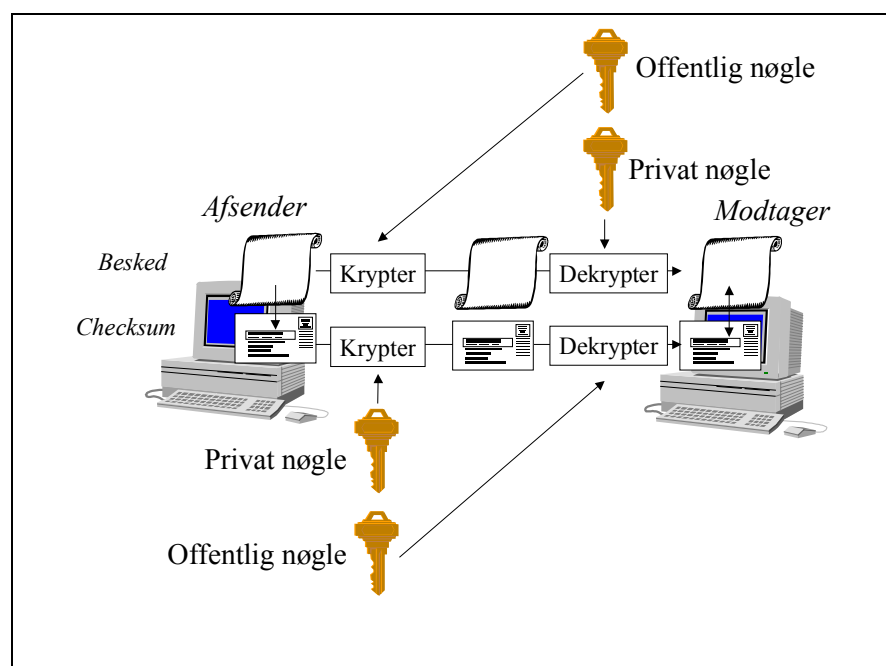
Modtageren kan derimod ikke være sikker på, at en bedrager ikke har modificeret beskeden undervejs. Eksempelvis kan bedrageren ændre lidt på den krypterede besked, således at den dekrypterer til en anden tekst end den afsendte.

Dette kan undgås ved at afsenderen sender en signeret checksum

(“message digest”) af dokumentet til modtageren. En checksum har den egenskab, at hvis teksten ændres blot en lille smule, ændrer checksummen sig radikalt. Efter at have dekrypteret beskeden fra afsenderen, kan modtageren beregne beskedens checksum og sammenligne denne med checksummen, beregnet af afsenderen. Hvis de ikke stemmer overens, er beskeden med stor sandsynlighed blevet ændret undervejs mellem afsenderen og modtageren.

Digitalt signeret dokument

Den komplette fremgangsmåde for fremsendelse af en fortrolig besked med en digital signatur er illustreret i figuren nedenfor.



Krypteret dokument med digital signatur

Afsenderen gør følgende:

1. Beregner beskedens checksum (i ikke-krypteret form) og krypterer checksummen ved hjælp af sin private nøgle. Kun afsenderens offentlige nøgle kan nu dekryptere checksummen til den rigtige værdi. Afsenderens offentlige nøgle er tilgængelig via afsenderens certifikat, og certifikatet relaterer nøglen med personen.
2. Henter modtagerens certifikat (offentlige nøgle) via nøglecenteret og krypterer beskeden med modtagerens offentlige nøgle. Nu kan kun den tilsvarende private nøgle (som kun modtageren har) dekryptere beskeden.
3. Sender den krypterede besked, den krypterede checksum og sit certifikat til modtageren.

For at læse beskeden gør modtageren følgende:

1. Kontrollerer afsenderens certifikat ved at kontakte nøglecenteret. I praksis sker kontrollen ved, at modtageren først kontrollerer nøglecenterets digitale signatur på certifikatet og dernæst spørger nøglecenteret, om certifikatet fortsat er gyldigt.
2. Dekrypterer beskeden med sin private nøgle.
3. Dekrypterer beskedens checksum med afsenderens offentlige nøgle (som modtageren har fra afsenderens certifikat).
4. Beregner beskedens checksum og sammenligner den med checksummen beregnet af afsenderen. Hvis checksummerne stemmer overens, er det usandsynligt, at beskeden er blevet ændret undervejs fra afsenderen til modtageren.
5. Samtidig ved modtageren med stor sandsynlighed, at beskeden virkelig kommer fra afsenderen, idet det er usandsynligt, at en anden nøgle end afsenderens private nøgle ville kryptere checksummen til netop den værdi, der fremkommer når checksummen dekrypteres med afsenderens offentlige nøgle.

Brugen af digital signatur og kryptering sikrer altså at :

- Parterne ved, at kun den tænkte modtager kan læse beskeden.
- Modtageren ved, at beskeden virkelig stammer fra afsenderen.
- Modtageren ved, at beskeden ikke er blevet ændret undervejs.

I praksis sker krypteringen af beskeden ved hjælp af en fælles hemmelig nøgle, der sendes krypteret fra afsenderen til modtageren ved hjælp af modtagerens offentlige nøgle. Dette sker af beregningsmæssige hensyn, idet kryptering med en algoritme baseret på en hemmelig nøgle er væsentlig hurtigere en kryptering baseret på offentlig/privat nøgler.

Public-key Infrastructure

Som beskrevet ovenfor, er at antal komponenter og tjenester nødvendige for brug af public-key kryptering og digital signatur. Et public-key infrastructure (PKI) etablerer den infrastruktur, der gør det muligt for en afsender at sende et digital signeret dokument til en modtager.

Et PKI består blandt andet af:

- En *Certificate Authority* (CA / nøglecenter), der fungerer som betroet tredjepart. Nøglecenteret udsteder certifikater og verificerer ægtheden af certifikater på anmodning.
- En *Local Registration Authority* (LRA), som verificerer identiteten af en person, medarbejder, eller virksomhed i forbindelse med udstedelse af et certifikat.
- Nødvendig hardware og software til at ovenstående to funktioner kan automatiseres.

Et public-key infrastructure er naturligt tæt forbundet med nøglecenteret

(CA). Der er dog intet til hinder for, at der eksisterer flere nøglecentre samtidigt, som alle udsteder certifikater. En konsekvens af dette er, at et nøglecenter kan blive anmodet om at verificere gyldigheden af et certifikat udstedt af et andet nøglecenter. Dette er det såkaldte *interoperabilitets* problem. Hvis et nøglecenter ikke kan verificere gyldigheden af et certifikat udstedt af et andet nøglecenter, er PKI'erne ikke interoperable. En typisk årsag til, at et nøglecenter ikke kan verificere gyldigheden af et "fremmed" certifikat er brugen af udvidelsesfelter. Hvis det andet nøglecenter anvender obligatoriske udvidelsesfelter, som det første nøglecenter ikke kender til, kan det første nøglecenter naturligvis ikke stå inde for certifikatets gyldighed, og må følgelig afvise det.

Kryptering og digital signatur i praksis

Kryptering og digital signatur er allerede - i en vis udstrækning - del af de standardprodukter, der typisk er installeret på en PC. For eksempel understøtter Microsoft Internet Explorer og Netscape Communicator både kryptering og digital signatur. Der er dog nogle begrænsninger.

Nøglelængde

De fleste krypteringsalgoritmer er teoretisk set ikke ubrydelige. Det vil sige at en bedrager - hvis han har tid nok - kan bryde en krypteret tekst og derved læse beskeden. Styrken af en kryptering afhænger af længden eller størrelsen på krypteringsnøglen. Jo større nøgle, jo flere muligheder skal bedrageren prøve, jo længere tid er bedrageren om at bryde koden. I praksis er det derfor tiden, der er afgørende for, om en bedrager finder det værd at bryde en krypteret tekst, eller om han opgiver på forhånd.

Længden af en krypteringsnøgle måles i det antal bits, som nøglen består af. I tilfælde, hvor kryptering er baseret på en fælles, hemmelig nøgle, kaldes krypteringen for *stærk*, hvis nøglen er 128bit eller større. Med nutidens computere vil det tage så lang tid at bryde en stærk krypteret tekst, at det i praksis ikke er gennemførligt. Grænsen for stærk kryptering flytter sig naturlig i takt med udviklingen af computere.

Der er naturligvis også forskel på, om bedrageren er en amatør-hacker eller en national efterretningstjeneste. I tabellen nedenfor er angivet tider for brydning af kryptering baseret på en fælles, hemmelig nøgle med forskellige nøglelængder og computerteknologi (1997).

Nøglelængde	Individuel hacker	Lille gruppe	Akademisk gruppe	Stor virksomhed	Efterretnings-tjeneste
40bit	Uger	Dage	Timer	Millisek.	Microsek.
56bit	>100 år	>10 år	År	Timer	Sek
64bit	>1000 år	>100 år	>10 år	Dage	Minutter
80bit	Ikke praktisk	Ikke praktisk	Ikke praktisk	>100 år	>100 år
128bit	Ikke praktisk	Ikke praktisk	Ikke praktisk	Ikke praktisk	>1000 år

Som det fremgår af tabellen, er det praktisk umuligt at bryde en

kryptering baseret på 128bit nøgle.

Kryptering baseret på public-key algoritmer kaldes for *stærk*, hvis nøglelængden er 1024bit eller større. En public-key nøgle på 1024bit "svarer" i styrke til en fælde, hemmelig nøgle på ca. 96bit.

For at hindre spredning af software med stærk kryptering til terroristlande, indførte den amerikanske regering eksportrestriktioner umiddelbart efter teknologiens fremkomst. Eksportrestriktionerne forbyder eksport af produkter, der indeholder kryptering med mere en 56bit nøgler. (Eksportrestriktionen blev lempet i december 1998 fra 40bit til 56bit.) En umiddelbar konsekvens af eksportrestriktionerne er, at browsere og post-programmer fra eksempelvis Microsoft og Netscape ikke understøtter stærk kryptering (baseret på 128bit nøgler) udenfor USA.

Som det fremgår af ovenstående tabel, er kryptering baseret på en 56bit nøgle dog ikke i praksis "sikker". Selv en lavteknologi-hacker kan bryde koden i løbet af kort tid. Den 19. januar 1999 blev en 56bit krypteret tekst brudt på 22 timer. Det skete i forlængelse af en annoncering fra det amerikanske sikkerhedsorganisation NIST om, at 56bit DES-kryptering ikke længere blev betragtet som sikker.

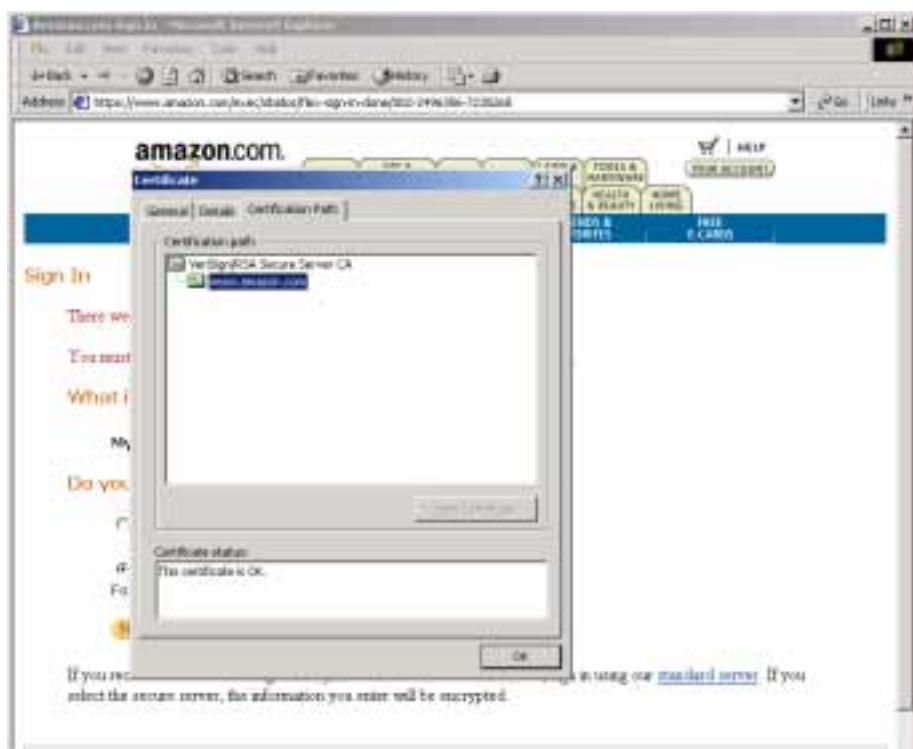
Den amerikanske regering har i starten af år 2000 lempet eksportrestriktionerne og alle væsentlige browsere og post-programmer understøtter nu kryptering baseret på 128bit nøgler.

Kryptering og SSL

Secure Socket Layer (SSL) er en protokol, der giver mulighed for kryptering af al kommunikation mellem en brugers browser og en web-server. En SSL-forbindelse gør det altså umuligt for tredjepart at "læse" kommunikationen mellem brugeren og web-serveren. Protokollen anvendes ofte ved overførsel af følsomme data fra brugeren til web-serveren, eksempelvis kreditkortnummer eller kendeord.

SSL blev udviklet af Netscape og understøttes nu af alle væsentlige browsere. SSL-protokollen er siden hen blevet overgivet til Internet Engineering Task Force (IETF), som har specificeret protokollen under navnet TLS.

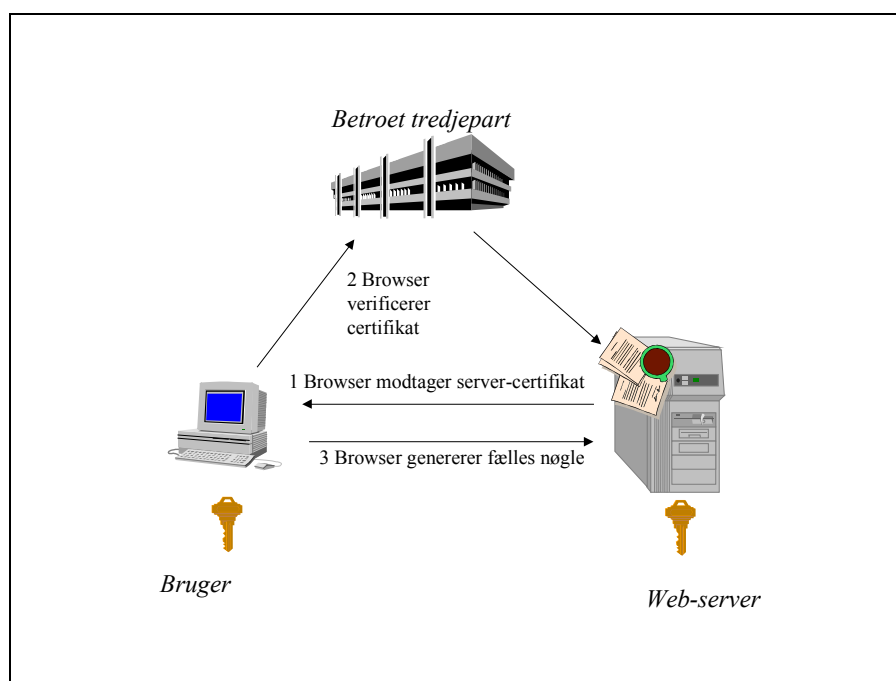
Det tekniske grundlag for SSL er PKI. For at der kan etableres en SSL-forbindelse mellem en browser og en web-server, skal web-serveren have et gyldigt server-certifikat, udstedt af en betroet tredjepart.



Amazon er certificeret af VeriSign

Ved at validere web-serverens certifikat, kan brugeren overbevise sig om, at han kommunikerer med den rigtige service og ikke for eksempel er ved at aflevere sit kreditkortnummer til en bedrager.

Etableringen af en sikker SSL-forbindelse er illustreret i figuren nedenfor.



Sikker forbindelse baseret på SSL

Når en bruger skifter til HTTPS-protokollen (SSL) sker følgende:

1. Web-serveren sender sit certifikat til brugerens web-browser.
2. Brugerens web-browser checker certifikatet ved at verificere certifikatets digitale signatur – altså om certifikater er underskrevet af en betroet tredjepart, såsom VeriSign.
3. Hvis server-certifikatet godkendes, genererer browseren en hemmelig, fælles krypteringsnøgle, krypterer denne med web-serveren offentlige nøgle (som browseren har fra serverens certifikat) og sender nøglen til web-serveren.
4. Web-serveren dekrypterer den fælles krypteringsnøgle ved hjælp af sin private nøgle.
5. Browseren og web-serveren krypterer al kommunikation ved brug af den fælles krypteringsnøgle.

Alt dette sker uden brugerens deltagelse. Det eneste brugeren oplever er, at browseren har en gul hængelås i nederste hjørne, og at transmissionshastigheden er nedsat.

Ved at klikke på hængelåsen kan brugeren "se" serverens certifikat. SSL giver altså brugeren mulighed for at overbevise sig om web-serverens identitet. Web-serveren kan derimod ikke "se", hvem brugeren er.

En senere version af Secure Socket Layer, SSL3 muliggør at brugeren skal identificere sig overfor web-serveren, ligesom serveren identificerer sig overfor brugeren. I praksis sker dette ved, at brugeren bliver bedt om at "sende" sit certifikat til web-serveren, der så kan hente relevante oplysninger om brugeren fra certifikatet.

SSL understøttes af alle væsentlige web-browsere og kan således anvendes uden installation af ekstra software. Brug af SSL3 forudsætter, at brugeren anskaffer sig et certifikat og installerer dette og den tilhørende private nøgle på sin PC.

På grund af amerikanske eksportrestriktioner af stærk kryptering, implementerer de fleste produkter dog kun SSL-kryptering baseret på 56bit nøgler. Efter lempelsen af de amerikanske eksportrestriktioner, er det nu muligt at opdatere de fleste produkter til stærk kryptering baseret på 128bit nøgler.

Digital signatur og elektronisk post

De fleste moderne programmer til elektronisk post understøtter tillige digital signatur. I Microsoft Outlook Express underskrives en elektronisk post blot ved at vælge "digital signatur" i menuen.



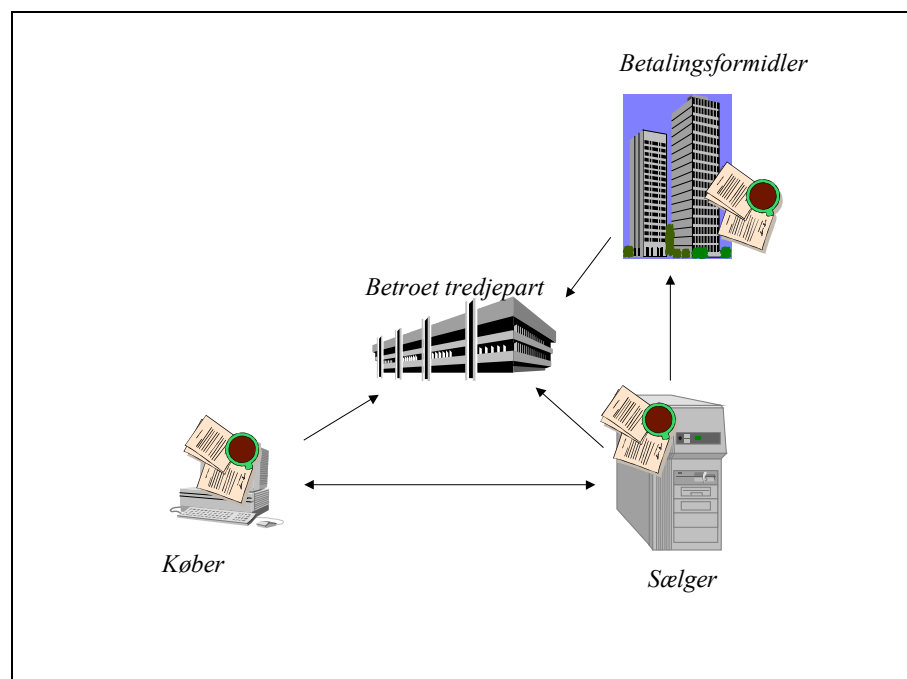
Digital signatur i Microsoft Outlook Express

En forudsætning for afgivelse af digital signatur er naturligvis, at brugeren har installeret et digitalt certifikat og den tilhørende private nøgle.

Secure Electronic Transactions

SSL anvendes ofte ved overførsel af kreditkortnumre i forbindelse med elektronisk handel på Internettet. Fremgangsmåden har dog den ulempe for køber, at sælgeren kan se købers kreditkortnummer. For at højne sikkerhedsniveauet har Visa og MasterCard udarbejdet en protokol, der beskytter købers kreditkortnummer fra sælgeren, men som tillader sælgers bank at se nummeret. Metoden er baseret på PKI og certifikater.

I figuren nedenfor er en betalingsproces ved hjælp af SET illustreret.



Betalingstransaktion med brug af SET

Fremgangsmåden ved gennemførelse af en betaling via SET er:

1. Sælger sender sig eget og betalingsformidlerens certifikater til køber. Sælger genererer tillige et unikt betalings-id, som entydigt identificerer betalingstransaktionen.
2. Køber verificerer sælger og betalingsformidler via den betroede tredjepart.
3. Køber krypterer sit kreditkortnummer med betalingsformidlerens offentlige nøgle, krypterer dernæst resultatet og betalings-id med sælgerens offentlige nøgle og sender det hele digitalt underskrevet til sælger. Køber sender tillige sit certifikat til sælger.
4. Sælger verificerer identiteten på køber på baggrund af købers certifikat. Sælger dekrypterer købers krypterede kreditkortnummer med sin private nøgle. Sælger kan ikke se købers kreditkortnummer, da dette er krypteret med betalingsformidlerens offentlige nøgle. Sælger sender købers krypterede kreditkortnummer til betalingsformidler.
5. Betalingsformidleren dekrypterer købers kreditkortnummer og verificerer identiteten på køberen via købers certifikat. Hvis køber er kreditværdig, returnerer betalingsformidleren svar til sælger om, at betalingen vil blive gennemført.

I en SET-løsning har alle parter et certifikat, og kan således identificere hinanden.

SET-løsningen kræver installation af ekstra software på brugerens PC. Dette har formentlig være delvis årsag til, at SET-løsningen ikke er blevet udbredt.

Software- eller smart card baserede løsninger

Sikkerheden i public-key kryptering er baseret på, at private nøgler ikke bliver kompromitterede. Ideelt set bør brugeren huske den private nøgle, og ikke gemme den i nogen form – ligesom med en PIN-kode. I praksis er det naturligvis urealistisk at bede en bruger indtaste en 1024bit nøgle efter hukommelsen ved hver brug.

I dag anvendes primært to metoder til elektronisk lagring af den private nøgle og disse karakteriseres som software-baserede løsninger og smart card baserede løsninger.

I en software-baseret løsning lagres den private nøgle i krypteret form på brugerens PC (eller på en diskette). Når nøglen skal bruges, indtastes en PIN-kode, som dekrypterer nøglen. Sikkerheden i denne løsning er altså baseret på, at brugeren kender PIN-koden.

Ulempen ved denne metode er, at den private nøgle ligger gemt på brugerens PC (i krypteret form), og en hacker kan derfor relativt nemt få

adgang til nøglen på krypteret form, og derved forsøge at bryde PIN-koden. Endvidere er løsningen ikke "mobil", idet brugeren er bundet til den PC, hvorpå nøglen er installeret (medmindre nøglen lagres på en diskette). Brugeren kan således ikke tage nøglen "med sig", eksempelvis for at bruge nøglen både i hjemmet og på arbejdspladsen. Fordelen ved metoden er, at løsningen ikke kræver ekstra hardware og at løsningen ofte kan implementeres relativt nemt (det vil sige med ingen eller få ekstra programmer).

I en smart card baseret løsning gemmes den private nøgle på et lille chip kort i kreditkort-størrelse. Når nøglen skal bruges, indsættes kortet i en kortlæser, og brugeren indtaster en PIN-kode. Sikkerheden i denne løsning er altså baseret på, at brugeren både har kortet og kender den tilhørende PIN-kode.

Ulempen ved metoden er, at de færreste PC'er indeholder kortlæsere, hvorfor eksterne kortlæsere må anvendes. Ud over den fysiske tilslutning af kortlæseren skal der ofte også ske installation af systemprogrammer til kommunikation med kortlæseren. Fordelen ved metoden er, at den private nøgle kun ligger lagret på brugerens smart card (som er "beskyttet" af brugeren), og at brugeren kan tage kortet med sig og derved anvende nøglen eksempelvis både i hjemmet og på arbejdspladsen. En kortlæser og tilhørende udstyr koster i dag mellem 300 - 700 kr.

I fremtiden vil der som alternativer til PIN-koder blive udviklet løsninger baseret på biometriske metoder, for eksempel fingeraftryk eller scanning af øjet. Disse teknologier er dog stadig umodne og forholdsvis dyre at implementere, og kan derfor ikke forventes anvendelige i nær fremtid.

Digital signatur og offentlige myndigheder

Offentlige myndigheder har i en årrække tilbudt forskellige former for elektronisk betjening til borgere og virksomheder. Eksempelvis har Told•Skat tilbudt elektronisk indberetning af selvangivelser via "Tast-selv" og Internettet. Sikkerhedsmæssigt er disse løsninger dog ikke tilstrækkelige til udvidet elektronisk selvbetjening og indberetninger.

Eksempelvis må en offentlig myndighed stille krav om uafviselighed af en ansøgning om boligstøtte, således ansøgeren ikke senere - i forbindelse med en bedragerisag - kan afvise at have afgivet urigtige oplysninger. Samtidigt må borgeren, i en digitaliseret verden - have en garanti for, at en offentlig myndighed ikke kan afvise en aftale fremsendt elektronisk til borgeren.

Dokumenter, der er forsynet med en digital signatur og et elektronisk tidsstempel, er principielt uafviselige for afsenderen, og vil juridisk kunne ligestilles med et underskrevet papirdokument.

Udbredelse af digital signatur er således en forudsætning for udvidet elektronisk borgerservice og offentlig digital sagsbehandling.

Lov om elektroniske signaturer

Loven om elektronisk signatur blev vedtaget i Maj 2000. Loven danner det juridiske grundlag for brug af digital signatur og opstiller krav til certifikater, og sikkerhed, tilsyn og drift af nøglecentre.

Loven sidestiller gyldigheden af et elektronisk dokument med en elektronisk signatur med et papir med en håndskreven underskrift, hvis den elektroniske signatur lever op til en række lovmæssige krav; hvis ikke andre juridiske regler forhindrer brug af elektronisk signatur, og hvis begge parter er enige om at acceptere elektroniske signaturer.

En konsekvens af loven er, at enhver organisation principielt kan drive nøglecenter-virksomhed i Danmark, blot den opfylder betingelserne i loven. Telestyrelsen fører på vegne af de offentlige myndigheder tilsyn med anmeldte nøglecentre.

Offentlige initiativer omkring digital signatur

Det offentlige har igangsat flere initiativer, der skal fremme brugen af digital signatur i Danmark, herunder pilotprojekter om digital signatur, som denne rapport evaluerer.

I forbindelse med den Telepolitiske redegørelse og Det Digital Danmark, er der udpeget en række fokusområder, hvor digital signatur naturligt finder anvendelse. Nogle af disse er personlig Internetadgang for alle og elektronisk indkøb for offentlige organisationer.

Endvidere forventer Forskningsministeriet i samarbejde med Staten og Kommunernes Indkøbscentral (SKI) at starte et udbud omkring anskaffelse af komponenter til PKI, blandt andet baseret på erfaringerne fra pilotprojekterne om digital signatur.

2. Pilotprojekterne

Følgende otte pilotprojekter indgår i evalueringen:

- *Erhvervs- og Selskabsstyrelsen*: Modtagelse af elektroniske indberetninger af årsregnskaber, ATP-indbetalinger, selskabsoplysninger og lønindeholdelse
- *EU-direktoratet*: Fordeling af hektarstøtte til landmænd på baggrund af elektroniske ansøgninger
- *SU-styrelsen*: Elektronisk selvbetjening af SU-systemet
- *Handelshøjskolen i København*: Elektronisk modtagelse af eksamensopgaver og smart card studiekort
- *Næstved Kommune*: Elektroniske ansøgning om ejendomsoplysninger ved salg af ejendomme
- *Ringsted Kommune*: Elektroniske blanketter til flyttemeddelelser, ændring af skattekort og ansøgninger om daginstitution
- *Vordingborg Kommune*: Elektronisk behandling af byggetilladelser og ejendomsoplysninger
- *Århus Amt*: Udveksling af sygesikringsafregninger mellem en række sundhedsinstitutioner

Indholdet af pilotprojekterne opsummeres kort i det efterfølgende.

Erhvervs- og Selskabsstyrelsen

Erhvervs- og Selskabsstyrelsen har i samarbejde med Told- og Skattestyrelsen, Danmarks Statistik, Finansstyrelsen og ATP gennemført et pilotprojekt om digital signatur VIDSIG (Virksomheders brug af Digital Signatur). ICL har udviklet løsningen og Post Danmark/PBS har fungeret som nøglecenter.

Projektets formål

Det overordnede formål med pilotprojektet var at undersøge muligheden for at lette de administrative byrder for virksomheder ved at bruge digital signatur i forbindelse med elektroniske indberetninger. Samtidigt ville projektet give de deltagende myndigheder mulighed for afprøvning af digital signatur på tværs af flere myndigheder og teknologier.

Det samlede pilotprojekt var planlagt til at indeholde følgende delområder:

- Indsendelse af regnskaber via EDIFACT-løsning. Brugen af digital signatur øger sikkerheden.
- Indbetaling af ATP som online indbetalinger via PBS.
- Indbetaling til fælles lønindeholdelsessystem som online

- indbetalinger via PBS, home-banking mm.
- Anmeldelse af ændringer i selskaber.

På grund af forsinkelser i projektforsløbet, blev anmeldelser om ændringer i selskaber ikke afprøvet i pilotprojektet. Endvidere er løsningen til indsendelse af regnskaber via EDIFACT endnu ikke sat i drift.



<http://www.indbetal.atp.dk>

Den digitale signatur anvendes både af virksomheder ved indberetning og indbetalinger og af myndighederne ved returnering af kvittering for modtagelse.

Løsningen er smart card baseret. Kortene udstedes af Post Danmark, og afhentes på landets posthuse.



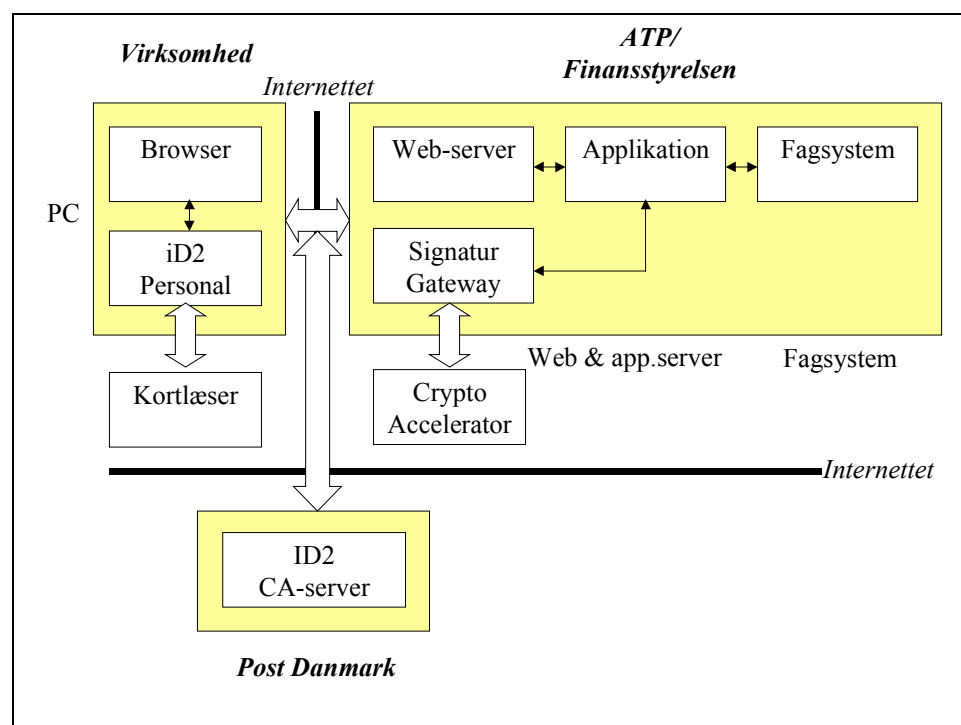
<http://www.finansstyrelsen.dk>

Da løsningen til indsendelse af årsregnskaber via EDIFACT endnu ikke blevet sat i drift, indgår dette delprojekt ikke i evalueringen.

Anvendelsen af digital signatur

Den digitale signatur anvendes til signering af de data, som virksomhederne indberetter via ATP og Finansstyrelsens hjemmesider. I praksis fungerer løsningen ved, at en HTML-form forsynes med brugerens digitale signatur, inden den overføres til styrelsernes web-servere.

Den tekniske opbygning af løsningen er illustreret i figuren nedenfor.



Brugeren (virksomheder) anvender en standard web-browser på en PC med en kortlæser tilsluttet tastaturporten eller en seriel port. Til generering af digital signatur og verifikation af modtagne signaturer anvendes iD2 Personal, som selvfølgelig skal være installeret på brugerens PC.

Hos styrelsen (ATP/Finansstyrelsen) modtages signerede HTML-forms af en Signatur Gateway, der verificerer den digitale signatur. Den centrale web-applikation sender data til bagvedliggende fagsystemer eller eksempelvis PBS. For at opnå høj (de)krypteringshastighed, er løsningen forberedt til ekstern krypteringshardware.

Post Danmark driver den anvendte CA-server, der er tilgængelig via

Internettet.

Status

Løsningen er blevet tilsendt ca. 100 virksomheder.

I perioden 6. - 15. april modtog ATP elektroniske indberegninger med digital signatur for første kvartal. Ca. 55 virksomheder gjorde brug af muligheden.

Finansstyrelsen satte deres del af løsningen i drift i starten af år 2000. Indtil medio april havde ca. 15 virksomheder anvendt den.

Endvidere har 10 revisionsvirksomheder tilmeldt sig afprøvning af løsningen til elektronisk forsendelse af regnskaber via EDIFACT. Afprøvningen af denne del af den samlede løsning er dog endnu ikke tilendebragt.

Erhvervs- og Selskabsstyrelsen følger løbende op på tilmeldte virksomheder, og har som mål, at alle anvender udstyret og løsningen i løbet af foråret år 2000.

Opnåede resultater

Løsningen har primært givet lettelser for de deltagende virksomheder. Før løsningen blev gjort tilgængelig, gennemførte virksomheder typisk indbetalinger ved hjælp af girokort.

Generelt har brugerne været tilfredse med løsningens udformning og funktionalitet. Specielt har virksomhederne vurderet, at indtastninger er nemme og at løsningen er hurtig at anvende i praksis.

Erhvervs- og Selskabsstyrelsen har endvidere foretaget en rundspørge blandt deltagende virksomheder om, hvor meget virksomhederne er villige til at betale for udstyr til løsningen. Gennemsnitlig finder virksomhederne det rimeligt at betale mellem kr. 250-749 for udstyret. Denne vurdering er dog afgivet efter virksomhederne har anvendt løsningen, og således er bekendt med løsningens indhold og fordele. Der er dog stor varians i besvarelsene. Halvdelen af virksomhederne vil have udstyret gratis eller til en meget lav pris.

Prisen på det anvendte udstyr (kortlæser og iD2 Personal) er i pilotprojektet opgjort til kr. 1240, hvilket virksomhederne overvejende finder lidt dyrt i forhold til anvendelsesmulighederne. Der er dog stor spredning i holdningen.

Projektets videre forløb

Erhvervs- og Selskabsstyrelsen forventer at kunne anvende de opnåede erfaringer fra pilotprojektet til at udvikle elektroniske indberetningsløsninger med digital signatur på andre områder.

Eksempelvis vurderer Erhvervs- og Selskabsstyrelsen mulighederne for at anvende digital signatur i forbindelse med LetLøn-initiativet.

ATP har indstillet brugen af digital signatur på grund af administrativ overbelastning. ATP opretter næste år et Call Center, bl.a. for at imødegå dette. Der er endnu ikke taget stilling til om systemet genåbnes, eller om der vælges en anden løsning til digital signatur.

Finansstyrelsen fortsætter med brugen af digital signatur i resten af år 2000. Der er endnu ikke taget stilling til, om løsningen skal gøres permanent. Dette afhænger bl.a. af, om Finansstyrelsen får flere tilmeldte virksomheder.

EU-direktoratet

EU-direktoratet har i samarbejde med et antal underleverandører, herunder WM-data, Oracle, IT+ og Cryptomatic, gennemført pilotprojekt vedrørende elektronisk indsendelse af ansøgning om hektarstøtte via Internettet.

Projektets formål

Formålet med projektet var at give mulighed for elektronisk indsendelse af ansøgninger om hektarstøtte med digital signatur via Internettet. EU-direktoratet tilbyder tillige modtagelse af ansøgninger uden digital signatur via Internettet, men i dette tilfælde skal en papir-baseret ansøgning eftersendes. Anvendelsen af digital signatur forenkler således ansøgningsprocessen, og giver EU-direktoratet mulighed for elektronisk datafangst uden manuel verifikation.



<http://www.eudirektoratet.dk/stoetteordninger/index.htm>

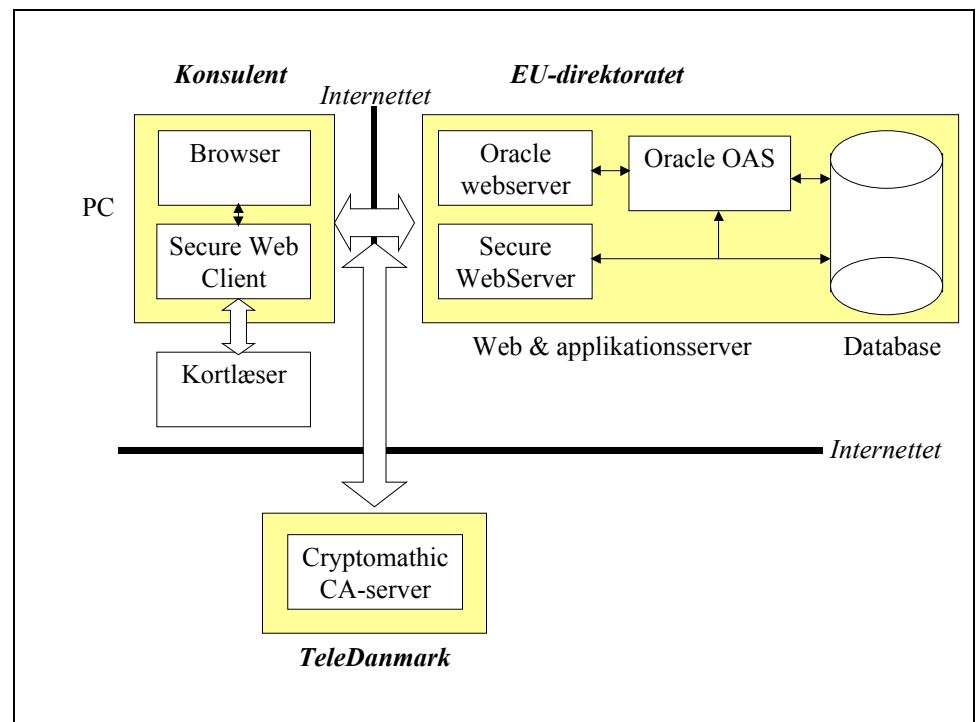
Løsningen med digital signatur blev via konsulentcentre tilbudt 500 landmænd.

Anvendelsen af digital signatur

Løsningen giver landmænd (konsulenter) mulighed for digitalt at signere en HTML-form, som udgør en ansøgning. Den private nøgle lagres på et smart card.

I modsætning til de øvrige løsninger tilbydes EU-direktoratets løsning via landmændenes konsulenter. Det har den konsekvens, at selvom alle deltagende landmænd skal have en digital signatur (et smart card), så skal selve løsningen (kortlæser og programmel) kun installeres hos de medvirkende konsulenter.

Den tekniske opbygning af løsningen fremgår af figuren nedenfor.



Brugeren (konsulent/landmand) anvender en standard browser på en PC, hvortil der er tilsluttet en kortlæser via tastaturporten. Den digitale signatur genereres ved hjælp af programmet Secure Web client.

Hos EU-direktoratet modtages den digitalt signerede ansøgning af en Secure Web Server, der verificerer landmandens digitale signatur ved at kontakte CA-serveren. Elektronisk modtagne ansøgninger lagres i en database, hvorefter de behandles manuelt efter ansøgningstidsfristens udløb.

Tele Danmark driver den CA-server, som anvendes af løsningen. Smart

cards initieres og udstedes af konsulenterne.

Status

Løsningen blev sat i drift januar 1999 og blev anvendt i forbindelse med ansøgningsrunden 1999. EU-direktoratet modtog i alt 59.069 ansøgninger om hektarstøtte, hvoraf 7.314 blev modtaget via Internettet (uden digital signatur) og 337 (ud af 500 mulige) blev modtaget via Internettet (med digital signatur). Årsagen til, at ikke samtlige 500 udpegede landmænd indsendte ansøgninger med digital signatur er, at to konsulentcentre på grund af tekniske problemer med løsningen trådte ud af projektet.

Opnåede resultater

EU-direktoratet har modtaget tilbagemeldinger fra de deltagende konsulenter og landmænd.

De deltagende konsulenter har udtrykt begejstring for pilotprojektet, men var ikke indstillet på det tidsforbrug, som pilotprojektet medførte.

Tidsforbruget skyldes primært tekniske problemer med det valgte smart card, samt opsætning og konfiguration af systemet.

De fleste deltagende konsulenter kan se potentielle muligheder for anvendelsen af digital signatur i forbindelse med elektroniske ansøgninger, men fremhæver dog også, at løsninger hertil ikke må påføre dem et mertidsforbrug. I pilotprojektet var det konsulenternes opgave at initiere og udstede smart card til landmændene.

For landmændene betød løsningen primært færre fejl, idet systemet indeholder online valideringer af oplysninger. Løsningen muliggør dog ikke en fuldstændig digital sagsbehandling, idet markplaner mm. fortsat skal indsendes på papir til EU-direktoratet.

EU-direktoratet primære gevinst ved løsningen er muligheden for elektronisk datafangst, samt reduktion i antallet af trivielle fejl i ansøgninger (på grund af online valideringer i løsningen).

For år 2000 har EU-direktoratet valgt at vedligeholde og udbygge Internetløsningen uden digital signatur, og er gået videre med et pilotprojekt under Fødevarerministeriet omfattende digital indberetning af geografiske anvendelsesdata (markkort), således at der er yderligere driftsklare anvendelsesmuligheder, når projektet "Digital forvaltning" kan gennemføres i stor skala.

Projektets videre forløb

EU-direktoratet har ikke planer om tilbyde modtagelse af ansøgninger med digital signatur i år 2000. Dette skyldes primært, at et sådant tilbud da skulle omfatte samtlige potentielle ansøgere, og EU-direktoratet har ikke økonomisk mulighed for at tilbyde gratis smart cards og kortlæser til

alle. Endvidere var lovgrundlaget ved pilotprojektets afslutning endnu ikke fastlagt.

EU-direktoratet vurderer, at digital signatur-teknologien har store anvendelsesmuligheder indenfor Fødevareministeriet generelt, men vurderer dog også, at antallet af anvendelsesmuligheder skal være større og f.eks. inkludere Told&Skat, for at løsningerne bliver interessante for landmænd.

Løsninger med digital signatur vurderes til at have større potentiale hos virksomheder, der har løbende kontakt med Fødevareministeriet, end hos landmænd, der kun sjældent foretager ansøgninger eller indberetninger.

SU-styrelsen

SU-styrelsen har i samarbejdet med WM-data, IT+ og et antal underleverandører igangsat et pilotprojekt vedrørende selvbetjening af SU-systemet.

På grund af forsinkelser i udviklingsarbejdet er systemet endnu ikke sat i drift, men er dog blevet afprøvet af en lille gruppe personer. Det forventes, at systemet kan tages i drift i midten af år 2000.

Projektets formål

Formålet med projektet er at give studerende mulighed for selvbetjening af SU-systemet, herunder indsendelse af SU-ansøgninger og visning af egne data. I dag kan studerende kun få oplysninger om egne forhold, eksempelvis tildelt støttebeløb eller status på klippekort ved at henvende sig personligt eller telefonisk til SU-styrelsen eller uddannelsesinstitutioner.

SU Klippekortet

Navn og adresse
 Navn: Olsen, Jens
 c/o navn:
 Nuværende adresse: Rådhuspladsen
 1559 København V
 CPR: 123456-1234

KØBENHAVNS UNIVERSITET
BACHELOR, SOCIOLOGI
 Start: September 1999, Slut: Juni 2002
 Nuværende uddannelse er indenfor klippekortet

Uddannelsesklippekortet		6 års klippekortet	
Konkret studieid + 1 år	46	Ramme	70
- forbrug af klip i uddannelsen	12	+ udvidelse af ramme	0
Heraf offentlig støtte	0	+ fødselsklip	0
- ældre fødselsklip	0	+ stægklip	0
- tilægklip	0	Ramme i alt	70
- tidligere opsparing	0	Forbrug af klip	19
Netto forbrug i uddannelsen	12	Heraf offentlig støtte	0
Fæsel (rådighed)	0		
Resterende klip i uddannelsen	34	Resterende klip i 6-års klippekortet	51
Opsparet dobbelklip	0	Forbrugte slutårsklip	0
Forbrugte dobbelklip	0		

<http://www.su.dk>

Pilotprojektet er målrettet mod ca. 1.000 unge under uddannelse på 4 udvalgte uddannelsesinstitutioner, men systemet er opbygget til at omfatte samtlige ca. 270.000 SU-modtagere.

De studerende kan via en Web/Java-brugergrænseflade enten indsende:

- SU-ansøgning eller ansøgning om ændringer af tidligere registrerede oplysninger, med digital signatur

Eller få vist:

- Forskellige lister over udbetalinger
- Oversigter pr. støtteår over tildelingen og det beregnede fribeløb
- Oplysninger om uddannelsen og status på klippekort.

Systemet skal tillige anvendes af administrative medarbejdere på de enkelte uddannelsesinstitutioner, som så elektronisk kan behandle og godkende SU-ansøgninger.

Løsningen er baseret på smart card-teknologi, og de enkelte uddannelsesinstitutioner fungerer som certifikat-udsteder.

Anvendelsen af digital signatur

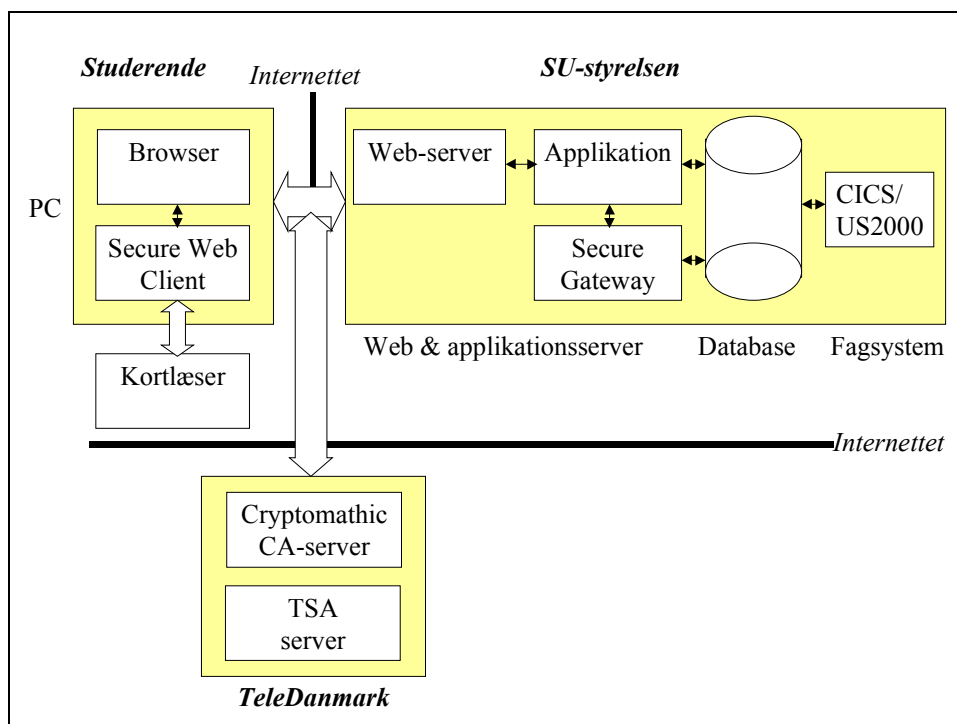
Brugerens digital certifikat anvendes til to formål: Til sikker identifikation af brugeren i forbindelse med visning af egne data i SU-

systemet, og til generering af digital signatur i forbindelse med elektronisk indsendelse af ansøgninger.

Medarbejdere på uddannelsesinstitutioner kan via løsningen forsyne SU-ansøgninger med ekstra oplysninger og godkende ansøgningerne, før disse overføres til styrelsens centrale EDB-system.

De godkendte SU-ansøgninger udstyres endvidere med digital signatur af uddannelsesinstitutionens medarbejder.

Den tekniske opbygning af løsningen er illustreret i figuren nedenfor.



Den studerende anvender en PC med en standard web-browser installeret. Tillige skal programmet Secure Web client være installeret, og den anvendte kortlæser tilsluttes via PC'en tastaturport.

Medarbejdere på de tilsluttede uddannelsesinstitutioner har udover ovenstående konfiguration også et LRA-program installeret på deres PC. Dette anvendes i forbindelse med udstedelse af certifikater til de studerende.

Hos SU-styrelsen modtages digital signerede ansøgninger af Secure Gateway, som verificerer signaturen ved at kontakte CA-serveren. Ansøgningen overføres til den centrale SU-system US2000 via en gateway.

Tele Danmark driver den anvendte CA-server.

Status

Det var oprindeligt planlagt at sætte SU-selvbetjeningssystemet i drift i 2. kvartal 1999. På grund af en række forsinkelser, bl.a. af teknisk karakter, er projektets start dog forsinket til 2. kvartal 2000.

Opnåede resultater

Selvbetjeningssystemet er ikke blevet anvendt af studerende på nuværende tidspunkt.

Der foreligger derfor ingen praktiske erfaringer om brugen af systemet.

SU-styrelsen forventer at studerende vil opnå følgende fordele ved systemet:

- Større fleksibilitet for studerende, idet SU-systemet principielt bliver døgnåbent og uafhængig af uddannelsesinstitutionens åbningstid.
- Kortere ekspeditionstider for ansøgninger og ændringer på grund af digital sagsbehandling.

SU-styrelsen forventer, at uddannelsesinstitutioner vil opnå følgende fordele ved systemet:

- Mindre papir-skemahåndtering på grund af elektroniske skemaer.
- Færre personlige forespørgsler fra studerende om SU-data.
- Færre indtastninger af SU-ansøgninger af uddannelsesinstitutionens SU-medarbejdere i det centrale SU-system.
- Færre fejl i modtagne SU-ansøgninger.

SU-styrelsen forventer selv at opnå følgende fordele ved systemet:

- Besparelse til trykning og distribution af skemaer mm.
- Færre rettelser i modtagne ansøgninger.
- Færre forespørgsler om SU-data fra studerende.

Opnåelse af den fulde rationaliseringsgevinst forudsætter dog, at ansøgninger prævalideres online mod SU-styrelsens centrale system. En sådan prævalidering er dog endnu ikke indbygget i løsningen, da dette kræver systemændringer i det centrale SU-system. Ændringerne forventes implementeres i 3. kvartal 2000.

Projektets videre forløb

SU-styrelsen forventer at sætte pilotprojektet i drift i maj 2000. I første omgang udstedes certifikater til ca. 1.000 studerende fordelt på fire uddannelsesinstitutioner.

Styrelsen ønsker at udbrede løsningen til samtlige studerende, men en

forudsætning herfor er, at der kan findes en økonomisk overkommelig finansieringsmodel. Styrelsen finder det ikke realistisk, at studerende for egen regning vil afholde udgiften til kortlæser og certifikat, på grund af den lave anvendeshyppighed af løsningen.

Handelshøjskolen

Handelshøjskolen i København (HHK) har gennemført et projekt omkring elektronisk aflevering af eksamensopgaver.

Projektets formål

Pilotprojektet havde oprindeligt to formål:

- Implementering af et nyt smart card baseret studiekort, der kan anvendes til ID-kort, digital signatur og betaling for små-indkøb
- Etablering af mulighed for elektronisk aflevering af eksamensopgaver via digitalt signeret elektronisk post.

På grund af problemer med tilvejebringelse af et egnet chip-kort, blev det samlede projekt delt op i to selvstændige projekter. Digital signaturprojektet anvender således ikke studiekortet til lagring af certifikater.



<http://www.adm.cbs.dk/ds>

Delprojektet vedrørende elektronisk indsendelse af eksamensopgaver havde dog stadig til hensigt at anvende smart cards til lagring af personlige certifikater. Under afprøvningen af løsningen viste det sig dog, at de anvendte chip-kort ikke var stabile. Pilotprojektet blev følgelig gennemført som en ren software-baseret løsning, hvor den studerende opbevarede sit personlige certifikat på en PC eller på en diskette.

Praktisk bruges løsningen som følger. Den studerende "pakker" de filer som indgår i eksamensopgaven sammen i en zip-fil, og signerer denne digitalt. "Pakken" sendes som et vedhæftet dokument til HHK's postsystem.

Når opgaven modtages af HHK, sender en medarbejder en digitalt signeret kvittering tilbage til den studerende for modtagelsen. Dernæst udskriver medarbejderen opgaven på papir og overgiver opgaven til den lærer, som skal bedømme opgaven. Samtidigt gemmes et kopi af opgaven i HHK's elektroniske arkiv.

Lærerne anvender på tilsvarende måde løsningen til at indsende bedømmelser. Dette som en elektronisk post indeholdende en digitalt signeret karakterliste.



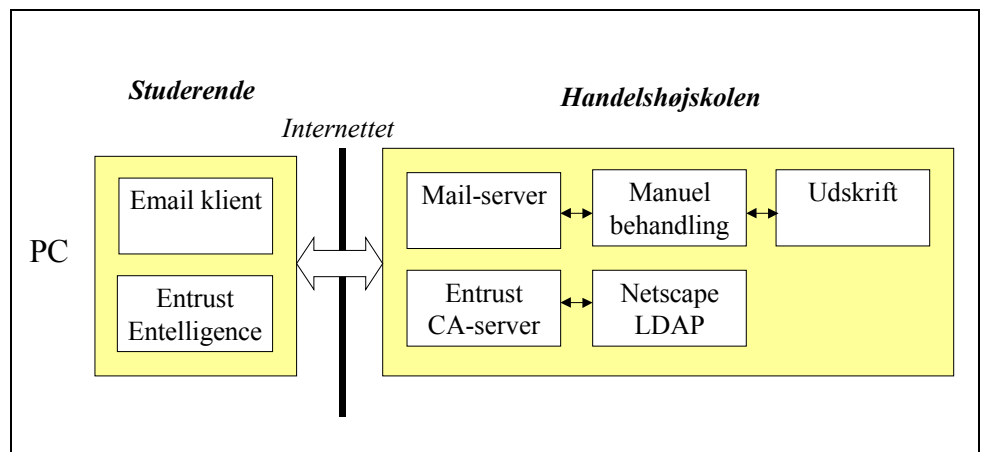
<http://www.adm.cs.dk/ds>

Handelshøjskolen planlægger endvidere at anvende de udstedte certifikater til adgangskontrol til skolens hjemmesider.

Anvendelsen af digital signatur

Selv om den anvendte software giver mulighed for digital signatur på elektronisk post, har de fleste studerende valgt at signere en zip-fil og dernæst sende denne som en vedhæftet fil til Handelshøjskolen. (En del af forklaringen på dette er, at løsningen i pilotperioden ikke understøttede stærk kryptering med Netscape-produkter på grund af de amerikanske eksportrestriktioner).

Den tekniske opbygning af løsningen er illustreret i figuren nedenfor.



Den studerende anvender et standard mail-program til indsendelse af den digitalt signerede opgave. Den digitale signatur genereres af Entrust Entelligence-programmet, som folgelig også skal være installeret på brugerens PC. Det digitale certifikat lagres enten på PC'ens harddisk eller på en diskette.

På handelshøjskolen modtages den elektroniske post af skolens mail-server. En medarbejder behandler manuelt de modtagne breve. Behandlingen består i kontrol af signaturens gyldighed og udskrivning af opgaven. Endvidere sender medarbejderen et kvittering til den studerende for modtagelse af opgaven.

Status

Løsningen blev færdiggjort i løbet af sommeren 1999 og blev anvendt i forbindelse med aflevering af en godkendelsesopgave den 29 oktober 1999. I forsøget deltog tre hold studerende, der alle var 3. semesterstuderende fra DØK (HA i datalogi). Ud af 74 indskrevne afleverede 64 studerende opgaven. En enkelt gruppe måtte af tekniske årsager opgive at sende opgaven pr. elektronisk post. Gruppen var opkoblet til Internettet igennem en firewall, der forhindrede dem i at anvende løsningen.

Pilotprojektet har således etableret et PKI-miljø inklusive en CA-funktion samt verificeret brugen af digital signatur i forbindelse med elektronisk aflevering af eksamensopgaver.

Opnåede resultater

En rundspørge blandt de deltagende studerende viser, at de studerende generelt er tilfredse med muligheden for elektronisk aflevering af opgaver. Enkelte studerende oplevede tekniske problemer i forbindelse med afleveringen, men de fleste fandt fremgangsmåden nem og tidsbesparende.

Kendetegnet for de fleste tilbagemeldinger er tilfredshed med at undgå

kopiering af opgaven og personligt fremmøde på Handelshøjskolen ved aflevering.

Enkelte studerende påpegede dog, at opkoblingshastigheden til Internettet kan være en begrænsende faktor for løsningens anvendelse.

Hos administrationen hos HHK er der ligeledes tilfredshed med løsningen, idet medarbejderne undgår at skulle modtage og distribuere opgaver.

Løsningen betyder dog ekstraarbejde for IT-gruppen, idet denne havde ansvaret for at returnere kvitteringer til studerende, samt at udskrive opgaver på papir. Det undersøges nu om disse processer kan automatiseres.

Projektets videre forløb

På grundlag af de opnåede erfaringer ønsker Handelshøjskolen at fortsætte projektet og udvide dette til flere anvendelser. Eksempelvis kan det digitale certifikat anvendes til at give adgang til Handelshøjskolens beskyttede hjemmesider og til personlige oplysninger.

Næstved Kommune

Næstved Kommune har gennemført pilotprojektet "Grønt skema" i samarbejde med PBS, IBM Danmark og Kommunernes Landsforening (KL).

Projektets formål

Næstved Kommune ønskede med projektet at afprøve samarbejdet mellem flere certifikat-udstedere (CA'er) for at bane vejen for aftaler om gensidig anerkendelse af certifikater. Herudover skulle projektet indeholde:

- En intern test af digital signatur blandt kommunens medarbejdere
- En test af digital signatur over for et antal lokale ejendomsmæglere og advokater
- Et tilbud om digital signatur til alle virksomheder og borgere i Næstved Kommune
- Brug af digital signatur i forbindelse med ibrugtagning af e-indkøbssystem
- Anvendelse digital signatur i forbindelse med indberetning af sygedagpenge.

På grund af forskellige vanskeligheder – primært af teknisk karakter – blev projektes formål revideret til:

- Test af digital signatur over for et antal lokale ejendomsmæglere i

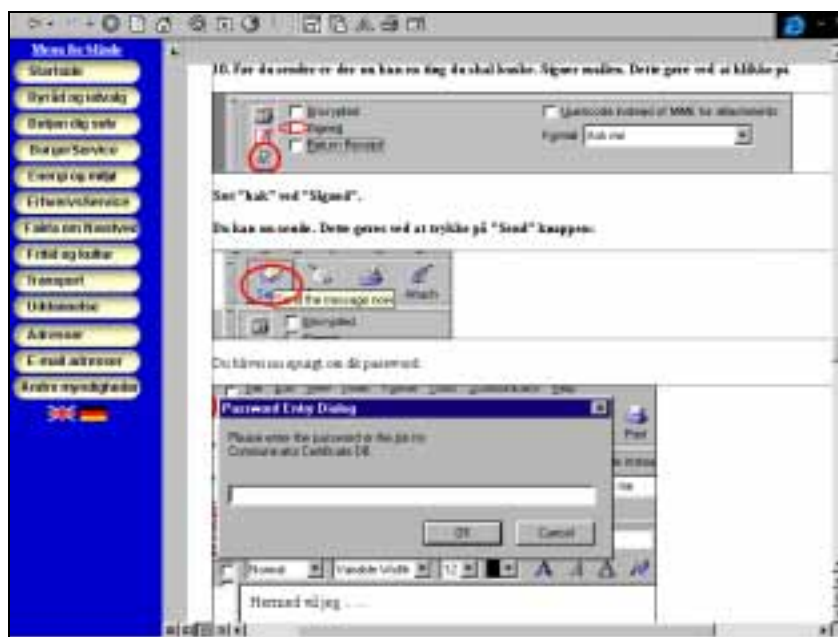
forbindelse med indhentning af ejendomsoplysninger

Af tidsmæssige årsager blev det opgivet at tilbyde digital signatur til samtlige borgere og virksomheder i Næstved Kommune, og elektronisk indberetning af sygedagpenge via blanket på Internettet er udsat til et senere projekt. Anvendelse af flere CA-udbydere blev opgivet på grund af pilotprojektets tidsmæssigt begrænsede omfang.



<http://www.naekom.dk>

Det gennemførte projekt giver ejendomsmæglere og advokater mulighed for at ansøge om og modtage ejendomsoplysninger fra Næstved Kommune. Ansøgningerne og oplysningerne fremsendes via digitalt signeret elektronisk post.



<http://www.naekom.dk>

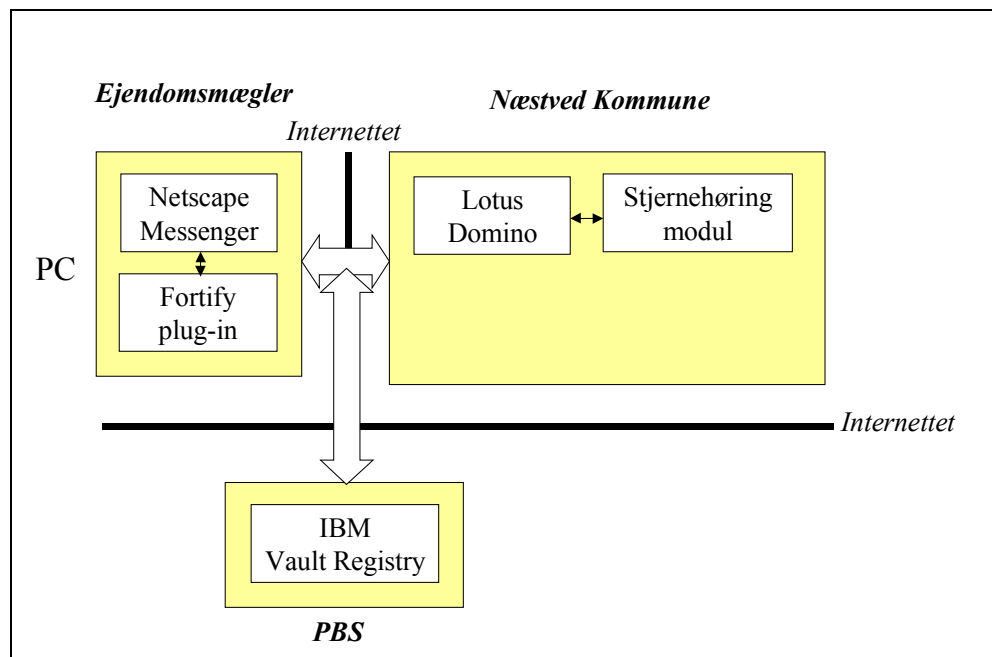
Anvendelsen af digital signatur

Den digitale signatur anvendes i forbindelse med indsendelse af en ansøgning om ejendomsoplysninger fra en ejendomsmægler eller advokat til Næstved Kommune. Selve ansøgningen er en elektronisk kopi af "det grønne skema", som hentes fra Næstved Kommunes hjemmeside. Ansøgningen sendes med digital signatur som elektronisk post til Næstved Kommunes tekniske forvaltning.

Kommunen behandler ansøgningen ved brug af et stjernehøringsmodul, og returnerer oplysningerne til ansøgeren via digital signeret elektronisk post. Stjernehøringsmodulet giver mulighed for en digital sagsbehandling og er blevet udviklet parallelt med pilotprojektet.

Løsningen er software-baseret og kræver følgelig ikke installation af kortlæser og systemprogrammell hos brugeren. Løsningen var dog i pilotperioden kun tilgængelig via Netscape Messenger.

Den tekniske opbygning af løsningen er illustreret i figuren nedenfor.



Brugeren (ejendomsmægleren) anvender Netscape Messenger til at indsende digitalt signeret elektronisk post. For at muliggøre brug af stærk kryptering (på det tidspunkt, da Netscape Messenger kun understøttede 56bit kryptering uden for USA) anvendes en plug-in Fortify.

Hos Næstved Kommune modtages posten af kommunens Notes mail-system. Mail-serveren checker den digitale signatur, og dirigerer ansøgningen ind i stjernehøringsmodulet, der ligeledes er baseret på Notes.

Som CA anvendes PBS, der har implementeret tjenesten ved brug af IBM Vault Registry.

Status

Næstved Kommunes løsning blev officielt åbnet den 10. maj 1999. På grund af tekniske vanskeligheder fungerede løsningen dog ikke optimalt, og først i november 1999 begyndte fem ejendomsmæglere at anvende løsningen regelmæssigt.

Kommunen kontaktede i projektets begyndelse 23 ejendomsmæglere og advokater og omkring 18 udtrykte interesse i at deltage i projektet. Primært på grund af tekniske problemer er løsningen dog ikke blevet udbredt til et større antal brugere.

I perioden frem til april 2000 har Næstved Kommune modtaget ca.100 elektroniske anmodninger om ejendomsoplysninger (ud af i alt ca. 500), og har besvaret ca. halvdelen elektronisk.

Opnåede resultater

Som en del af pilotprojektet har Næstved Kommune tillige digitaliseret sagsbehandlingen af anmodning om ejendomsoplysninger. Dette har resulteret i en reduktion af sagsbehandlingstiden på mellem 10 - 15 minutter pr. ansøgning.

Generelt har pilotbrugerne været tilfredse med løsningen, idet den overflødigger afhentning af skemaer hos kommunen, manuel udfyldelse af skemaet, indsendelse af skemaet pr. post samtidigt med at løsningen reducerer sagsbehandlingstiden.

De deltagende ejendomsmæglere vurderes at have opnået en tidsbesparelse på 2-4 dage, idet sagsbehandlingstiden er nedsat fra 5 - 14 dage til nu 5 - 10 dage og i nogle tilfælde helt ned til 2 dage.

Projektets videre forløb

På baggrund af de deltagende ejendomsmæglere positive reaktion over projektet, har Næstved Kommune besluttet at gøre projekt "grønt skema" permanent.

Endvidere har Næstved Kommune indsendt en ansøgning om, at gennemføre et pilotprojekt vedrørende indberetning af sygedagpenge via en netblanket på Internettet.

Ringsted Kommune

Ringsted Kommune har gennemført pilotprojektet "Det Digitale Rådhus" i samarbejde med Kommunedata (KMD).

Projektets formål

Ringsted Kommune ønskede at give borgerne mulighed for at kommunikere elektronisk med rådhuset via Internettet. Dette skulle styrke dialogen mellem borgeren og rådhuset, og give den enkelte borger mulighed for at "betjene sig selv" - uafhængigt af tid og sted.

Til dette formål har Ringsted Kommune opbygget en portal på Internettet, der giver en fælles indgang til alle de serviceydelser og informationer, som kommunen tilbyder elektronisk. Portalen er udviklet af Kommunedata, der også afvikler løsningen for Ringsted Kommune.



<http://www.ringsted.dk>

Projektet giver mulighed for at borgeren kan hente, udfylde og sende blanketter til kommunen via Internettet og Ringsted Kommunes hjemmeside. De indsendte blanketter forsynes med en digital signatur, således at deres ægthed og oprindelse er garanteret.



<http://www.ringsted.dk/default.asp?infoId=1054117>

Serviceydelserne, som kommunen tilbyder er:

- Flytteanmeldelse integreret med lægevalg, og adressebeskyttelse
- Ansøgning om optagelse i daginstitution
- Ansøgning om friplads i daginstitution

- Ændring af skattekort (fra maj 2000)
- Ændring af pensionsoplysninger
- Ansøgning om gravetilladelse (fra maj 2000)
- Elektronisk post med digital signatur
- Publicering af annoncer (var en del af projektet, men er senere blevet opgivet).

Endvidere giver løsningen adgang til en række blanketter, der indsendes uden digital signatur.

Løsningen er integreret i Ringsted Kommunes øvrige hjemmesider, der blandt andet indeholder en servicehåndbog om Ringsted.

Indtil videre er sagsbehandlingen af elektronisk modtagne ansøgninger ikke blevet digitaliseret. Under pilotprojektet er ansøgninger sendt via elektronisk post fra Kommunedata til Ringsted Kommune, hvor de er blevet udskrevet og behandlet i den normale sagsgang.

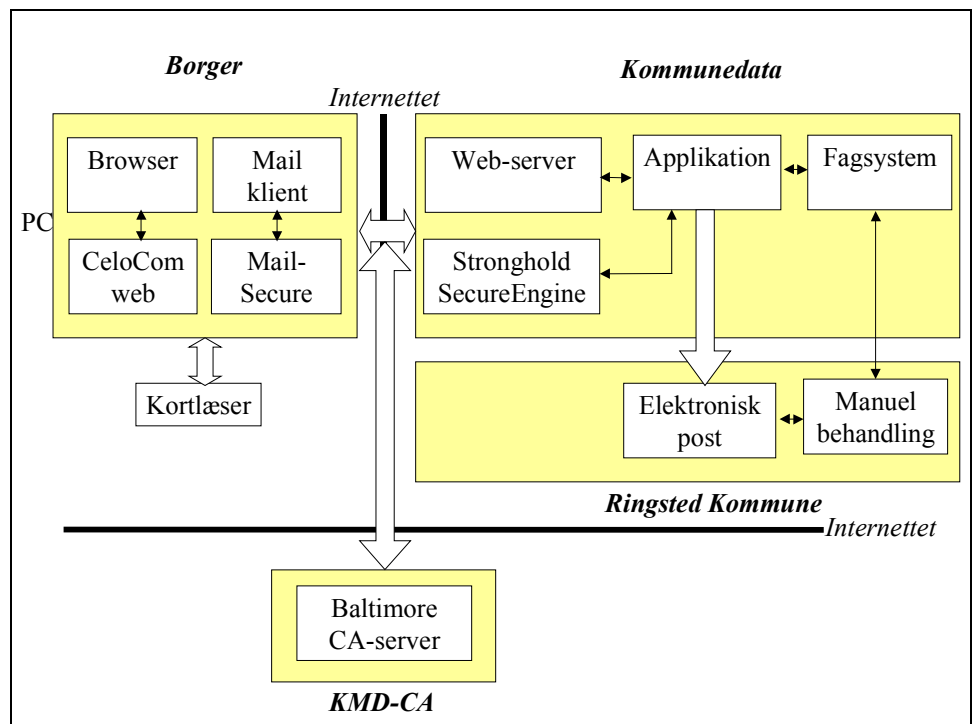
Anvendelsen af digital signatur

Brugen af digital signatur sikrer, dels at blanketter indsendt til kommunen via Internettet kommer fra den borger, som står som afsender, dels at indholdet ikke er blevet ændret af tredjepart.

Løsningen i Ringsted Kommune er baseret på, at borgeren udfylder blanketten på skærmen og underskriver denne elektronisk, før den sendes til kommunen. Projektet anvender smart card til opbevaring af borgerens private nøgle og digitale certifikat.

Den tekniske løsning giver både mulighed for digital signatur på HTML-forms (ansøgninger) og for at sende digitalt signeret elektronisk post til Ringsted Kommune. Et antal medarbejdere i Ringsted Kommune er blevet udstyret med et medarbejdercertifikat, og der er oprettet en fælles postkasse med et tilhørende virksomhedscertifikat (for Ringsted Kommune).

Den tekniske løsning er illustreret i figuren nedenfor.



Løsningen understøtter Microsoft Internet Explorer og Netscape Communicator. For at opnå stærk kryptering anvendes en række tredjepartsprodukter, som altså skal være installeret på brugerens PC. Kortlæseren tilsluttes via tastaturporten.

Den udviklede applikation er i et vist omfang integreret med bagvedliggende fagsystemer. Således kan blanketter forudfyldes med personlige oplysninger, eksempelvis navn, adresse, CPRNR m.m. For at kunne identificere brugeren, har KMD-CA kodet et person-id på de anvendte certifikater, som Kommunedata efterfølgende entydigt kan "oversætte" til personens CPRNR.

Kommunedata fungerer ligeledes som CA i løsningen. CA-serveren drives af Kommunedatas KMD-CA.

Status

Ringsted Kommunes nye hjemmeside blev officielt åbnet i august 1999. Løsningen til digital signatur var dog først parat i december 1999, og den 17. december 1999 modtog kommunen den første digitalt underskrevne blanket fra en borger.

Oprindeligt var der planlagt deltagelse af 500 borgere i forsøget, men dette antal blev reduceret til 250 og senere til 170 på grund af udgifter til borgerens udstyr.

Ud af de tilmeldte deltagere har 80 fået udstedt et personligt certifikat, og 53 har sendt digitalt underskrevet post (blanketter m.m.) til kommunen.

Opnåede resultater

Etableringen af Det Digitale Rådhus har udvidet rådhusets åbningstid til principielt 24 timer i døgnet.

På grund af det lille antal blanketter, der er modtaget elektronisk fra borgerne, er det vanskeligt at opgøre servicegevinsten for borgerne.

Tidsbesparelsen skal tillige ses i sammenhæng med den tid hver enkelt borger har anvendt til at installere systemet.

Kommunen har ikke opnået nogen rationaliseringsgevinst med løsningen. Dette skyldes, at løsningen til Det Digitale Rådhus ikke er integreret med kommunens fagsystemer. Kommunen modtager blanketter fra web-applikationen via elektronisk post, som efterfølgende udskrives og behandles i den traditionelle sagsgang.

Projektets videre forløb

På trods af en forholdsvis stor forhåndsinteresse fra borgerne har kun et lille antal faktisk installeret den gratis software til digital signatur og rekvireret et certifikat. Ud af ca. 280 interesserede personer har 80 borgere anskaffet sig et certifikat.

Ringsted Kommune har besluttet at gennemføre en målrettet kampagne for at involvere alle tilmeldte personer i projektet.

Muligheden for indsendelse af blanketter med digital signatur vil blive bevaret og udbygget i den nærmeste fremtid.

Vordingborg Kommune

Vordingborg Kommune har i samarbejde med ICL Danmark gennemført et pilotprojekt med henblik på modtagelse af byggetilladelser og ansøgninger om ejendomsoplysninger via Internettet.

Projektets formål

Formålet med pilotprojektet var at etablere en fuldstændig elektronisk sagsbehandling for visse serviceydelser, som kommunen tilbyder virksomheder. Herved kan der opnås en serviceforbedring, idet de kan betjene sig selv uafhængigt af åbningstider.

I forbindelse med projektet har kommunen oprettet en hjemmeside som indgang til ydelserne.



<http://www.tastselv.vordingborg.dk>

I pilotprojektet indgår følgende ydelser:

- Anmodninger om ejendomsoplysninger
- Ansøgninger om byggetilladelser.

Ansøgningerne sendes fra Vordingborgs hjemmeside direkte til kommunens sagsbehandlere.



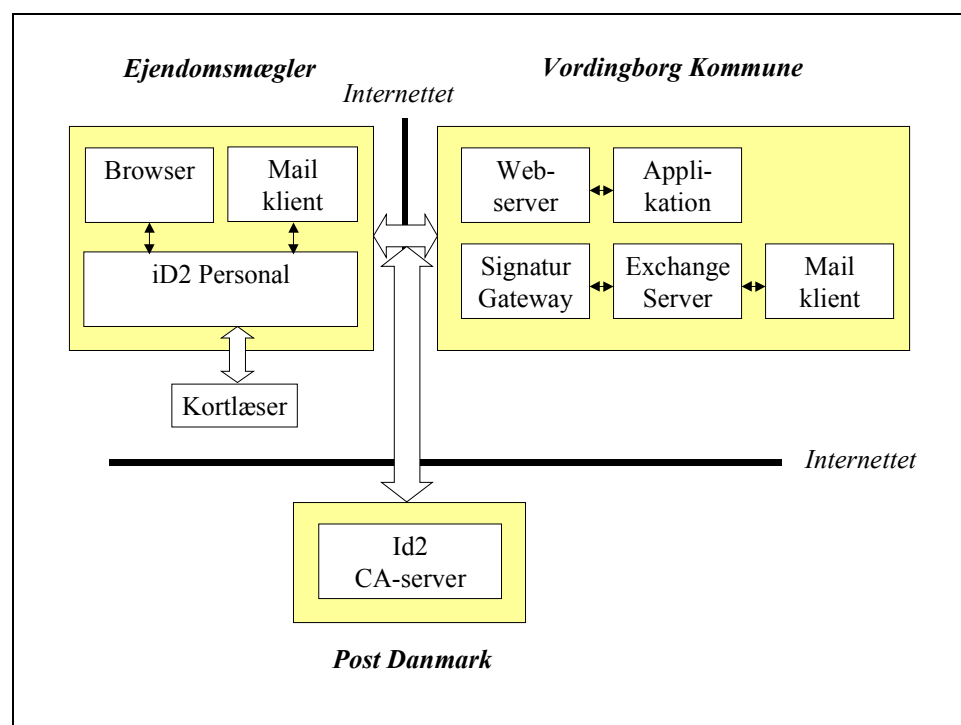
<http://www.tastselv.vordingborg.dk/servlets/EjendomGenerateFormServlet>

Løsningen giver tillige mulighed for indsendelse af digitalt underskrevet post til kommunens sagsbehandlere.

Anvendelsen af digital signatur

Løsningen anvender digital signatur på HTML-forms i forbindelse med indsendelse af ansøgninger. Vordingborg Kommune returnerer en digitalt signeret kvittering ved modtagelsen af en ansøgning.

Den tekniske løsning er illustreret i figuren nedenfor og er i øvrigt magen til den løsning, Erhvervs- og Selskabsstyrelsen har anvendt.



Brugeren (ejendomsmæglere og advokater) anvender en PC, hvortil en kortlæser er tilsluttet tastaturporten. Endvidere skal programmet iD2 Personal være installeret. Interaktionen med Vordingborgs Kommunes hjemmeside sker via en standard browser.

Hos Vordingborg Kommune modtages digitalt signerede ansøgninger af en Signatur Gateway, der verificerer den digitale signatur. Ansøgningen sendes via elektronisk post til sagsbehandleren. Sagsbehandleren overfører ansøgningen via sin post-klient til kommunens dokument- og sagshåndteringssystem.

Post Danmark fungerer som CA i løsningen og udsteder smart cards til løsningen.

Status

Vordingborgs tast-selv hjemmeside blev indviet 9. april 1999, og har

været i drift siden.

Løsningen er installeret hos 6 ejendomsmæglere, hvoraf de 4 anvender systemet intensivt, og hos et rådgivende ingeniørfirma, der dog ikke anvender systemet. Der er udstedt 10 smart cards til kommunens medarbejdere og 11 kort til medarbejdere hos ejendomsmæglere. Endvidere er systemet installeret på 3 arbejdspladser hos et ingeniørfirma.

Der modtages gennemsnitlig 2 transaktioner pr. dag fra ejendomsmæglere vedrørende anmodning om ejendomsoplysninger. Endvidere modtager kommunen digitalt underskrevet post fra de tilsluttede ejendomsmæglere.

Opnåede resultater

Indførelsen af elektroniske blanketter har givet en række fordele for de deltagende ejendomsmæglere og kommunen.

Sagsgangen i forbindelse med anmodning om ejendomsoplysninger er halveret fra ca. fire dage til to dage; i nogle tilfælde behandles en anmodning på en dag.

Den interne papirbaserede sagsgang i kommunen er blevet afløst af en effektiv papirløs sagsgang. Færre medarbejdere er involveret i sagsgangen, hvilket sparer tid og giver serviceforbedringer, idet medarbejderne har det fulde overblik på en sags status ved henvendelser.

Herudover har løsningen som sidegevinst lettet ejendomsmæglernes arbejdsproces i forbindelse med indsendelse af anmodninger, eksempelvis behøver mæglerne ikke længere at hente skemaer hos kommunen, udfylde skemaerne manuelt på skrivemaskine og indsende skemaerne via almindelig post til kommunen. Samtidig har Vordingborg Kommune indgået aftale med de involverede parter om automatisk træk af gebyrer m.v. via PBS, således er betalingselementet blevet effektiviseret.

Projektets videre forløb

På grund af projektets gode resultater har Vordingborg Kommune besluttet at fortsætte projektet. På kort sigt gøres en aktiv indsats for at motivere flere til at anvende de tilgængelige ydelser.

På længere sigt planlægges introduktion af flere elektroniske ydelser, rettet både mod virksomheder og private borgere.

Århus Amt

Århus Amt har gennemført et projekt omkring elektronisk forsendelse af regninger fra læger, tandlæger m.m. til Sygesikringen/Århus Amt. Projektet er gennemført i samarbejde med IT+.

Projektets formål

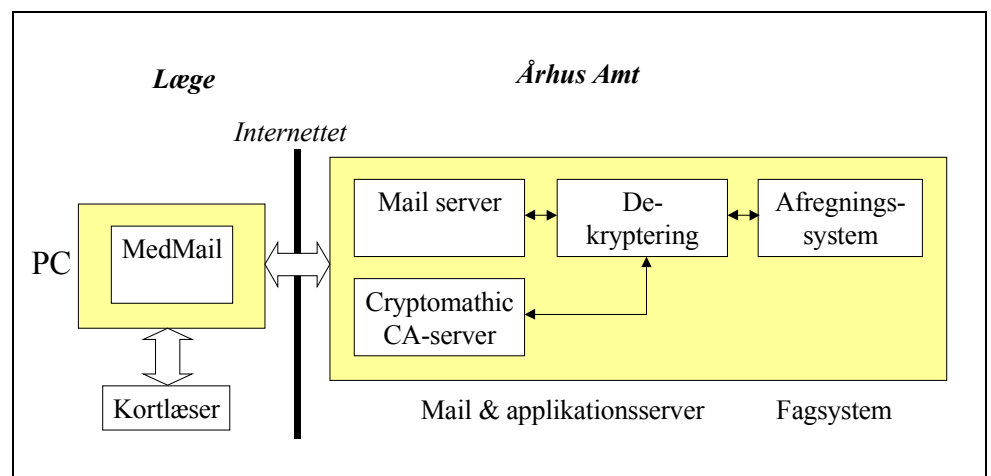
Projektet har til formål at give læger og tandlæger mulighed for at indsende regningsopgørelser elektronisk til Sygesikringen via Internettet. Førhen skete indsendelse af afregninger via VANS eller disketter med efterfølgende indsendelse af opgørelsen på papir (for kontrol af den elektronisk fremsendte opgørelse).

Løsningen giver læger og tandlæger mulighed for at fremsende opgørelser som elektronisk post med en digital signatur og uden efterfølgende indsendelse af en papirbaseret opgørelse. Løsningen rummer endvidere en økonomisk besparelse for brugerne, idet brugen af Internettet som kommunikationsmiddel er billigere end dedikerede VANS-forbindelser eller forsendelse af disketter.

Anvendelsen af digital signatur

Løsningen er baseret på elektronisk post med digital signatur. I forbindelse med forsendelsen udføres en række summeringer og grupperinger af regningerne til Sygesikringen. Brugerens digitale certifikat lagres på smart cards.

Den tekniske løsning er illustreret i figuren nedenfor.



Brugeren anvender programmet MedMail til indsendelse af afregninger. Ud over funktionalitet til afsendelse af elektronisk post med kryptering og digital signatur implementerer programmet nogle forbehandlinger af afregningerne.

Hos Århus Amt modtages den elektroniske post af amtets mail-server. En dedikeret server verificerer den digital signatur og dekrypterer forsendelsen. Herfra overføres afregningerne til amtets mainframe-system.

Status

Pilotprojektet har deltagelse af fire læger, to tandlæger og to apotekere. Samlet set indsender deltagerne mellem 60 - 70.000 enkeltregninger til Sygesikringen pr. måned.

De første afregninger blev indsendt via løsningen i april 1999. Fra juli 1999 indsendte deltagende læger, tandlæger og apotekere via løsningen. Indtil oktober 1999 indsendte deltagerne parallelt med den digitalt underskrevne afregning tillige afregninger på den hidtidige måde.

Opnåede resultater

Etableringen af den elektroniske løsning har haft følgende resultater for både deltagerne og Århus Amt.

Fordelene for læger, tandlæger og apotekere er:

- Eliminering af udgifter til porto i forbindelse med forsendelse af disketter og papirafregninger og udgifter til VANS for elektroniske overførelse af afregninger
- Nemmere afregningsproces
- Ingen genforsendelse på grund af defekte disketter.

Århus Amt har primært opnået:

- Fulldautomatisk sagsbehandling
- Tidsbesparelse i sagsbehandlingen idet integritetskontrollen af elektroniske afregninger sikres af den digitale signatur, hvorved den manuelle sammenligning med papir-baserede afregninger undgås
- Eliminering af tid forbrug på rekvirering af disketter i tilfælde af fejl.

Samtidig er sikkerheden omkring afregningsproceduren forbedret, idet afregninger krypteres under elektronisk transport (i modsætning til den tidligere transport på VANS).

Projektets videre forløb

På grund af projektets succes planlægger Århus Amt at udvide løsningen i år 2000. Potentielle anvendelsesområder inkluderer rekvisitioner af analyser til mikro-biologisk afdeling, svar fra laboratorier og sygehuse samt udveksling af patientjournaler.

På grund af projektets succes anbefaler Sygesikringen udbredelse af løsningen til andre amter.

3. Sammenfattende evaluering

I første del af dette kapitel gives en systematisk sammenfattende sammenligning og evaluering af pilotprojekterne. Projekternes ligheder og forskelligheder vurderes med hensyn til de formål, som Forskningsministeriet havde med pilotprojekterne. I kapitel 4 diskuteres nogle af de åbne problemstillinger, som pilotprojekterne har identificeret.

Forskningsministeriets formål med pilotprojekterne

I forbindelse med tildeling af støtte til pilotprojekterne opstillede Forskningsministeriet en række generelle krav, som projekterne skulle tilfredsstille:

- Pilotprojektet skulle sigte mod at sikre kommunikationen mellem det offentlige og borgerne eller virksomhederne i forbindelse med en konkret anvendelse, f.eks. et elektronisk selvbetjeningssystem, et system til elektronisk indberetninger, elektroniske blanketter, el.lign.
- Pilotprojektet kunne alternativt sigte mod at sikre kommunikation mellem offentlige institutioner i forbindelse med en konkret anvendelse, f.eks. sikker adgang til en offentlig database, sikker udveksling og behandling/registrering af dokumenter mellem offentlige myndigheder, el.lign.
- Pilotprojektet skulle kunne sættes i drift senest primo 1999.
- Pilotprojektet skulle være udformet således, at systemerne kan overgå til egentlig drift ved udløbet af projektperioden.
- Pilotprojektet skulle overholde markedsledende standarder for digital signatur, således at det kan danne basis for etablering af en universel sikker infrastruktur i Danmark.

De indkomne forslag til pilotprojekter blev, ud over overholdelse af generelle krav, vurderet efter følgende hovedkriterier:

- Serviceforbedringer som opnås for borgerne/virksomheder ved projektet.
- Rationaliseringsgevinster som opnås for myndigheden ved projektet.
- Robusthed over for den teknologiske udvikling.

I forbindelse med indkaldelsen af forslag til pilotprojekter var der udarbejdet et udkast til standarder og protokoller. Disse standarder og protokoller blev senere udbygget i samarbejde med de udvalgte pilotprojekter og Forum for Digital Signatur. Den oprindelige indkaldelse af forslag til projekter er gengivet i bilag 1.

Målgruppe og løsningstype

Pilotprojekterne varierer i deres målgruppe samt i bredden af målgruppen. Endvidere er løsningerne af forskellig art. Nogle løsninger er opbygget omkring signering af en HTML-form, mens andre er baseret

på elektronisk post.

Målgruppe

De enkelte pilotprojekter henvender sig til forskellige målgrupper. I nedenstående tabel er hvert pilotprojekt klassificeret, afhængig af om projektet:

- Vedrører elektronisk kommunikation mellem offentlig myndighed og borgere
- Vedrører elektronisk kommunikation mellem offentlig myndighed og erhverv
- Vedrører elektronisk kommunikation mellem offentlig myndighed og anden offentlig myndighed.

	Offentlig-Borger	Offentlig-Erhverv	Offentlig-Offentlig	Målgruppe
E&S-styrelsen		X		Erhverv
EU-direktoratet		X		Landmænd
SU-styrelsen	X			Studerende
Handelshøjskolen	X			Studerende
Næstved Kommune		X		Ejendomsagl.
Ringsted Kommune	X			Borgere
Vordingborg Kommune		X		Ejendomsagl.
Århus Amt		X		Læger m.m.

Som det fremgår af tabellen, henvender majoriteten af pilotprojekterne sig til erhvervsgruppen. SU-styrelsens og Handelshøjskolens projekter henvender sig til deres egne "kunder" og kan derfor godt karakteriseres som "erhvervsrettede". Kun projektet i Ringsted Kommune har et egentligt borger-fokus. Ingen pilotprojekter har behandlet elektronisk kommunikation med digital signatur mellem to offentlige myndigheder.

De fleste af pilotprojekterne har været målrettet mod en snæver målgruppe, eksempelvis landmænd, læger eller ejendomsmæglere.

Fokuseringen på erhvervsgruppen er i flere tilfælde begrundet i ønsket om at sikre et tilstrækkeligt højt antal transaktioner og volumen i løsningen. Vurderingen har været, at dette er vanskeligere at opnå med løsninger, der henvender sig bredt til borgere.

Løsningstype

Løsningernes funktionalitet kan klassificeres i tre grupper:

- *Indberetning*: Løsningen anvendes af brugergruppen til systematisk indberetning af oplysninger til den offentlige myndighed. Resultatet af indberetningen vil ofte blot være en kvittering for modtagelse af indberetningen.
- *Netblanket*: Løsningen anvendes af brugergruppen til indsendelse af en elektronisk ansøgning/formular - ofte som alternativ til en papir-baseret ansøgning.

- *Selvbetjening*: Løsningen anvendes af brugergruppen til elektronisk selvbetjening med den offentlige myndighed, som alternativ til eksempelvis telefonisk eller personlig henvendelse. Løsningen er karakteriseret ved, at svaret på en interaktion ikke blot er en kvittering, men et egentlig svar.

I nogle projekter er der naturligvis tale om grænsetilfælde – eksempelvis indeholder løsningen i Ringsted Kommune både elementer af netblanketter og egentlig selvbetjening. Løsningerne i Næstved og Vordingborg Kommuner indeholder også elementer af selvbetjening, men i disse tilfælde returneres svaret ikke som følge af en automatiseret proces, men som en elektronisk post på grundlag af en traditionel sagsbehandling.

	Løsningstype	Funktionalitet	Ny service	Ny kanal
E&S-styrelsen	Indberetning	Indbetaling ATP/Løn	X	X
EU-direktoratet	Netblanket	Ansøg hektarstøtte		
SU-styrelsen	Selvbetjening	SU-selvbetjening	X	X
Handelshøjskolen	Indberetning	Aflevering opgaver		X
Næstved Kommune	Netblanket	Ansøg ejendomsopl.		X
Ringsted Kommune	Selvbetjening	Borger-selvbetjening		X
Vordingborg Kommun	Netblanket	Ansøg ejendomsopl.	X	X
Århus Amt	Indberetning	Indberet afregninger	X	X

I tabellens højre side er det angivet, om løsningen etablerer en ny service (det vil sige om den offentlige myndighed med løsningen tilbyder en service, som ikke før var tilgængelig), eller om løsningen giver adgang til en eksisterende service via en ny kanal (det vil sige via Internettet).

Med undtagelse af EU-direktoratets løsning indeholder alle løsninger et element af "ny Internet-kanal".

Brugen af digital signatur kan således ses som en fremmede løsning, der åbner op for brug af elektronisk kommunikation via Internettet.

EU-direktoratet tilbød også elektronisk ansøgning af hektarstøtte via terminalforbindelse fra rådgivningscentre til en central server, før pilotprojektet blev igangsat. Uden brug af digital signatur var det dog påkrævet, at ansøgeren indsendte en papir-baseret underskrevet ansøgning til EU-direktoratet af juridiske årsager. Brugen af digital signatur forenkler således ansøgningsprocessen og er nødvendig for en fuldstændig elektronisk sagsbehandling.

En række pilotprojekter har - enten direkte eller indirekte som følge af pilotprojektet - haft mulighed for at tilbyde en ny service til brugerne. For eksempel tilbyder Vordingborg Kommune at "automatisere" betalingen af ejendomsoplysninger ved, at kommunen indgår en aftale med

brugeren om automatisk træk af gebyret via PBS. Erhvervs- og Selskabsstyrelsen giver deres kunder mulighed for at betale via PBS LeverandørService. SU-styrelsen giver studerende adgang til egne data i SU-systemet via Internettet. Århus Amt giver mulighed for indberetning via Internettet uden indsendelse af papirbaseret kontrolafregning.

Serviceforbedringer og rationaliseringsgevinster

I forbindelse med vurderingen af pilotprojekterne blev der lagt vægt på, at projekterne både resulterede i en serviceforbedring for brugerne og i en rationaliseringsgevinst for den offentlige myndighed.

I tabellen nedenfor er identificerede serviceforbedringer og rationaliseringsgevinster anført.

	Serviceforbedring	Rationaliseringsgevinst
E&S-styrelsen	Tidsbesparelse	Elek. Sagsbehandl.
EU-direktoratet	Tidsbesparelse	Elek. Sagsbehandl.
SU-styrelsen	Døgnåbent;tidsbesparelse	Færre henvendelser
Handelshøjskolen	Døgnåbent;tidsbesparelse	Elek. Sagsbehandl.
Næstved Kommune	Døgnåbent;tidsbesparelse	Elek. Sagsbehandl.
Ringsted Kommune	Døgnåbent	Elek. Sagsbehandl.
Vordingborg Kommun	Døgnåbent;tidsbesparelse	Elek. Sagsbehandl.
Århus Amt	Forsendelsesomkostninger	Auto. datafangst

Som det fremgår, indeholder de fleste pilotprojekter en serviceforbedring i form af en tidsbesparelse for brugeren. Endvidere er et væsentligt element i flere løsninger muligheden for "døgnåbent" – det vil sige systemet giver brugeren mulighed for at have interaktion med myndigheden uafhængig af den "normale" åbningstid.

Med undtagelse af projektet i Næstved Kommune har ingen pilotprojekter adresseret rationaliseringsgevinster som det primære formål med projektet.

Kendetegnet for alle projekter er dog, at muligheden for elektronisk sagsbehandling er identificeret.

Pilotprojekterne giver således isoleret set ikke belæg for egentlige konklusioner omkring rationaliseringsgevinster ved indførelse af systemer med digital signatur.

Alle projekter ser dog potentielle rationaliseringsgevinster ved elektronisk sagsbehandling, og at disse gevinster ikke i samme omfang ville kunne realiseres uden brug af digital signatur.

Løsningens opbygning

Hovedelementerne i løsningerne er angivet i tabellen nedenfor. Der sondres mellem brug af smart cards eller software-baserede løsninger, og om løsningen er baseret på digital signatur på HTML-forms eller elektronisk post (emails). Endvidere er den estimerede anvendeshyppighed angivet som enten sjældent, regelmæssigt eller hyppigt.

	Metode	Smart card	Anvendeshyppighed
E&S-styrelsen	Form/email	X	Hyppigt
EU-direktoratet	Form	X	Sjældent
SU-styrelsen	Form	X	Regelmæssigt
Handelshøjskolen	Form		Sjældent
Næstved Kommune	Email		Regelmæssigt
Ringsted Kommune	Form/email	X	Sjældent
Vordingborg Kommune	Form/email	X	Regelmæssigt
Århus Amt	Email	X	Hyppigt

Som det fremgår af tabellen, anvender alle pilotprojekter på nær projekterne på Handelshøjskolen og i Næstved Kommune smart cards til lagring af brugerens private nøgle/certifikat.

Handelshøjskolen havde oprindeligt planlagt brug af smart cards, men overgik til en software-løsning på grund af driftsproblemer. Næstved Kommune valgte ikke at bruge smart cards af strategiske hensyn: En ren software-løsning blev vurderet lettere at udbrede og mere økonomisk rentabel.

Løsningerne hos Erhvervs- og Selskabsstyrelsen og Århus Amt har høj anvendeshyppighed. Eksempelvis anvendes løsningen i Århus Amt hver uge/måned, og antallet af transaktioner er højt pr. bruger. Løsningerne hos SU-styrelsen, Næstved Kommune og Vordingborg Kommune anvendes regelmæssigt, men kun med få transaktioner pr. gang. Eksempelvis anvendes løsningen i Vordingborg Kommune ca. to gange om dagen (med 7 brugere). De øvrige løsninger anvendes kun sjældent. Løsningen hos EU-direktoratet anvendes kun i forbindelse med en årlig hektarstøtteansøgning; mens løsningen hos Handelshøjskolen kan anvendes ved hver opgave-aflevering. Ringsted Kommunes løsning tilbyder en bred vifte af service-ydelser, men den typiske borger vil kun sjældent anvende hver ydelse.

Bemærk at angivelsen af løsningens hyppighed med hensyn til anvendelse ikke er relateret til løsningens afprøvning i pilotperioden. Eksempelvis har Erhvervs- og Selskabsstyrelsens løsning kun været åbent i en kort periode, selvom løsningen på sigt kan anvendes hyppigt. Løsningerne hos EU-direktoratet og på Handelshøjskolen har kun været afprøvet i een situation. Dette forhold må naturligvis indgå ved

vurderingerne af brugernes rapportering omkring brug af løsningerne.

Løsningens omfang

I det følgende sammenholdes pilotprojekterne med hensyn til antal pilotbrugere, pilotperiode og brugeroplevelser i pilotperioden.

Antal pilotbrugere

Pilotprojekterne har haft differentierede antal pilotbrugere og sammensætning. Antallet af brugere, både det planlagte og det faktiske, er angivet i tabellen nedenfor. SU-styrelsen har i maj 2000 endnu ikke igangsat drift af pilotløsningen, og har derfor ingen faktiske brugere.

	Planlagt brugere	Faktisk brugere	Bruger-deltagelse	Bemærkning
E&S-styrelsen	100	70	70%	
EU-direktoratet	500	337	67%	
SU-styrelsen	1.000	0	0%	Løsning er ej i drift
Handelshøjskolen	74	62	84%	
Næstved Kommune	13	5	38%	24 certifikater
Ringsted Kommune	280	53	19%	106 certifikater
Vordingborg Kommun	7	4	57%	
Århus Amt	8	8	100%	

I tabellen er forholdet mellem antallet af planlagte brugere og antallet af faktiske brugere angivet. Dette tal skal dog tages med forbehold. Eksempelvis har de udvalgte brugere ved Handelshøjskolen ikke haft et reelt valg, mens det planlagte antal brugere i Ringsted Kommune mere er udtryk for antal interesserede, hvoraf så kun 19% rent faktisk har anvendt løsningen efterfølgende.

Endvidere er der stor forskel i den måde, hvorpå de udvalgte brugere er blevet gjort bekendt med løsningen og muligheden for at anvende den. Eksempelvis har EU-direktoratet udbredt løsningen til konsulentcentre, der efterfølgende har brugt løsningen på vegne af de reelle brugere (nemlig landmændene).

Kendetegnet for projekterne med et lille antal planlagte brugere er, at det har været lettere for projektet at animere brugerne til faktisk at anvende løsningen – hvis de overhovedet var interesserede; eksempelvis ved telefonisk henvendelse eller lignende. Tilsvarende har EU-direktoratet haft en fordel ved, at løsningen blev anvendt af konsulenter på vegne af landmænd, idet EU-direktoratet derved kunne målrette en kampagne for løsningen mod et lille antal personer fremfor mod hele målgruppen.

Samlet set har pilotprojekterne henvendt sig til et lille antal brugere, og antallet af brugere, der rent faktisk har gennemført transaktioner i løsningerne, er beskedent. Der er dog intet der indikerer, at de erfaringer

og resultater, som pilotprojekterne har frembragt, ville have været anderledes, hvis løsningerne havde været anvendt af flere brugere.

Flere pilotprojekter rapporterer, at flere potentielle brugere har meldt deres interesse i og forståelse for brugen af digital signatur, men har ikke set noget behov for løsningerne. Dette afspejler sig også i ovenstående tal.

Pilotperiode

Driftsperioden for de enkelte pilotprojekter er summeret i nedenstående tabel. I driftsperioden er ikke medregnet eventuelle afprøvningsperioder.

	Driftsperiode	Uafbrudt drift	Bemærkning
E&S-styrelsen	April/00	X	Ca 14 dages drift
EU-direktoratet	Mar/99 - Apr/99	X	
SU-styrelsen	N/A	N/A	Ej i drift
Handelshøjskolen	Oktober/99	X	I drift en dag
Næstved Kommune	Nov/99 - nu		
Ringsted Kommune	Dec/99 - nu	X	
Vordingborg Kommune	April/99 - nu	X	
Århus Amt	Juli/99 - nu	X	

Løsningerne udviklet af Erhvervs- og Selskabsstyrelsen, EU-direktoratet og Handelshøjskolen har alle kun været i drift i en kort tidsperiode. SU-styrelsens løsning er ved pilotprojekternes officielle afslutning endnu ikke i drift, men er dog blevet afprøvet.

Løsningerne hos Vordingborg, Næstved og Ringsted Kommuner samt Århus Amt har alle været i længerevarende drift og er fortsat i drift.

De fleste løsninger har været i uafbrudt drift siden ibrugtagningen. Løsningen implementeret hos Næstved Kommune har været ramt af en række tekniske problemer, der har bevirket, at løsningen ikke har været tilgængelig i en kortere periode.

De korte pilotperioder for nogle af projekterne betyder naturligvis, at erfaringsopsamlingen hos brugerne er begrænset. Endvidere har pilotprojekterne ikke haft mulighed for at vurdere mere langsigtede konsekvenser ved løsningerne.

Eksempelvis: Er løsningerne følsomme over for installationer på klientmaskiner? Er løsningernes brugergrænseflader også velegnede, når brugerne opbygger kompetence og kendskab til disse? Har brugerne ændret opfattelse om løsningerne over tid?

Det vurderes, at det samlede antal transaktioner har været tilstrækkeligt højt til, at den offentlige myndigheds erfaringer med løsningerne kan

tillægges vægt.

Generelle brugervurderinger

De enkelte pilotprojekter har gennemført en mere eller mindre omfattende evaluering af brugernes generelle vurdering af løsningen. Vurderingen er gengivet i tabellen nedenfor.

	Brugernes tilfredshed	Bemærkning
E&S-styrelsen	Tilfredshed med løsningen	
EU-direktoratet	Positive over for løsningen	Løsningen må ikke forsinke arbejdsgangen
SU-styrelsen	N/A	Løsning ej i drift
Handelshøjskolen	Tilfredshed med løsningen	Problem ved aflevering af store opgaver
Næstved Kommune	Væsentlig serviceforbed.	
Ringsted Kommune	Positive over for løsningen	Tekniske problemer er en barriere
Vordingborg Kommun	Positive over for løsningen	
Århus Amt	Tilfredshed med løsningen	

Generelt har alle deltagende brugere været positive eller tilfredse med løsningen. I flere tilfælde har tilfredsheden hos brugerne dog først meldt sig, efter en indledende barriere er blevet forceret. Dette kan for eksempel være installations eller forståelsesproblemer ved løsningen.

Brugerne påpeger i flere tilfælde, at løsningerne (det vil sige brugen af digital signatur) ikke i unødigt grad må nedsætte effektiviteten i arbejdsprocessen. Omvendt kan de fleste brugere se potentialet i brugen af digital signatur og har således forståelse for, at løsningen – og den kompleksitet løsningen medfører – er nødvendig for at de offentlige myndigheder kan stille en given service til rådighed via Internettet.

Brugernes holdning til løsningerne afspejler naturligvis løsningernes samlede funktionalitet – ikke brugen af digital signatur i sig selv. Den digitale signatur muliggør udbydelse af nogle serviceydelser via Internettet, som ellers ikke ville være mulige. Mange brugere ser den digitale signatur som et "nødvendigt onde" fremfor en parallel til den håndskrevne signatur. Dette betyder også, at brugen af digital signatur ikke må være for kompleks i forhold til den service, som udbydes.

Årsag til brugerfrafald

De deltagende brugere har generelt været tilfredse med løsningen, men alligevel har et antal potentielle pilotbrugere valgt ikke at anvende løsningen. De væsentligste årsager er angivet i tabellen nedenfor.

	Primære årsag til at nogle brugere har valgt ikke at anvende løsningen
E&S-styrelsen	1) Installation af løsning
EU-direktoratet	1) Mer-tidsforbrug ved brug af løsning (certifikat-generering) 2) Umuliggjort pga firewall
SU-styrelsen	N/A (løsning ej i drift)
Handelshøjskolen	1) Umuliggjort pga firewall
Næstved Kommune	1) Ikke behov for løsning 2) Installation af løsning
Ringsted Kommune	1) Installation af løsning 2) Ikke behov for løsning
Vordingborg Kommune	1) Ikke behov for løsning
Århus Amt	

Der har været to primære årsager til, at pilotbrugere har opgivet at anvende løsningen.

Tekniske problemer, især i forbindelse med installation af nødvendig software og kortlæser, har afholdt brugere fra at anvende løsningen.

I de fleste pilotprojekter har en massiv IT-støtte bevirket, at mange tekniske problemer er blevet løst undervejs, men nogle brugere har helt opgivet.

Manglende behov for løsningen har ligeledes være årsag til en del frafald.

Denne årsag er naturligvis nøje forbundet med løsningens formål og målgruppe. Det er unægtelig lettere for en pilotbruger i Ringsted Kommune end i Århus Amt at fravælge løsningen på grund af manglende behov.

Endelig har en del brugere fravalgt løsningen på grund af en kombination af tekniske problemer og manglende behov: Indsatsen ved installation og konfiguration af løsningen er simpelthen blevet vurderet til ikke at stå mål med gevinsten. Der er grænser for, hvor meget besvær man vil gå igennem for at kunne gennemføre nogle få transaktioner lidt mere effektivt med myndighederne.

Pilotprojekterne har tydeligt vist, at kendskabet til digital signatur er lille, og at det ikke kan forventes at små organisationer og private borgere har tilstrækkeligt kendskab til teknologien til at afhjælpe installations- og driftsproblemer.

Udvikling og drift

I det følgende sammenholdes udviklings- og driftserfaringer fra de enkelte pilotprojekter.

Udviklingserfaringer

De fleste pilotprojekter har været nødsaget til at udsætte åbningen af løsningen på grund af forsinkelser i udviklingsarbejdet. De væsentligste årsager til udviklingsforsinkelser er opsummeret i tabellen nedenfor.

	Udvikling forsinket	Produkt- valg	Fag- system	Andet
E&S-styrelsen	X		X	Integration med kortlæser
EU-direktoratet				
SU-styrelsen	X		X	Problem med CA-programmel
Handelshøjskolen	X	X		Tekniske begrænsninger i smart card
Næstved Kommune	X			Problem med CA-programmel
Ringsted Kommune	X	X		Etablering af CA
Vordingborg Kommune				
Århus Amt				

Pilotprojekterne har oplevet en bred vifte af problemer.

Fælles erfaringer har været problemer med kommunikation med CA-programmel, integration med kortlæsere og diverse platform- og software-afhængigheder.

Projekterne på Handelshøjskolen og i Ringsted Kommune blev forsinket på grund af større tidsforbrug til produktvalg end forudset. En del af forsinkelserne kan tilskrives bestræbelserne på at overholde de standarder, som blev krævet af Forskningsministeriet, herunder kravet om stærk kryptering. Flere projekter, bl.a. projekterne hos Erhvervs- og Selskabsstyrelsen og SU-styrelsen, er blevet forsinket på grund af tilpasninger og udvikling på bagvedliggende fagsystemer med henblik på integration med pilotløsningen.

Installations- og driftserfaringer

De fleste løsninger kræver installation og konfiguration af tredjeparts software på brugernes PC, før løsningen kan anvendes. I denne sammenhæng betegnes software, der ikke normalt installeres som en del af "standard-opsætningen" af en PC, som værende tredjeparts software.

Installation af software og/eller hardware stiller altid visse krav til brugerens edb-kundskaber og giver mulighed for fejl.

I tabellen nedenfor er de problemer, brugerne oplevede som følge af installation og konfiguration af løsningen, gengivet.

	Installationsproblemer (software)	Installationsproblemer (hardware)	Konfigurationsproblemer	Bemærkning
E & S-styrelsen	X	X		Kortlæser
EU-direktoratet			X	Firewall
SU-styrelsen	N/A	N/A	N/A	Ej i drift
Handelshøjskolen			X	Firewall
Næstved Kommune	X		X	Netscape
Ringsted Kommune	X	X		
Vordingborg Kommune		X		Kortlæser
Århus Amt		X		Kortlæser

Som det fremgår af tabellen, har alle projekter i et større eller mindre omfang oplevet problemer omkring installation af den software eller hardware (kortlæsere), som er del af løsningen.

Omfanget af installationsproblemer afhænger naturligvis af antallet af tredjepartsprodukter, som indgår i løsningen, men sammenhængen er ikke direkte.

Eksempelvis består løsningen i Næstved Kommune "blot" af Netscape Communicator (der kan betegnes som et standardprodukt) samt en plugin, men alligevel har projektet oplevet installations- og konfigurationsproblemer hos brugere, der anvender andre typer mail-systemer.

Et andet hyppigt problem har været manglende kontakt mellem bruger og CA-server på grund af restriktive firewalls på pilotbrugerens arbejdsplads. En firewall vil normalt ikke være "åben" for LDAP-opslag mod en CA-server, og ændring af en firewall-konfiguration forudsætter kompetence, der normalt ikke er tilstede i mindre IT-organisationer.

Alle projekter, der anvender kortlæsere og smart cards, har rapporteret problemer vedrørende installation af kortlæseren.

Der har været anvendt kortlæsere, der tilsluttes PC'ens serielle-, muse- eller tastaturport, men i flere tilfælde har der manglet frie porte, eller de medfølgende systemdrivere har ikke virket eller været i konflikt med anden software. Samtidig har flere projekter oplevet, at en type kortlæser ikke kan anvendes til forskellige styresystemer (eksempelvis Windows 98 eller Windows NT).

På grund af løsningernes komplekse opbygning er disse tillige sårbare over for ændringer i PC'ernes opsætning. Eksempelvis har nogle projekter erfaret, at når brugerne installerer andre programmer kan dette påvirke digital signatur-løsningen i en sådan grad, at den ikke længere fungerer.

Pilotprojekterne har tydeligt vist, at antallet af tredjepartsprodukter bør holdes på et minimum, og at løsningerne i så høj grad som muligt bør baseres på standard-software, som kan forventes installeret på målgruppens PC'er.

Ud over installationsproblemer på brugersiden har flere projekter også rapporteret om problemer med installation af systemet hos myndighederne. Problemerne har naturligvis generelt været størst der, hvor integrationen med bagvedliggende fagsystemer er stor. Installation og integration af løsningerne kræver spidskompetence, og denne viden besiddes ofte kun af de enkelte systemleverandører.

Samtidig er systemer på grund af teknologiens manglende modenhed sårbare over for opdateringer og ændringer. Eksempelvis bevirkede en År 2000-opdatering i Næstved Kommune, at digital signatur-systemet ophørte med at fungere.

Teknologi og standarder

I dette afsnit sammenholdes de teknologier og standarder, der er anvendt i de forskellige projekter.

Anvendte teknologier

Pilotprojekterne har anvendt et antal tredjepartsprodukter i den samlede løsning. Brugen af tredjepartsprodukter er primært begrundet i kravet om stærk kryptering samt brug af smart card.

De enkelte løsningers sammensætning er summeret i tabellen nedenfor. Bemærk, at projekterne hos Erhvervs- og Selskabsstyrelsen og Vordingborg Kommune anvender samme løsning (ICL/DigiSign2000), og at projekterne hos EU-direktoratet og SU-styrelsen er baseret på de samme komponenter (IT+/Secure Web client).

	Klient-software	CA-server	Kortlæser
E&S-styrelsen	Explorer/Netscape, DigiSign2000 (iD2 SSL klient, iD2 WebSigner-plugin, iD2 WebSign verifikator)	Id2	GemPlus GCR410/ GCR420
EU-direktoratet	Explorer/Netscape, IT+ Secure Web client	Cryptomathic	GemPlus 410
SU-styrelsen	Explorer, IT+ Secure Web client	Cryptomathic	Gemplus GCR420
Handelshøjskolen	Explorer/Netscape, Entrust Entelligence	Entrust	N/A
Næstved Kommune	Netscape, Fortify plugin	IBM Vault Registry	N/A
Ringsted Kommune	Explorer, Netscape, CeloCom Web (128bit SSL klient), Mailsecure plugin	Baltimore	GemPlus CGR410/ CCR420
Vordingborg Kommune	Explorer/Netscape, DigiSign2000 (iD2 SSL klient, iD2 WebSigner-plugin, iD2 WebSign verifikator)	Id2	GemPlus GCR410/ GCR420
Århus Amt	MedMail	Cryptomathic	GemPlus GCR410

En væsentlig udfordring for projekterne har været kravet om stærk kryptering ved kommunikation mellem en web-browser og web-server. På grund af amerikanske eksportrestriktioner implementerer Microsoft Internet Explorer og Netscape Navigator kun 56bit kryptering (SSL). For at opnå stærk kryptering baseret på 128bit nøgler har anvendelse af diverse tredjepartsprodukter været nødvendig. Da USA netop har ophævet eksportforbudet mod software med stærk kryptering, er denne hindring nu fjernet.

Ud over produkterne angivet i tabellen, har også systemdrivere til kortlæsere m.m. skullet installeres (i tilfælde hvor kortlæsere blev anvendt). Sluttelig skulle brugeren i flere tilfælde installere et eller flere certifikater i browser/mail-programmer, før løsningen kunne tages i brug.

Brugen af tredjepartsprodukter gør naturligvis, at brugeren er bundet til at anvende den PC, hvorpå softwaren er installeret. Brugen af smart cards sikrer således ikke mobilitet, men giver kun ekstra beskyttelse af brugerens private nøgle (idet nøglen ikke lagres på brugerens PC). Ingen af pilotprojekterne understøtter ikke-Windows platforme, eksempelvis Mac eller Unix-miljøer.

Pilotprojekterne viser tydeligt, at det endnu ikke er praktisk muligt at opnå høj mobilitet ("roaming") med de udviklede løsninger.

Brugerne er i praksis tvunget til at anvende løsningen på deres "egne" PC'er.

Standarder

Forskningsministeriet stillede som krav for støtte til pilotprojekterne, at de opfyldte gældende standarder og protokoller. De vigtigste er gengivet i tabellen nedenfor.

	Certifikat	Chipkort	Kommunikation	Nøglelængde
E & S-styrelsen	X.509v3	PKCS #11	HTTPS / S-MIME	128 / 1024
EU-direktoratet	X.509v3	PKCS #11	HTTP	1024
SU-styrelsen	X.509v3	PKCS #11	HTTP	1024
Handelshøjskolen	X.509v3	N/A	MIME	1024
Næstved Kommune	X.509v3	N/A	S-MIME	128 / 1024
Ringsted Kommune	X.509v3	PKCS #11	HTTPS / S-MIME	128 / 1024
Vordingborg Kommune	X.509v3	PKCS #11	HTTPS / S-MIME	128 / 1024
Århus Amt	X.509v3	PKCS #11	S-MIME	1024

Alle opstillede standarder er gengivet i bilag 1.

Alle pilotprojekter har opfyldt kravene til standarder og protokoller, som Forskningsministeriet stillede for accept af projekterne.

Der er dog alligevel en vis variation i projekterne. Eksempelvis er projekterne i Næstved Kommune og på Handelshøjskolen begge baseret på, at brugerne indsender signeret elektronisk post til myndighederne. Næstved Kommune har implementeret løsningen ved hjælp af en plug-in, der giver mulighed for stærk kryptering i Netscape Messenger. I Handelshøjskolens løsning krypteres og signeres den ønskede tekst eksternt og sendes som vedhæftet fil i en elektronisk post uden kryptering.

Endvidere er en række tekniske forhold ikke reguleret af standarderne. Eksempelvis anvender flere projekter IP-porte til opslag i CA-serveren eller til sikker kommunikation. Dette giver problemer for brugere som arbejder bag en firewall, der er lukket for IP-trafik ud over gængse standard kommunikationsporte.

Certifikater og deres anvendelser

Et centralt aspekt i løsninger baseret på public-key kryptering og signering er anvendelsen af certifikater. Alle løsninger anvender certifikater baseret på standarden X.509v3. Brugen af certifikater er opsummeret i nedenstående tabel. Der anvendes tre forskellige typer certifikater: Personcertifikater (P), medarbejdercertifikater (M) og virksomhedscertifikater (V).

	P	M	V	CA	LRA	Data på certifikat
E & S-styrelsen			X	PostDanmark/ PBS	Posthuse	CVR-nummer
EU-direktoratet			X	TeleDanmark	EU-direktoratet	
SU-styrelsen	X	X		TeleDanmark	Uddan.steder	Person-id
Handelshøjskolen	X			HHK	HHK	
Næstved Kommune		X	X	PBS	Tek.forvaltning	
						Person-id, medarb-id, CVR-nummer
Ringsted Kommune	X	X	X	KMD-CA	Kunde betjening	
Vordingborg Kommune			X	PostDanmark/ PBS	IT afdeling	CVR-nummer
Århus Amt			X	Århus Amt	Århus Amt	Ydernummer

Pilotprojekterne har ikke anvendt samme CA (Certificate Authority).

Handelshøjskolen og Århus Amt har valgt at opsætte egen CA-server og derved selv at udstede certifikater. EU-direktoratet og SU-styrelsen har anvendt TeleDanmark som driftsoperatør (TeleDanmark har ikke fungeret som en egentlig CA i forbindelse med pilotprojekterne, men blot afviklet CA-applikationen).

Pånær Erhvervs- og Selskabsstyrelsen, har projekterne valgt egne LRA (Local Registration Authority). For Erhvervs- og Selskabsstyrelsen har det været naturligt at anvende lokale posthuse, idet projektets pilotbrugere geografisk er spredt over et større område.

Pilotprojekterne har ligeledes haft forskellige behov for data på certifikater. Fælles for projekterne er dog, at løsninger rettet mod virksomheder har behov for virksomhedens CVR-nummer, mens borgerrettede løsninger forudsætter et entydig identifikation. Ringsted Kommune og Kommunedata har valgt en løsning, der er baseret på person-id, der af Kommunedata kan "oversættes" til CPR-numre, mens eksempelvis Handelshøjskolen anvender de studerendes email-adresse til entydig identifikation.

Løsningernes fremtidige anvendelse

I dette afsnit diskuteres løsningernes fremtidige anvendelser.

Løsningens fortsatte eksistens

I forbindelse med ydelse af støtte til pilotprojekterne ønskede Forskningsministeriet, at løsningerne kunne gøres permanente, og at de blev opbygget på en sådan måde, at de kunne skaleres op.

I forbindelse med slutevalueringen af pilotprojekterne har hvert projekt taget stilling til, om løsningen skal gøres permanent, og i benægtende fald

hvorfor ikke. Dette er opgjort i tabellen nedenfor.

	Perma- nent?	I drift?	Bemærkning
E&S-styrelsen	X	X	
EU-direktoratet			Økonomisk umuligt at tilbyde kortlæsere og smart cards
SU-styrelsen			Økonomisk umuligt at tilbyde kortlæsere
Handelshøjskolen	X		
Næstved Kommune	X	X	
Ringsted Kommune	X	X	Omkostninger til udstyr/certifikater er hindring
Vordingborg Kommune	X	X	
Århus Amt	X	X	

EU-direktoratet har besluttet at stoppe med brugen af digitale signaturer på grund af manglende mulighed for at finansiere kortlæsere og chipkort til samtlige landmænd.

SU-styrelsen har ikke besluttet at stoppe med brugen af digitale signaturer. Pilotprojektet fortsætter i SU-styrelsens eget regi i hvert fald i 2000. SU-styrelsen har dog ingen mulighed for at udvide brugergruppen ud over de 1.000 studerende der var budgetteret med i det oprindelige forsøg, grundet den manglende mulighed for finansiering af kortlæsere og chipkort.

Erhvervs- og Selskabsstyrelsen vil gerne på længere sigt udbrede digital signatur til andre myndigheder. ATP valgte at stoppe deres løsning på grund af administrativ overbelastning. ATP tager først næste år stilling til hvilken digital signatur, man vil anvende fremover. Finansstyrelsen fortsætter i år 2000 med løsningen. Det er dog en forudsætning for fremtidig drift, at flere virksomheder tilmelder sig.

Handelshøjskolen og Århus Amt ønsker at fortsætte og udvide brugen af digital signatur.

Løsningerne i Næstved, Ringsted og Vordingborg kommuner fortsætter. Ringsted Kommune ser dog en væsentlig barriere i løsningens fortsatte brug i anskaffelse af nødvendigt udstyr.

Selvom størsteparten af projekterne gøres permanente, kan det ikke konkluderes, at løsningerne udbredes til en større målgruppe.

Flere projekter påpeger, at der ikke er økonomisk mulighed for at uddele gratis udstyr til brugerne. Samtidig vurderes det, at løsningen isoleret set ikke animerer potentielle brugere til selv at afholde omkostninger til udstyr.

Forudsætning for udbredelse af digital signatur

Pilotprojekterne har ligeledes overvejet, om og i givet fald hvilke, forudsætninger der er for løsningens udbredelse til flere brugere.

	Målgruppe	Forudsætning for digital signatur
E&S-styrelsen	Virksomheder	Uddannelsesbehov; høj volumen
EU-direktoratet	Landmænd	Gratis udlevering af udstyr og certifikater samt bredere anvendelsesmuligheder
SU-styrelsen	Studerende	Gratis udlevering af udstyr og certifikater
Handelshøjskolen	Studerende	Løsning ikke-afhængig af arbejdsplads
Næstved Kommune	Ejendomsmgl.	Lav pris på udstyr og certifikater
Ringsted Kommune	Borgere	Lav pris på udstyr og certifikater
Vordingborg Kommun	Ejendomsmgl.	Lav pris på udstyr og certifikater
Århus Amt	Læger m.m.	Ikke anført

Som det fremgår af tabellen, opfattes prisen på det nødvendige udstyr som en barriere for udbredelse af digital signatur. Afhængig af brugergruppen vurderes enten gratis udstyr eller udstyr til en tilpas lav pris som værende af afgørende betydning for brugen af løsningerne.

Næstved Kommune har som konsekvens heraf valgt en ren software-baseret løsning. Løsningen hos Handelshøjskolen er ligeledes software-baseret. Brugen af disse løsninger afhænger derfor ikke af anskaffelse af kort og kortlæsere etc.

Nogle af projekterne, der henvender sig til erhvervsvirksomheder, har fundet frem til, at virksomhederne faktisk er villige til at betale en vis pris for det nødvendige udstyr. Den aktuelle pris afhænger naturligvis af den gavn, som virksomhederne har af løsningen.

Derimod har projekterne, der henvender sig til borgere (inklusive studerende m.m.) konkluderet, at anvendelsesmulighederne skal være store, før disse målgrupper er villige til at investere i udstyret for egne midler.

Denne konklusion er ikke overraskende set i lyset af, at erhvervsvirksomheders hyppigere brug af løsningen gør, at udgiften hurtigere tjener sig ind igen.

Robusthed for teknologisk udvikling

Da Forskningsministeriet igangsatte brugen af digital signatur, var teknologien forholdsvis ny og standarderne ikke fuldstændig definerede. For at undgå at de udviklede produkter og tjenester skulle være forældede efter pilotprojekternes gennemførelse, ønskede Forskningsministeriet, at produkterne skulle være robuste over for den teknologiske udvikling.

En vurdering af dette aspekt er gengivet i tabellen nedenfor.

	Eksport-restriktion	Proprietær løsning	Løsningen moden?
E&S-styrelsen		X	X
EU-direktoratet			X
SU-styrelsen			X
Handelshøjskolen	X		X
Næstved Kommune	X		X
Ringsted Kommune	X		X
Vordingborg Kommune		X	X
Århus Amt		X	X

En væsentlig hindring for gennemførelsen af pilotprojekterne har været kravet om stærk kryptering. Stærk kryptering var indtil starten af år 2000 ikke implementeret i standardprodukter så som Microsoft Internet Explorer og Netscape Communicator på grund af eksportrestriktioner af amerikansk software. Denne eksportrestriktion er nu ophævet.

Lempelsen af eksportrestriktionen medfører, at brugen af tredjepartsprodukter kan reduceres, hvilket tilsvarende reducerer potentielle installations- og konfigurationsproblemer.

I tabellen er det angivet, om løsningen påvirkes af eksportrestriktionens lempelse, eksempelvis i reduktion af brugen af tredjepartsprodukter.

På trods af modenhedsproblemer under udviklingen og gennemførelsen af piloterne vurderer alle projekter, at de anvendte produkter inklusiv kort og kortlæsere nu kan betegnes som "modne".

Ingen af pilotprojekterne har identificeret grundlæggende forhindringer for at skalere løsningen op til flere brugere. I praksis vil udbredelse af løsningerne naturligvis kræve større server- og lagerkapacitet.

Som det fremgår, er flere af løsningerne proprietære i større eller mindre omfang. Eksempelvis understøttes løsningen anvendt af Erhvervs- og Selskabsstyrelsen og Vordingborg Kommune kun af een CA-udbyder. Løsningen i Århus Amt er baseret på en specifik mail-klient, men dette er egentlig ikke knyttet til den digitale signatur, men til at mail-klienten implementerer en given funktionalitet i forhold til systemerne hos Århus Amt.

4. Resultater, erfaringer og problemstillinger

I dette kapitel evalueres pilotprojekternes resultater i forhold til Forskningsministeriets oprindelige formål med projekterne. Endvidere gengives nogle af de erfaringer, som pilotprojekterne har opsamlet. Kapitlets sidste del beskriver de væsentligste identificerede åbne problemstillinger.

Formål med pilotprojekter

Forskningsministeriet havde tre overordnede formål med at igangsætte pilotprojekterne om brug af digital signatur. Disse var:

- At fremme brugen af digital signatur hos offentlige myndigheder.
- At fremme udviklingen af produkter og tjenester til digital signatur.
- At fremme udviklingen af nødvendige standarder og protokoller til digital signatur.

Ved evalueringen af indkomne forslag blev der endvidere lagt vægt på projekternes potentielle serviceforbedringer for brugerne, rationaliseringsgevinster for den offentlige myndighed, og at projekterne var robuste over for den teknologiske udvikling.

Brug af digital signatur hos offentlige myndigheder

Som en umiddelbar konsekvens af pilotprojekterne er der nu etableret løsninger med brug af digital signatur i Ringsted Kommune, Næstved Kommune, Vordingborg Kommune, Århus Amt og Erhvervs- og Selskabsstyrelsen. Endvidere har Handelshøjskolen i København intentioner om at fortsætte og udbygge de udviklede løsninger.

Pilotprojekterne har således igangsat brugen af digital signatur i Danmark.

Yderligere har et antal offentlige myndigheder høstet en række praktiske erfaringer omkring brugen af digital signatur, som kan være nyttig ved fremtidige udviklingsprojekter.

Flere projekter peger dog på finansiering af slutudstyr som en kritisk faktor for fortsat udbredelse af digital signatur.

Dette er naturligvis særligt kritisk for den type løsninger, hvor brugerne ikke kan forventes at være villige til at investere i udstyr for egen regning, medmindre udstyret tillige kan anvendes i andre sammenhænge. Dette gælder eksempelvis projektet hos EU-direktoratet, hvor det vurderes, at løsningen kun vil blive anvendt, såfremt EU-direktoratet sponsorerer udstyr til brugerne. Ligeledes peger SU-styrelsen og Ringsted Kommune på et uløst finansieringsproblem.

Parallelt med gennemførelsen af pilotprojekterne har IT-sikkerhedsrådet på opfordring af Forskningsministeriet udarbejdet en håndbog i praktisk brug af digital signatur. Denne indeholder råd og vejledninger omkring indførelse og anvendelse af digital signatur og bygger til en vis grad på nogle af de erfaringer, som pilotprojekterne har tilvejebragt. Håndbogen er tilgængelig på Forskningsministeriets hjemmeside.

Kommunernes Landsforening (KL) har udarbejdet en pjece omkring brug af digital signatur med udgangspunkt i elektronisk borgerservice. Omfattende løsninger til elektronisk borgerservice indeholder naturligt digital signatur, idet retslige ansøgninger og information kun derved kan videregives fra borgeren til den offentlige myndighed (eksempelvis kommunen). Samtidig kan borgerens certifikat anvendes som effektiv beskyttelse af følsomme oplysninger, som gøres tilgængelige for borgere via elektronisk borgerservice.

I forlængelse af pilotprojekterne har Kommunernes Landsforening opfordret Forskningsministeriet til at udarbejde en strategi for udbredelsen af digital signatur i forbindelse med selvbetjening i den offentlige sektor. Arbejdet er sat i gang i samarbejde med amter og kommuner og sker i regi af det Koordinerende Informationsudvalg under Forskningsministeriet

Udvikling af produkter og tjenester

Pilotprojekterne har igangsat udviklingen af et antal løsninger, og eksisterende produkter til digital signatur er blevet installeret og afprøvet.

Projekterne hos Erhvervs- og Selskabsstyrelsen og Vordingborg Kommune har resulteret i udviklingen af DigiSign2000 (ICL), og projektet hos Ringsted Kommune har resulteret i udviklingen af KMD Portal (Kommunedata). Projekterne hos EU-direktoratet og SU-styrelsen har anvendt produktet Secure Web Client (IT+); Handelshøjskolen i København har anvendt produkter fra Entrust (Protect Data) og projektet i Århus Amt har anvendt produktet MedMail (IT+). Projektet i Næstved Kommune var som eneste produkt baseret på funktionalitet indbygget i standard web-browser (Netscape Navigator).

Herudover er der anvendt et antal produkter til certifikat-generering og administration.

Pilotprojekterne har således initieret udvikling og markedsføring af en række produkter på det danske marked.

I forbindelse med pilotprojekterne er der tillige blevet etableret et antal nøglecentre. Disse har efter vedtagelsen af loven om digital signatur, der danner det juridiske grundlag for drift af nøglecentre, annonceret tilbud om certificeringsydelser. Disse er PostDanmark, PBS, Kommunedata og

TeleDanmark.

Ud over udviklingen af konkrete produkter og løsninger har flere virksomheder placeret strategisk udviklingsarbejde i Danmark, blandt andet initieret af pilotprojekternes brug af teknologi til digital signatur.

Udvikling af standarder og protokoller

Ved igangsættelse af pilotprojekterne havde Forskningsministeriet udarbejdet en anbefaling vedrørende brug af standarder og protokoller, som pilotprojekterne i størst muligt omfang skulle følge. Parallelt med gennemførelsen af projekterne blev standarderne videreudviklet i samarbejde med Forum for Digital Signatur.

Pilotprojekterne har opfyldt de stillede standarder og således verificeret deres praktiske anvendelighed.

I forlængelse heraf har Forum for Digital Signatur udarbejdet en standard for kodning af CPR-numre på personlige certifikater. Princippet i kodningen er, at et unikt person-id kodes i certifikatets serienummer-felt. Serienummeret kan dernæst anvendes som nøgle i et autorisationsregister af det modtagne system.

Desuden er der udarbejdet standard for indholdet af certifikater og profil til smart cards. Standarden er offentliggjort på Forskningsministeriets hjemmeside.

Loven om Digital Signatur blev endelig vedtaget 31. maj 2000, og blev udformet under hensyntagen til nogle af de erfaringer, som pilotprojekterne har tilvejebragt. Loven udgør det juridiske grundlag for drift af nøglecentre og gyldigheden af digital signatur.

Delkonklusion

Som beskrevet i foregående afsnit har pilotprojekterne tilfredsstillet de opstillede formål:

- Offentlige myndigheder i Danmark anvender nu digital signatur i praksis, og en række praktiske erfaringer er blevet gjort.
- Der er blevet udviklet et antal løsninger, som er blevet afprøvet i praksis. Dette har medvirket til, at en række produkter nu markedsføres i Danmark
- Der er opbygget en betydelig kompetence i offentlige og private organisationer.
- Standarder og protokoller er blevet specificeret, og deres anvendelighed i praksis er blevet demonstreret.

Pilotprojekterne har således opfyldt deres mission.

Der er dog fortsat en række problemstillinger, som skal adresseres. Disse beskrives i de efterfølgende afsnit.

Erfaringer fra pilotprojekterne

De enkelte pilotprojekter har opsamlet en række praktiske erfaringer i forbindelse med udviklingen og implementeringen af digital signatur i offentlige forvaltninger. Mange af disse erfaringer udspringer naturligt af, at teknologien var forholdsvis ukendt og umoden, da pilotprojekterne startede, og at pilotprojekterne kun havde begrænset adgang til tilsvarende erfaringer fra andre implementeringer.

Integration af systemer

En væsentlig forudsætning for opnåelse af rationaliseringsgevinster for offentlige myndigheder i forbindelse med indførelse af elektronisk selvbetjening og digital signatur er, at Internet-løsningen integreres med de bagvedliggende fagsystemer.

Løsninger baseret på elektronisk modtagelse af henvendelser fra borgere/virksomheder efterfulgt af traditionel sagsbehandling vil kun i ringe grad give anledning til besparelser.

Et eksempel på effektivisering af sagsbehandlingen findes på projektet i Næstved Kommune, der implementerede et stjernehøringsmodul til behandling af ansøgninger om ejendomsoplysninger og derved opnåede en markant besparelse i sagsbehandlingstiden.

Flere projekter har dog også erfaret, at integration mellem fagsystemer og Internet-baserede systemer er kompliceret og ofte en væsentlig hindring for projektets gennemførelse. Således er pilotprojektet hos SU-styrelsen blevet forsinket på grund af indførelse og ændringer i det bagvedliggende fagsystem. Andre projekter har erfaret, at den samlede løsning er meget sårbar over for ændringer og opgraderinger. En del af forklaringen er naturligvis, at teknologien og mange af de anvendte produkter er forholdsvis nye, og erfaringsgrundlaget fra tilsvarende løsninger er lille.

Organisatorisk implementering

De fleste pilotprojekter har anvendt mange ressourcer på den organisatoriske implementering af løsningen. Ressourcerne har især været anvendt på:

- Markedsføring af løsningen over for målgruppen for at tiltrække brugere.
- Oplysningsmøder m.m. for at informere brugerne om digital signatur og den bagvedliggende teknik.
- Opfølgingsmøder m.m. for at aktivere brugerne til at anvende løsningen.
- IT-støtte m.m. for at afhjælpe problemer, der har hindret brugerne i at anvende løsningen.

En væsentlig årsag til ressourceforbruget skyldes naturligvis, at bred, offentlig kendskab til digital signatur er begrænset.

Det må forventes, at behovet for information og uddannelse mindskes i takt med udbredelse af digital signatur.
--

En parallel kan drages til udbredelsen af Dankortet. Da løsningen blev introduceret, var interessen for sikkerhedsniveauet og ansvarsfordelingen meget stor. Nu er tilliden til Dankort-systemet så stor, at kun de færreste stiller spørgsmål ved brugen af Dankort.

Brugen af digital signatur stiller også krav til involverede medarbejdere i den offentlige forvaltning. Eksempelvis skal medarbejdere, der elektronisk behandler henvendelser fra borgere, have kendskab til brug af digital signatur. I praksis er det ofte blot et spørgsmål om at uddanne medarbejderne i, hvorledes de signerer og verificerer elektronisk post digitalt. Medarbejdere, der varetager en støtte- og informationsfunktion over for borgere og virksomheder, skal naturligvis have et mere detaljeret kendskab til den bagvedliggende teknik og funktionsmåde.

I takt med produkternes udvikling vil behovet for støttefunktioner til afhjælpning af tekniske problemer formentlig falde.

Erfaringerne fra pilotprojekterne er dog, at indtil videre kan myndighederne ikke forlade sig på, at tilstrækkelig kompetence til afhjælpning af tekniske problemer er tilstede i lokale IT-organisationer og hos private borgere.

Lovmæssige aspekter

Loven om Elektroniske Signaturer regulerer tilsynet med nøglecentre og udgør det juridiske grundlag for dokumenter med digital signatur.

Brug af digital signatur rejser dog en række lovmæssige problemstillinger, der ikke er omfattet af loven.

Anvendelse af digital signatur har flere formål: At sikre det elektronisk underskrevne dokumentets uafviselighed, autenticitet, og integritet. Dette har nogle konsekvenser for myndighedernes opbevaring og arkivering af modtagne dokumenter.

Skal den offentlige myndighed eksempelvis arkivere dokumenter med eller uden digital signatur?

Arkivering med digital signatur er problematisk, idet den digitale signatur har en begrænset levetid. Typisk vil et personligt certifikat eksempelvis have en levetid på ca. 2 år. Endvidere er myndighederne afhængige af det aktuelle nøglecenter. Hvis nøglecenteret eksempelvis ophører med at eksistere, kan myndigheden principielt ikke validere

brugerens certifikat og derved kontrollere ægtheden af den digitale underskrift. Problemstillingen er endnu værre, hvis dokumentet tillige er krypteret og derved ulæseligt uden en gyldig dekrypteringsnøgle.

Alternativt kan myndighederne vælge at arkivere borgerens dokument uden digital signatur. Dette er dog problematisk, idet den digitale signatur netop giver dokumentet juridisk gyldighed. I en eventuel tvist mellem afsenderen og myndighederne kan myndighederne principielt ikke længere hævde uafviselighed og integritet. Myndighederne kan også vælge at forsyne dokumentet med en betroet parts (notar) digitale signatur, som er garanteret validitet i et tilpas antal år. En sådan løsning forudsætter dog, at alle parter har tillid til den betroede tredjepart.

Problemstillingen er ligeledes aktuel i forbindelse med arkivering af offentlige dokumenter hos Statens Arkiv. På grund af ovennævnte problemstillinger vælger Statens Arkiv at arkivere dokumenter uden digital signatur og i ikke-krypteret form.

Åbne problemstillinger

Pilotprojekterne har trods deres succes også vist, at der fortsat er en række problemstillinger, som skal adresseres i forbindelse med udbredelsen af digital signatur.

Interoperabilitet

Der eksisterer i Danmark ikke et nationalt nøgle- og certificeringscenter. Udbydelse og drift af sådanne tjenester er overladt til markedet, men er dog reguleret af loven om elektronisk signatur, der bl.a. stiller krav til centrenes sikkerhedsniveau og tilsyn. Der er i dag et antal virksomheder, som udbyder certificeringstjenester tillige med et ukendt antal interne nøglecentre.

I praksis betyder dette, at offentlige myndigheder (og private virksomheder) som en del af etableringen af en løsning med digital signatur må vælge at gøre brug af et blandt flere nøglecentre. For den offentlige myndighed har det valgte nøglecenter primært to funktioner: At udstede certifikater til borgere (der ikke har et certifikat) og at validere gyldigheden af de certifikater, som brugerne anvender ved tilgang til løsningen. For brugerne er der dog en række konsekvenser.

Hvis en løsning aktivt gør brug af data på brugerens certifikat, eksempelvis et "kundennummer", kan brugeren kun anvende løsningen, såfremt han/hun er i besiddelse af et certifikat udstedt specifikt til ham/hende. Eksempelvis vil en løsning, der anvender person-id på certifikater (jf. standard for kodning af person-relaterede oplysninger på certifikater) være afhængig af kendskab til relationen mellem PID og certifikatets ejer - en oplysning som kun nøglecenteret besidder.

Omvendt kan det meget vel også tænkes, at nogle brugere ikke ønsker at

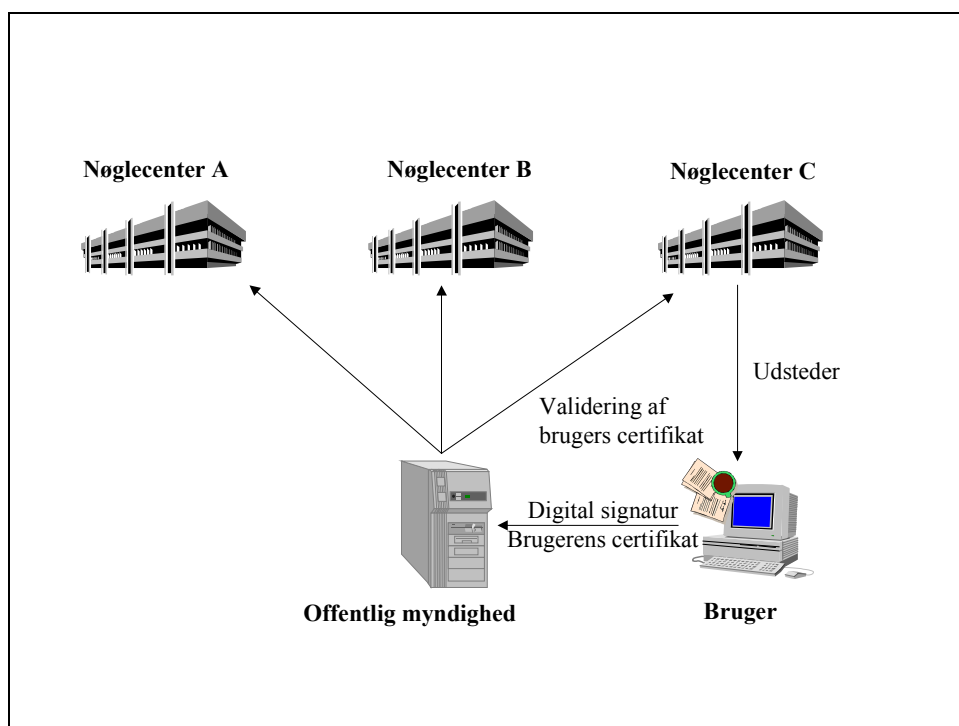
anvende samme certifikat/nøgle ved kommunikation med en offentlig myndighed som ved kommunikation med eksempelvis en bank. Nogle borgere kan ønske at holde adgangen til disse to organisationer adskilte.

For at stimulere brugen af offentlige løsninger med digital signatur, og for at undgå at offentlige løsninger bliver afhængige af et nøglecenter, er det formålstjenligt, at offentlige løsninger i størst muligt omfang kan acceptere certifikater udstedt af forskellige nøglecentre, så den enkelte bruger kun behøver eet certifikat til alle offentlige løsninger.

Dette kan opnås på flere måder.

- Den offentlige myndighed indgår aftale med flere nøglecentre om validering af certifikater.

I praksis betyder dette, at hvis det offentlige system skal validere et certifikat udstedt af nøglecenter C, kontakter den offentlige myndighed specifikt dette nøglecenter.

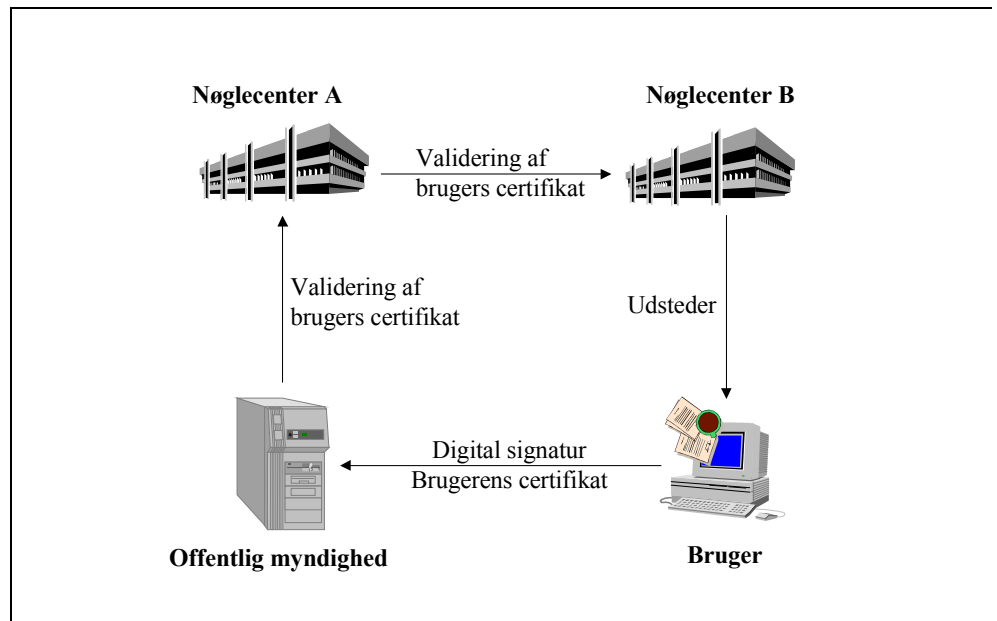


Fordelen ved denne model er, at den offentlige myndighed kan acceptere certifikater fra flere nøglecentre. Ulempen er, at den offentlige myndighed skal indgå aftale med og etablere teknisk infrastruktur til flere nøglecentre.

- De enkelte nøglecentre indgår aftale om at acceptere og validere hinandens certifikater.

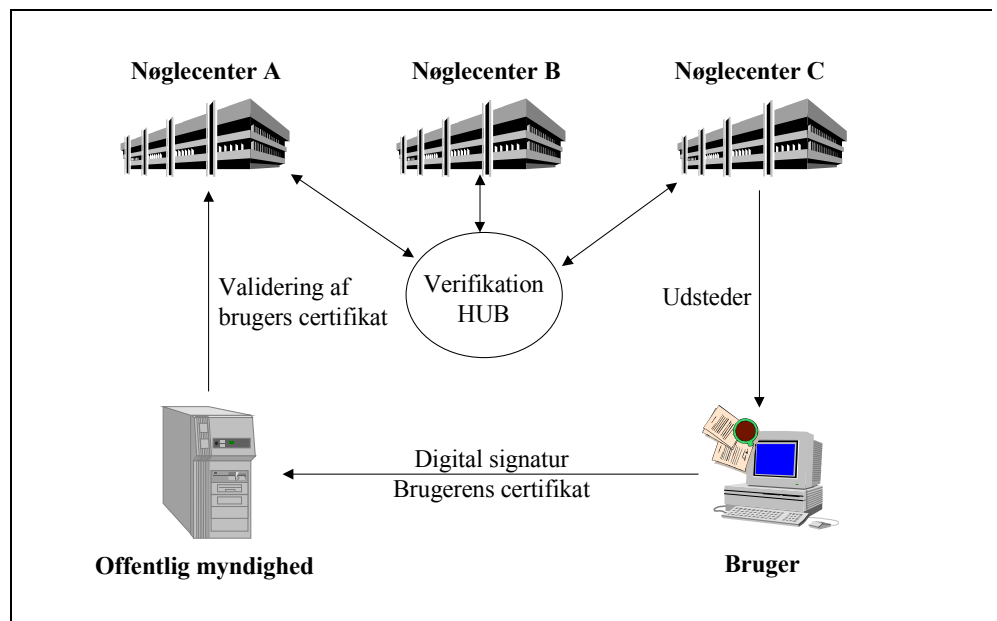
I praksis betyder dette, at hvis nøglecenter A bliver bedt om at validere et certifikat udstedt af nøglecenter B, så kontakter nøglecenter A – uden

systemet/brugeren aktivt gør noget – nøglecenter B og returnerer svaret til systemet/brugeren.



Fordelen ved denne model er, at hver offentlig myndighed (system) kun behøver at kontrahere med et nøglecenter, men alligevel kan acceptere certifikater fra andre nøglecentre. Ulempen ved løsningen er, at hver nøglecenter skal indgå individuelle aftaler med andre (relevante) nøglecentre. Løsningen etableres ved at de enkelte nøglecentre krydscertificerer hinanden.

- Der etableres en central enhed, der har ansvar for krydscertificering af nøglecentre.



Fordelen ved denne model er, at den offentlige myndighed kun behøver at indgå aftale med eet nøglecenter, og at hvert nøglecenter ligeledes kun skal krydscertificeres med een enhed.

Tekniske barrierer

Forskningsministeriet ønskede, at løsningerne, som pilotprojekterne udviklede, skulle være baseret på stærk kryptering (brug af 128bit/1024bit nøgler til kryptering/digital signatur). Da pilotprojekterne startede, var amerikansk software omfattet af USA's eksportforbud vedrørende software med stærk kryptering, og standard produkter så som Internet Explorer og Netscape Communicator implementerede derfor kun svag kryptering (56bit/512bit nøgler til kryptering/digital signatur). Pilotprojekterne måtte derfor finde alternative måder at implementere stærk kryptering - ofte under anvendelse af tredjeparts produkter.

USA har lempet eksportrestriktionen, hvilket betyder, at de fleste standard web-produkter nu understøtter stærk kryptering. For brugernes vedkommende har dette betydet, at installation af påkrævet software for anvendelse af løsninger med digital signatur bliver lettere, idet antallet af nødvendige produkter og programmer mindskes.

Fjernelsen af den amerikanske eksportrestriktion betyder dog ikke nødvendigvis, at digital signatur-løsninger udelukkende kan være baseret på standard web-produkter. Nogle løsninger kan eksempelvis forudsætte, at visse former for databehandling sker, inden data afleveres i digital signeret form. Dette er for eksempel tilfældet i løsningen udviklet af Århus Amt til indsendelse af afregninger, hvor post-programmet, som er en del af løsningen, foretager visse beregninger og grupperinger, før afregningen sendes.

Pilotprojekterne har dog klart vist, at der er behov for mindre komplekse installations- og konfigurationsprocedurer, idet mange privatbrugere, organisationer og virksomheder ikke kan forventes at have den nødvendige kompetence til at foretage ikke-trivielle installationer.

Pilotprojekterne har endvidere vist, at løsningerne er sårbare over for installation af kortlæsere. De enkelte brugeres PC'er er konfigureret og udstyret forskelligt, og det kan ikke forudsættes, at kortlæsere m.m. uden videre kan tilsluttes serielle porte eller lignende. Endvidere har det vist sig, at software installeret på brugernes PC'er kan konflikte med systemdrivere til kortlæserne. Der er således behov for mere fleksible løsninger.

Efterhånden som understøttelse af digital signatur, certifikater og smart cards bliver standard i software og hardware, mindskes betydningen af disse problemstillinger.

Behov for yderligere standarder

Nogle af pilotprojekterne, der henvender sig til erhvervs-kunder, har identificeret behovet for flere CVR-numre på samme certifikat. Behovet opstår, hvis samme medarbejder underskriver "på vegne" af flere virksomheder.

Problemstillingen er analog med begrænsning af de rettigheder, der følger med et medarbejdercertifikat. For eksempel kan man forestille sig, at en medarbejder på virksomhedens vegne ikke kan underskrive visse transaktioner af stor betydning. Der eksisterer ingen standardiseret metode til at angive sådanne forhold på et medarbejdercertifikat.

I den papirbaserede verden angives sådanne forhold ofte ved organisations- og stillingsbeskrivelse, som kan rekvireres af interesserede. I den elektroniske verden kan sådanne oplysninger publiceres via en hjemmeside, men denne fremgangsmåde forudsætter kontrol af underskriverens rettigheder. For at muliggøre elektronisk kontrol af en underskrivers rettigheder er der behov for en ensartet kodning af autorisationer og rettigheder, eksempelvis i XML-format.

Finansiering af løsninger med digital signatur

Omkostningerne til etablering af en løsning med digital signatur omfatter mere end blot udgifter til certifikater og (eventuelt) kortlæsere. Nogle væsentlige omkostninger er:

- Drift af løsning hos brugere (for eksempel support).
- Betaling for ydelser leveret af tredjepart (for eksempel nøglecenter).

Pilotprojekterne har erfaret, at nødvendig IT-kompetence til løsning af tekniske problemer ofte ikke er tilstede hos private borgere og mindre virksomheder. Samtidig betyder produkternes korte levetid, at

installations- og konfigurationsprocedurer ofte ikke tager højde for alle forhold og situationer. Ud over tekniske problemstillinger kan brugere også have behov for at få belyst juridiske og andre ikke-tekniske forhold omkring brugen af digital signatur.

Det må endvidere forventes, at de involverede nøglecentre ønsker at få dækket deres omkostninger ved at udstede og validere certifikater. Nøglecentrene kan vælge forskellige betalingsmodeller, for eksempel en engangsafgift eller en transaktionsafgift. En transaktionsafgift kan endvidere deles mellem brugeren og den offentlige myndighed, eller afholdes af den ene part alene.

I forbindelse med implementering af løsninger med digital signatur må den offentlige myndighed overveje, om og i givet fald hvor meget brugeren er villig til at betale for at anvende løsningen. Pilotprojekterne har vist, at virksomheder ofte er indstillet på at afholde alle direkte omkostninger til udstyr (for eksempel til kortlæser og certifikat), hvis blot udbyttet ved at anvende løsningen vurderes til at være tilstrækkeligt højt. Private borgere er derimod mere tilbageholdne med at købe udstyr, da antallet af serviceydelser – og derved anvendelsesmuligheder – er lille.

På grund af finansieringsomkostninger har pilotprojektet i Næstved Kommune valgt en software-baseret løsning. Omvendt har pilotprojektet i Århus Amt vist, at målgruppen gerne vil betale for udstyr, idet besparelsen ved løsningen hurtigt overstiger investeringen.

For myndighedernes vedkommende kan en eventuel rationaliseringsgevinst anvendes til at finansiere en del af udgiften til etableringen af løsningen.

Flere ydelser med digital signatur

Flere pilotprojekter påpeger, at et kritisk antal elektroniske serviceydelser er nødvendigt, for at borgere tager løsningerne i brug og i særdeleshed hvis borgerne selv skal finansiere nødvendigt udstyr.

Mange offentlige myndigheder, eksempelvis kommuner, har dog det problem, at borgere ikke anvender kommunen særlig ofte. Kun et lille segment af borgere, typisk socialt dårligt stillede, har et højt engagement med kommunen, men dette segment er samtidigt mindst motiveret for at investere i udstyr til elektronisk selvbetjening for egen regning.

Det kan derfor være fordelagtigt for offentlige myndigheder at "gå sammen". Eksempelvis kan biblioteker være med til at drive antallet af transaktioner op på en kommunal hjemmeside.

En nødvendig forudsætning for dette er dog, at de offentlige løsninger er kompatible, således at den enkelte borger ikke skal have forskelligt udstyr og certifikater for at anvende de forskellige løsninger.

For at skabe kritisk volumen kan offentlige myndigheder fokusere på erhverv, der ofte har et større antal transaktioner med offentlige myndigheder, end borgere.

Problemstilling ved mistet privat nøgle til kryptering

En tekst krypteret med en offentlig nøgle kan kun dekrypteres med den tilhørende private nøgle. Hvis en offentlig myndighed "mister" sin private nøgle, kan dokumenter gemt i krypteret form ikke længere læses.

Mange nøglecentre tilbyder "key recovery". Det vil sige, at den offentlige myndighed kan få en "erstatningsnøgle", i tilfælde den private nøgle mistes.

Da en offentlig myndighed gemmer følsomme oplysninger, eksempelvis patientjournaler, kan dette skabe utryghed ved løsningernes sikkerhed. Endvidere må den offentlige myndighed tage stilling til, hvorvidt man ønsker at basere en "sikkerhedsmekanisme" på en ekstern organisation.

Denne problemstilling er behandlet af IT-Sikkerhedsrådet i "Praktisk brug af kryptering og digital signatur", side 32.

5. Digital signatur i fremtiden

I dette kapitel gives nogle vurderinger af anvendelsen af digital signatur i fremtiden. Endvidere diskuteres et antal indsatsområder, som vil kunne stimulere den fortsatte brug og udbredelse af digital signatur hos offentlige myndigheder i Danmark.

Tendenser og udvikling for digital signatur

Udbredelse og anvendelse af kryptering, PKI og digital signatur er kraftigt stigende, og en væsentlig vækstfaktor er elektronisk handel. Elektronisk handel stiller krav til beskyttelse af kundedata, eksempelvis kreditkortnumre og metoder til at forhindre bedrageri mod den forretningsdrivende. Den stadigt voksende elektroniske borgerservice stiller krav til uafviselighed og beskyttelse af følsomme persondata.

Analyser og forudsigelser

International Data Corporation (IDC) mener, at salg af krypteringssoftware vil blive betydelig i 2001. Krypteringssoftware vil være indbygget i applikationer og systemsoftware og transparent for brugeren. Kryptering vil være teknologien, der muliggør en lang række applikationer, som ikke er muligt med det nuværende sikkerhedsniveau (*"Encryption software: marked and trends"*, IDC, Dec 98, Doc #17701, p 1-40.)

META Group mener, at man bør vente med at implementere omfangsrige og kritiske løsninger baseret på PKI, indtil teknologien modner. Kryptering i kritiske løsninger bør implementeres ved hjælp af dedikeret krypteringshardware. I 2002 vil netværkssikkerhed blive implementeret via PKI-teknologi. (*"Security authentication technologies"*, META Group, Nov 98, File 740, p 1-2.)

Gartner Group forudsiger, at i 2001 vil 40% af alle forretningskorrespondancer blive sendt elektronisk. Omkring 80% af alle store virksomheder vil gennemføre pilotprojekter med digitale certifikater mellem 1999 og 2003. Konkurrencen mellem PKI-produkter vil stige mellem 1999 og 2001 med prisreduktion til følge. (*"PKI trends: 1999 and beyond"*, V. Wheatman, Gartner Group, Jan 99, Doc #ISS: SPA-06-9580.)

Anvendelse af digital signatur i andre sektorer

Kryptering og digital signatur har i flere år været anvendt i andre sektorer og brancher.

I takt med at flere økonomisk og retslig bindende transaktioner gøres tilgængelige via Internettet, har bankerne identificeret et stort behov for kryptering og digital signatur. De nuværende Internet Banking-løsninger er typisk baseret på (svag) SSL-kryptering, men Home Banking-løsninger implementerer software-baserede digital signatur med proprietær

software.

Flere banker og finansielle sammenslutninger er nu begyndt at undersøge muligheden for at anvende smart cards, der kan bruges både som bankkort (hævekort) og til lagring af digital signatur. PBS har ligeledes overvejelser omkring et nyt Dankort baseret på smart cards.

Andre lande

Andre lande i Skandinavien og Europa har ligesom Danmark vedtaget love omkring brugen af elektronisk signatur. Finland har besluttet at oprette et nationalt nøglecenter og at udstede kombinerede pas- og identitetskort med digitale certifikater. Sverige har derimod, ligesom Danmark, valgt at overlade markedet omkring digital signatur til fri konkurrence. Repræsentanternes Hus i USA har netop vedtaget E-SIGN, der juridisk ligestiller digital signatur med underskrifter.

Det må forventes, at den stigende globale anvendelse af software og hardware til digital signatur også vil skabe gunstige prisstrukturer i Danmark.

Standardiseringsarbejde

På trods af PKI-teknologiens beskedne alder eksisterer der allerede et stort antal standarder og protokoller vedrørende kryptering, digitale certifikater og digital signatur. Parallelt med udviklingen og fastlæggelsen af disse generelle specifikationer foregår der tillige en række branche-specifikke standardiseringsarbejder, herunder vedrørende brug af certifikater i offentlige forvaltninger.

The Internet engineering Task Force (IETF) er hovedansvarlig for udviklingen af standarder og protokoller, som gør Internettet brugbart og interessant. En af arbejdsgrupperne under IETF er Public-Key Infrastructure, X.509 (PKIX), som blev dannet i 1995 med det formål at målrette standarder for certifikater og CRL til Internettet.

Resultatet af arbejdet var fire standarder. PKIX#1 beskriver syntax af X.509 certifikater. PKIX#2 specificerer driftsrutiner, der er nødvendige i et PKI-miljø, herunder initiering af certifikater og nøglepar. PKIX#3 indeholder protokoller til dag-til-dag rutiner i et PKI-miljø, herunder tilbagetrækning af certifikater og online check af status på certifikater. PKIX#4 indeholder retningslinier til CPS-dokumenter. Disse fire standarder blev afsluttet i 1999.

PKIX-gruppen har fortsat sit arbejde og arbejder på et antal nye specifikationer. I pilotprojekterne er PKIX standarderne bl.a. anvendt i forbindelse med kommunikation med CA-server og smart cards.

Secure MIME (S/MIME) blev udviklet af en samling af virksomheder, der tilføjede kryptering og digital signatur til MIME-protokollen.

Specifikationen blev overgivet til IETF i 1995. Protokollen er senere blevet opdateret og eksisterer nu i version 3 (RFC 2630-RFC2634). S/MIME-protokollen er anvendt i pilotprojekterne i forbindelse med signeret elektronisk post.

United States Federal Public-Key Infrastructure (U.S.FPKI) er dannet af den amerikanske regering med henblik på at definere et PKI til eget brug. Et af gruppens fokusområder er specifikation af en profil på X.509v3 certifikater specielt egnet til offentlige myndigheder. På sigt vil U.S.FPKI angive standarder for et komplet offentligt PKI, og disse standarder vil danne grundlag for krav om kompatibilitet ved indkøb af PKI-produkter til offentlige systemer. En af U.S.FPKI's målsætninger er dog, at den "offentlige PKI-standard" kommer til at ligge så tæt på specifikationer for andre brancher, at forhandlere af offentlige PKI-produkter ikke forhindres i at sælge deres løsninger til andre brancher. (<http://csrc.nist.gov/pki>.)

Minimum Interoperability Specification for PKI Components (MISPC) er en del af U.S.FPKI men udvikles dog separat. Formålet med MISPC er at danne grundlag for interoperabilitet mellem PKI-komponenter fra forskellige leverandører. Eksempelvis identificerer MISPC, hvilke af de mange valgfrie felter i et X.509-certifikat som virkelig skal implementeres, for at certifikatet kan processeres af andre enheder i et PKI. MISPC er ikke blot en specifikation; den indeholder også en reference-implementering, som leverandører kan anvende for at dokumentere deres produkters opfyldelse af MISPC-specifikationen. (<http://csrc.nist.gov/pki/mispc/welcome.html>.)

The Government of Canada Public-Key Infrastructure (GOCPKI) definerer et PKI, tilpasset den canadiske statslige forvaltning men med hensyn til senere national brug. GOCPKI er en fuld PKI-specifikation, inklusive standarder for certifikater, CRL, kommunikationsprotokoller og driftsrutiner. Specifikationen stiller nødvendige krav til PKI-leverandører, men GOCPKI har som målsætning, at produkter udviklet med henblik på opfyldelse af GOCPKIs-specifikationen også kan anvendes i andre sammenhænge. (<http://www.cse-cst.gc.ca>.)

Det amerikanske institut for standarder og teknologi (NIST) er i gang med at udvælge en symmetrisk krypteringsalgoritme (det vil sige en algoritme baseret på en fælles hemmelig nøgle) til erstatning for den nu de-facto standard algoritme DES. *Advanced Encryption Standard* (AES) forventes at blive fastlagt i løbet af sommeren 2000, og vil blive anvendt af USA's offentlige forvaltninger. Da AES forventes at blive anvendt i de næste 20-30 år, er et af kravene til algoritmen, at nøglelængden er variabel og op til 256bit. Det må forventes, at ledende softwareleverandører vil indbygge en understøttelse af AES i deres produkter, så snart den nye standard er fastlagt.

En undergruppe under W3C arbejder med inkorporering af digital signatur i XML. Gruppens arbejde, XML-Sign, forventes at blive

anbefalet som "draft proposal" i år 2000. Mange leverandører betragter "draft proposals" som værende så stabile, at de implementerer standarderne i deres produkter. Dette betyder, at digital signatur kan være en standard funktionalitet i næste version web-browsere, ligesom digital signatur er implementeret i de fleste post-klienter i dag.

Indsatsområder

Med pilotprojekterne om digital signatur har Forskningsministeriet igangsat brugen af digital signatur i offentlige forvaltninger og fremmet udviklingen af produkter og tjenester. Det er nu op til markedet selv at videreudvikle produkter og tjenester i henhold til behov og efterspørgsel. Forskningsministeriet har således meldt ud, at det ikke har planer om etablering af offentlige nøglecentre, og at det offentlige ikke økonomisk vil støtte udbredelsen af udstyr til befolkningen i almindelighed.

Forskningsministeriet har dog afsat betydelige midler til at stimulere og udbrede brugen af digital signatur hos offentlige myndigheder. Midlerne er i udgangspunktet ikke beregnet til finansiering af slutudstyr til borgere og virksomheder, men til at øge antallet af ydelser og services, hvori digital signatur indgår.

Sikker datakommunikation mellem offentlige myndigheder

Kommunernes Landsforening, Amsrådsforeningen og Forskningsministeriet har indgået en aftale om sikker datakommunikation mellem offentlige myndigheder. Aftalen har fire hovedelementer:

- Fremtidige offentlige systemer udvikles med web-baserede brugergrænseflader
- Kommunikation mellem offentlige IT-systemer, og mellem det offentlige og borgere/virksomheder baseres på standard Internet-protokoller
- Al tele- og datakommunikation omlægges til Internet-baserede protokoller, herunder IP-protokollen.
- Intern og ekstern sikkerhed i offentlige IT-systemer bliver baseret på public-key kryptering og digital signatur.

Til sikring af aftalens gennemførelse er der nedsat et koordinationsudvalg med tre primære arbejdsopgaver:

- Udarbejdelse af retningslinier for web-baserede brugergrænseflader.
- Klassifikation af sikkerhedsniveauer og databeskyttelse, og retningslinier for brug af kryptering og digital signatur.
- Gennemførelse af offentligt udbud vedrørende produkter og tjenester til den fremtidige offentlige datakommunikation.

De to første delopgaver er gennemført. Endvidere er der indgået en rammeaftale om Internet-opkobling af offentlige forvaltninger. Udbuddet

om digital signatur vil vedrøre produkter og tjenester til etablering af Public-Key Infrastructure.

I forbindelse med gennemførelsen af udbuddet er det vigtigt, at der udarbejdes åbne standarder og specifikationer, således at een offentlig myndighed ikke behøver to ikke-kompatible systemer til kommunikation med to andre offentlige myndigheder. Endvidere bør det tilsigtes, at alle offentlige IT-systemer, som har eller kan forventes at få borger- eller virksomhedsadgang, har samme tekniske grænseflade.

Et sådant udbud vil naturligvis virke voldsomt stimulerende på markedet, idet både antallet af brugere og mængden af transaktioner er stor. Udbuddet kan også ventes at have en effekt på den ikke-offentlige anvendelse af PKI-produkter og -tjenester, idet udbuddet formentlig vil yderligere modne produkter og ydelser samt sikre priskonkurrence. Rameaftalens udbud ventes gennemført i foråret 2001.

Offentlige initiativer

I redegørelserne "*Det Digital Danmark*" og "*Omstilling til Netværkssamfundet*" er der fremhævet en række initiativer, som det offentlige vil gennemføre. Flere af disse enten forudsætter eller vil have gavn af digital signatur. Der er reserveret betydelige økonomiske midler til gennemførelsen af flere af disse projekter.

Nogle væsentlige initiativer er:

- Hjemmeside til alle studerende
- En offentlig auktionshal på Internettet
- Personlig adgang til det offentliges data via Internettet
- Offentlig informationsserver
- Elektroniske blanketter i det offentlige.

Flere af disse projekter indeholder elementer af indberetning af retslig bindende oplysninger (eksempelvis SU-ansøgning via hjemmeside for studerende) og adgangskontrol til personfølsomme oplysninger (eksempelvis informationer tilgængelige via personlig internetadgang).

En væsentlig målsætning ved udvikling af et eller flere af disse projekter bør være, at grænsefladen mellem brugeren og det offentlige system er standardiseret og offentligt tilgængelig. Herved sikres, at forskellige leverandører kan udvikle slutprodukter, som brugeren frit kan vælge imellem.

Fortsættelse af pilotprojekter

Flere af de gennemførte pilotprojekter er gjort permanente efter pilotperiodens udløb. Dette gælder eksempelvis løsningerne i Næstved og Vordingborg Kommune, Århus Amt, og til dels Ringsted Kommune. Andre projekter er parate til udbredelse til hele målgruppen, men er

begrænset af brugernes villighed til at investere i nødvendigt udstyr. Dette gælder eksempelvis for løsninger hos SU-styrelsen og EU-direktoratet.

I forbindelse med gennemførelse af ovennævnte offentlige initiativer er det muligt at tage udgangspunkt i et eller flere pilotprojekter. Eksempelvis er SU-selvbetjening en naturlig del af en hjemmeside for studerende. Tilsvarende kan løsningen udviklet af Handelshøjskolen i København tænkes anvendt af andre uddannelsesinstitutioner.

Informationskampagne

Kryptering og digital signatur er nye teknologier, der endnu ikke er bredt kendt i befolkningen. Manglende forståelse for teknologien kan både skabe utryghed omkring løsningernes sikkerhed, men også stille tvivl om behovet for kryptering og digital signatur. Eksempelvis har Told•Skat i flere år givet befolkningen mulighed for ændringer i selvangivelsen via Internettet – en løsning der ikke er beskyttet af personlige certifikater og digital signatur. Hvorfor er det så nødvendigt at anvende digital signatur i andre sammenhænge?

Der er behov for en informationskampagne, der eksempelvis kan belyse:

- Retsvirkning ved brug af digital signatur på dokumenter
- Kryptering og sikkerhedsniveauer
- Anvendelse af digital signatur i praksis
- Konsekvenser ved indførelse af smart cards – hvilke oplysninger lagres eksempelvis på smart card? Og hvilke oplysninger kan udledes af et personligt certifikat?

Det må tilstræbes, at befolkningen i et netværkssamfund har samme almindelige forståelse for kryptering og digital signatur som for infrastruktur til betalinger og Dankortet.

Finansiering af løsninger til offentlige myndigheder

Pilotprojekterne fokuserede i lige så høj grad på teknologiens anvendelighed som på opnåelse af serviceforbedringer og rationaliseringsgevinster. Ved udvikling og implementering af nye IT-løsninger bør der dog i stadig stigende grad fokuseres på serviceforbedringer og rationaliseringsgevinster.

Finansieringen af slutudstyr kan ske på flere måder. Det er tænkeligt, at når blot antallet af anvendelsesmuligheder er tilstrækkelig stor, vil brugerne gerne selv afholde de nødvendige omkostninger. En interessant parallel kan drages til Internet-opkoblinger (PC, modem, telefonforbindelse) for borgere, som heller ikke betales af det offentlige, og som er langt dyrere. Tilsvarende er erhvervsvirksomheder også "vant" til at betale omkostningerne for eksterne serviceydelser. Eksempelvis online clearing af betalingskort og data fra offentlige

myndigheder.

Brugen af billig Internet-datakommunikation, muligheden for selvbetjening, automatisk datafangst og digital sagsbehandling kan give betragtelige rationaliseringsgevinster, der potentielt kan selv-finansiere IT-løsningerne. I nogle tilfælde kan det endog tænkes, at rationaliseringsgevinsten er så stor, at en del af denne kan anvendes til at yde tilskud til brugernes udgifter til at tage løsningen i brug.

Der er således behov for cost-benefit analyser og forretningsmodeller for brugen af digital signatur i forskellige offentlige myndigheder.

Fortsættelse af standardiseringsarbejde

Der er fortsat behov for standardiseringsarbejde og udvikling af protokoller og grænsesnit. Selv om udviklingen af standarder og protokoller drives af markedet, kan det være hensigtsmæssigt, at arbejdet koordineres i et fælles udvalg. Udvalget kan blandt andet sikre, at forskellige sektorer tilpasser sig hinanden til gavn for både brugerne og udbyderne af løsninger. Eksempelvis kan man tænke sig, at betalingskort udstedt af bankerne kan anvendes til digital signatur på en ordre i forbindelse med handel på Internettet. Tilsvarende kan en offentlig myndighed, eksempelvis Told•Skat, der kommunikerer elektronisk med virksomhederne, have gavn af at koordinere og standardisere med private organisationer, som kommunikerer med de samme virksomheder, eksempelvis revisionsfirmaer.

Et standardiseringsudvalg behøver ikke nødvendigvis at være under offentligt regi eller ledelse, men de offentlige myndigheder bør deltage aktivt i arbejdet set i lyset af deres størrelse og betydning.

Erfaringerne fra andre lande, herunder USA og Canada, viser dog, at offentlige myndigheders krav til PKI kan være specielle i forhold til andre brancher og sektorer. Der er derfor behov for, at offentlige myndigheder hurtigt udvikler udkast til standarder, der forventes at være bredt anvendelige i hele den offentlige sektor. Udgangspunktet for disse er naturligt de standarder og protokoller, som er udarbejdet i forbindelse med pilotprojekterne. Forum for Digital Signatur, som blev oprettet som en del af pilotprojekterne, kan fortsætte arbejdet i nye rammer og være koordinator for det videre arbejde.

I forbindelse med udarbejdelse af standarder kan der udvikles en referenceplatform, som uafhængige leverandører og serviceydere kan anvende med henblik på certificering af produkter og tjenester. Lignende initiativer kendes eksempelvis fra finansverdenen, hvor leverandører kan afprøve deres produkter mod SET-specifikationen. Et tilsvarende initiativ er taget af regeringen i Canada i forbindelse med GOCPKI-specifikationen.

Bilag 1: Indkaldelse af forslag til projekter

I dette bilag er den oprindelige indkaldelse af forslag til pilotprojekter om digital signatur gengivet.

Udkast til indkaldelse af pilotprojekter

6. maj 1998

1. Indgivelse af forslag

Forslag til pilotprojekter med digital signatur kan indgives af offentlige myndigheder (stat, amt eller kommune). Forslag indgives skriftligt senest **mandag den 8. juni 1998, kl. 12.00 til** : Forskningsministeriet Bredgade 43, 1260 København K, Att: Per Helge Sørensen. Forslag mærkes: "Pilotprojekter for digital signatur".

Forslag kan indgives elektronisk via Internet til: fsk@fsk.dk

2. Form

Forslag til pilotprojekter skal indeholde:

Teknisk beskrivelse:

- Beskrivelse af projektets mål
- Overordnet beskrivelse af projektet - I hvilken anvendelse skal den digitale signatur indgå - Hvilke offentlige myndigheder vil indgå i projektet - Mod hvilke brugere retter projektet sig - Hvor mange brugere vil indgå
- Overordnet beskrivelse af den forventede tekniske løsning - software/hardware/chipkort - certifikater - anskaffelse af CA-tjenester
- Tidsplan

Økonomi:

- Budget
- Ansøgt støttebeløb

Projektstyring:

- Ansvarlig offentlig myndighed
- Nøglepersoner

3. Generelle krav

Forskningsministeriet stiller følgende generelle krav til projekterne: Pilotprojektet skal sigte mod at sikre kommunikation mellem det offentlige og borgerne eller virksomhederne i forbindelse med en konkret anvendelse, f.eks. et elektronisk selvbetjeningsystem, et system til elektroniske indberetninger, elektroniske blanketter el. lign.

Pilotprojektet kan alternativt sigte mod at sikre kommunikation mellem

offentlige institutioner i forbindelse med en konkret anvendelse - f.eks. sikker adgang til en offentlig database, sikker udveksling og behandling/registrering af dokumenter mellem offentlige myndigheder el. lign.

Pilotprojektet skal sættes i drift senest primo 1999.

Den maksimale projektperiode er 12 måneder. Pilotprojektet skal være udformet således at systemet kan overgå til egentlig drift ved udløbet af projektperioden.

Pilotprojektet skal overholde markedsledende standarder for digital signatur, således at det kan danne basis for etablering af en universel sikker infrastruktur i Danmark (krav til standarder er nærmere beskrevet i vedlagte dokument: "Krav om standarder").

4. Vurdering

Forslagene vurderes af Forskningsministeriet, som blandt forslagene udvælger, hvilke projekter der tildeles tilskud.

Beslutning om valg af pilotprojekter vil blive offentliggjort. Der vil i den forbindelse blive offentliggjort en overordnet beskrivelse af de udvalgte projekter. Hvis særlige forhold (f.eks. af hensyn til senere udbud) ønskes holdt fortroligt, bedes dette angivet eksplicit i forslaget.

Valg af pilotprojekter forventes offentliggjort senest: fredag den 26. juni 1998.

5. Kriterier for valg af projekter

Forskningsministeriet har afsat i alt ca. 10 mio. kr. i tilskud til pilotprojekterne. Forskningsministeriet forventer at yde tilskud til 3-5 projekter.

Det vil blive tilstræbt, at de støttede projekter repræsenterer et bredt udsnit af offentlige institutioner og serviceydelser.

Følgende faktorer vil blive tillagt betydning i vurderingen af pilotprojekterne:

- Den serviceforbedring som opnås for borgerne/virksomhederne i forbindelse med projektet
- Rationaliseringsgevinster i det offentlige
- Pilotprojekterne er robuste over for den teknologiske udvikling.

6. Hjemmeside

Der er på Forskningsministeriets hjemmeside <http://www.fsk.dk> oprettet en særlig hjemmeside i forbindelse med indkaldelse af forslag til pilotprojekter.

I perioden frem til fristen for indgivelse af forslag vil evt. ny information om forslag til pilotprojekter blive lagt på denne side. Herunder vil svar på spørgsmål, som skønnes at være af generel interesse, blive tilgængelige på siden.

7. Spørgsmål

Spørgsmål kan rettes til Per Helge Sørensen på Internet: phs@fsk.dk.
Telefon: 3392 9911 Fax: 3393 8012.

Som nævnt ovenfor vil svar på spørgsmål som skønnes at være af generel interesse, blive offentliggjort på Forskningsministeriets hjemmeside.

8. Opfølgning

For at sikre koordination mellem pilotprojekterne vil Forskningsministeriet afholde opfølgningsmøder med de udvalgte pilotprojekter.

Opfølgningsmøderne skal bl.a. sikre, at kravene om fælles standarder i pilotprojekterne løbende tilpasses markedsudviklingen. Opfølgningsmøderne skal samtidig tjene til at sikre erfaringsopsamling fra pilotprojekterne.

Krav om standarder

26. november 1998

1. Baggrund

Nedenfor følger de reviderede krav til fælles standarder i pilotprojekterne med digital signatur. Kravene er tilrettet efter kommentarer fra de enkelte projekter samt efter diskussion i Forum for Digital Signatur under Dansk Standard.

2. Sikkerhedsniveau

Idet der er tale om pilotprojekter for digital signatur, sigtes der i nedenstående krav mod et middelhøjt sikkerhedsniveau. Der åbnes f.eks. mulighed for anvendelse af rene softwareløsninger, kravene til identifikation i forbindelse med udstedelse af certifikater er fleksible, og der opstilles ikke meget specifikke krav til CA'ers fysiske og logiske sikkerhed.

De stillede krav omkring nøglelængder er dog på et sikkerhedsniveau, som vil betyde, at en række af de kommercielle browsere og e-post klienter ikke direkte vil kunne anvendes (på grund af amerikanske eksportregler).

Det kan således være nødvendigt i pilotprojekterne at stille soft- eller hardware til rådighed for brugerne, som muliggør dette højere sikkerhedsniveau. Dette kan f.eks. ske ved, at brugerne anskaffer produkter fra alternative leverandører, at den offentlige myndighed stiller

særligt udviklet (eller tilpasset) software til rådighed for brugerne el. lign.

Dette forhold vil naturligvis være en komplikation i det enkelte pilotprojekt. Kravet stilles dog helt bevidst, idet målet med at give tilskud til pilotprojekter med digital signatur netop er at fremme udviklingen af sikre produkter til det danske marked.

3. Digital signatur og kryptering

Anvendte digitale signaturer skal være baseret på public key krypteringsteknikker.

Der skal anvendes åbne og (de facto) standardiserede algoritmer, f.eks.:

- For digital signatur: RSA, DSA Diffie-Hellman
- For envejs hash funktioner: SHA-1

Anvendte algoritmer og nøglelængder skal være af en sikkerhed mindst svarende til RSA med nøglelængde 1024 bit.

Såfremt der anvendes kryptering med henblik på fortrolighed, skal dette ske ved åbne standardiserede algoritmer, f.eks: TripleDes, Idea, Blowfish, RC4 . Algoritmer og nøglelængde til kryptering skal være af en sikkerhed mindst svarende til 2 nøgle TripleDes (128 bit).

4. Certifikater

Digitale signaturer skal være baseret på udstedelse af certifikater til den enkelte bruger.

Certifikater skal følge X.509 version 3 standarden.

Indholdet i certifikater skal muliggøre, at den digitale signatur kan anvendes i forbindelse med sikker kommunikation med offentlige myndigheder.

Personcertifikater, som udstedes til fysiske personer i deres egenskab af at være borgere i samfundet (til kommunikation med det offentlige m.v.), skal som minimum indeholde følgende oplysninger:

- Fulde navn
- Plads til et evt. senere unikt identifikationsnummer

Medarbejdercertifikater, som udstedes til fysiske personer i deres egenskab af at være medarbejdere i en virksomhed eller en offentlige myndighed, skal indeholde følgende minimumsoplysninger:

FDS anbefaler, at medarbejdercertifikater som minimum indeholder følgende oplysninger:

- Virksomhedens fulde navn (inkl. A/S betegnelse m.v.)
- Virksomhedens SE-nummer (afløses af CVR-nummer når dette

etableres)

- Medarbejderens fulde navn

Det anbefales endvidere, at medarbejdercertifikater indeholder medarbejderens stillingsbetegnelse samt organisatoriske tilhørsforhold (afdeling el. lign), idet inkludering af disse oplysninger dog er optionel.

Virksomhedscertifikater, som udstedes til juridiske personer (virksomheder og offentlige myndigheder) til anvendelse i sammenhænge, hvor der ikke er behov for at der står en fysisk person bag meddelelsen (server certifikater, EDI certifikater, m.v.) skal som minimum indeholde følgende oplysninger:

- Virksomhedens fulde navn
- Virksomhedens SE-nummer

Certifikaterne kan derudover indeholde applikationsspecifikke oplysninger. Det noteres dog, at applikationer, som er baseret på applikationsspecifikke oplysninger i certifikatet, ikke vil kunne anvende certifikater fra andre certifikatudstedere. Applikationer bør derfor kun være baseret på applikationsspecifikke oplysninger, hvis det ikke forventes, at der kan være behov for at acceptere andre udbydernes certifikater.

Der er under Forum for Digital Signatur (FDS) nedsat en særlig arbejdsgruppe med henblik på at koordinere implementering af certifikater. Pilotprojekterne bedes anmode deres leverandører (eller den relevante underleverandør) om at deltage i denne.

5. Identifikation ved udstedelse af certifikater

Ved udstedelse af certifikater skal der ske en sikker identifikation af brugerne. Identifikationen skal være baseret på personligt fremmøde med fremvisning af billedlegitimation.

Der kan i pilotprojekterne indgås aftale om at basere identifikationen af brugerne på identifikation, der er foretaget af andre myndigheder eller virksomheder, hvis denne identifikation opfylder ovennævnte sikkerhedskrav. F.eks. identifikation ved personligt fremmøde ved oprettelse af en konto i en bank, ved indskrivning på en uddannelsesinstitution el. lign.

6. Adgang til certifikater

Den enkelte brugers digitale signatur skal kunne anvendes i andre systemer, som kan være baseret på et andet CA. Brugernes certifikater bør derfor være offentligt tilgængelige.

Certifikater bør gøres tilgængelige på Internet via LDAPv2 directory protokollen. Alternativt kan anvendes X.500 directory, som gøres tilgængelig via DAP.

Forespørgsel på certifikater bør desuden kunne ske via HTTP til en Web-server, der efterfølgende omsætter forespørgslen til LDAP.

7. Spærring af certifikater

Den enkelte brugers digitale signatur skal kunne anvendes i andre systemer, som kan være baseret på et andet CA. Information om spærring af certifikater skal derfor være offentligt tilgængelig.

Information om spærring af certifikater skal gøres tilgængelig via en af følgende standarder:

- En tilbagetrækningsliste i henhold til X.509 version 2 certificate revocation list (CRL) standarden, som gøres tilgængelig via LDAPv2 directory protokollen.
- Forespørgsel via OCSP protokollen (PKIX arbejdsgruppen)

8. Certifikathåndtering

Certifikathåndtering betegner de aktiviteter, som er nødvendige i forbindelse med at udstede og vedligeholde brugernes certifikater, f.eks. ansøgning om certifikater, overdragelse af certifikater m.v.

Certifikathåndtering kan ske både on-line (via Internet) og off-line, f.eks. ved personlig overdragelse (af chipkort, diskette eller lign), fremsendelse med posten m.v.

Sker certifikat anmodningen online skal standarden for certification requests, PKCS#10 følges.

9. Applikationer

Pilotprojekterne ønskes så vidt muligt baseret på standard Internet applikationer, som er bredt tilgængelige på markedet, f.eks.:

- Browsers
- E-post klienter
- EDI moduler

Mængden af specialudviklet soft - eller hardware, som brugerne skal anskaffe ud over disse produkter ønskes således holdt på et minimum. Der kan dog inden for hvert enkelt projekt være behov for selv at udvikle (eller indkøbe og stille til rådighed) særlig soft- eller hardware, f.eks. med henblik på:

- At opnå en særlig funktionalitet, som er nødvendig for projektet
- At kompensere for manglende eller svage krypteringsfunktioner i kommercielle produkter, som skyldes amerikansk eksportkontrol med kryptering.

Såfremt særlig software eller hardware indeholdende krypterings-

funktioner udvikles eller stilles til rådighed i pilotprojektet, bør disse såvidt muligt overholde standardiserede grænseflader (API'er), således at andre applikationer kan udnytte disse krypteringsfunktioner. Der ser endnu ikke ud til at være enighed om krypto API på markedet, og der stilles derfor ikke krav om overholdelse af en bestemt API. Følgende er eksempler på relevante API'er:

- Generic Cryptographic Services – GCS-API
- Microsoft CryptoAPI 2.0 og Microsoft CryptoAPI 1.0
- Common Data Security Architecture – CDSA 1.2

10. Chipkort

Anvendelse af chipkort med henblik på at opnå mobilitet og større sikkerhed vil formodentlig være naturligt i en række pilotprojekter.

Pilotprojekterne opfordres til at understøtte følgende standarder:

- at PC/SC standarden anvendes til alle applikationer som er Windows baserede
- at PKCS#11 standarden for grænsefladen mellem applikation og chipkort understøttes
- at Open Card Framework arkitekturen anvendes til Java baserede løsninger.

11. Beskyttelse af den private nøgle

Benyttede systemer (software, hardware, chipkort) skal sikre en god beskyttelse af den private nøgle. Der kan bl.a. peges på følgende forhold:

- at private nøgler ikke forekommer i klar tekst under lagring, f.eks. ved at nøgler krypteres med et brugervalgt kodeord
- at private nøgler er beskyttet under eksekvering f.eks. ved at nøgler er fragmenterede og overskrives, dersom de ikke har været anvendt i en periode
- at private nøgler gemmes i hardware eller hardware tokens (chipkort m.v.)

12. Meddelelsesformater

For at sikre at soft- og hardware udviklet eller stillet til rådighed under projektet kan anvendes ved kommunikation med andre offentlige myndigheder, anvendes standardiserede meddelelsesformater og protokoller.

For sikker e-post anvendes S/MIME v3.

For EDI anvendes enten

- EDIINT eller
- EDIFACT version 4

EDIINT standarden åbner mulighed for at anvende enten S/MIME eller PGP. Idet anvendelse af PGP i EDIINT ikke synes at vinde udbredelse på markedet, kræves det i pilotprojekterne, at EDIINT bliver baseret på S/MIME.

Digital signatur på HTML blanketter (form sign) kan opnås ved, at data fremsendes som en POST meddelelse underskrevet digitalt efter PKCS#7 standarden (implementeret i version 4.03 af Netscape Communicator).

Indtil andre standarder for dette fremkommer på markedet, anbefales denne fremgangsmåde fulgt i pilotprojekterne.

13. Sikkerhed i CA'er (nøglecentre)

Der bør i CA'er etableres en høj grad af sikkerhed omkring:

- Fysisk adgangskontrol
- Uddannelse af personale
- Adskillelse af funktioner
- Logning og backup
- Logisk adgangskontrol
- M.v.

Idet der kun er tale om pilotprojekter vil Forskningsministeriet ikke stille konkrete krav til sikkerheden af CA'er. Sikkerhedskrav til CA'er vil blive overvejet nærmere i forbindelse med udformning af bekendtgørelser til lovforslaget om digital signatur.

Der bør dog i pilotprojekterne lægges vægt på at vælge modeller til organisering af CA funktionen, som på et senere tidspunkt kan forventes at kunne leve op til de relativt høje sikkerhedskrav, som forudses i lovgivningen om digital signatur.

14. Softwareløsninger

Design:

Software implementeringer af kryptografiske løsninger er særligt følsomme for kompromittering og skal designes på en måde der tilgodeser:

- Sikring af transaktioner med digital signatur bør ske på en måde, der bedst muligt sikrer, at de data, brugeren ønsker at påføre den digitale signatur, også er de data, der faktisk underskrives. (f.eks. ved at brugeren kan overbevise sig om skærbilledets ægthed).
- Bedst mulig beskyttelse af hemmelige nøgler under eksekvering (f.eks. at hemmelige nøgler er fragmenterede og slettes, dersom nøglen ikke har været anvendt i en periode).
- At hemmelige nøgler ikke forekommer i klar tekst under lagring, og at de er bedst muligt beskyttet mod udtømmende søgning (f.eks. ved at nøglen krypteres med et brugervalgt kodeord, og at

korrekt dekryptering af den hemmelige nøgle ikke verificeres lokalt hos brugeren).

- At der er kontrolspor for alle væsentlige hændelser, og at kontrolsporet er bedst muligt beskyttet (f.eks. logning af alle afsendte og modtagne transaktioner med digital signatur, nye versioner af sikkerhedsløsningen).

Distribution:

Modtager af sikkerhedssoftwaren skal være bedst muligt beskyttet mod at anvende falsk software.

Bilag 2: Høring om digital signatur

I forbindelse med den sammenfattende evaluering af Forskningsministeriets pilotprojekter om digital signatur indkaldte Forskningsministeriet til en fælles høring. Høringen havde deltagelse af samtlige pilotprojekter og leverandører og indeholdt en foreløbig sammenfattende status på pilotprojekterne. I forlængelse heraf blev der afholdt en debat blandt deltagerne om en række centrale spørgsmål. Synspunkterne er opsummeret i det efterfølgende.

Sikring af interoperabilitet i løsninger

Pilotprojekterne har ikke demonstreret, at digitale signaturer/certifikater kan anvendes på tværs af offentlige myndigheder.

Hvorledes sikres interoperabilitet i løsningerne? Skal brugerne have flere smart cards, eller skal man tilstræbe at udvikle et fælles smart card?

- I England anvendes forskellige kort til forskellige løsninger.
- Brug af flere kort kræver at brugeren kan huske flere kendeord, hvilket besværliggør brugen af digital signatur.
- Nogle borgere kan være betænkelige ved et fælles kort, idet eksempelvis adgang til private og offentlige data derved blandes sammen.
- Man bør tilstræbe at have eet kort til alle offentlige systemer.
- Nye smart cards med større lagerkapacitet gør det muligt at gemme flere digitale certifikater på samme kort.
- Brug af flere smart cards giver valgmuligheder hos udbyderne af serviceydelser. Flere kort giver for eksempel mulighed for at vælge, i hvilke og hvor mange data der gemmes på certifikatet.

Finansiering af digital signatur

Pilotprojekterne har identificeret, at borgere kun er villige til at betale et vist beløb for den nødvendige hardware og software til digital signatur.

Hvorledes sikres udbredelsen af digital signatur? Hvem skal betale for slutbrugerens udstyr og certifikater?

- Kun software-baserede løsninger kan tilbydes til en så lav pris, at borgerne er villige til at anvende digital signatur.
- Det er vigtigt, at løsningerne dækker hele den offentlige sektor. Borgeren skal ikke investere i to "forskellige" løsninger.
- Rationaliseringsgevinsten ved løsningerne kan anvendes til at dække - helt eller delvist - brugernes omkostninger.
- Offentlige løsninger kan delvis finansieres ved at private virksomheder "køber sig ind" i løsningen, det vil sige, baseret på

samme PKI m.m.

- Nøglecentre kan dække deres udgifter ved transaktionsafgifter. Offentlige myndigheder kan eventuelt opkræve gebyrer i visse tilfælde. En gebyropkrævning kan dog virke hæmmende på løsningens udbredelse, hvis den tilsvarende "papir-baserede" sagsgang ikke er pålagt gebyr.
- Offentlige myndigheder bør i særdeleshed animere virksomheder til at investere i digital signatur for at stimulere markedet.
- Betaling af udstyr er primært et problem for borgerne, der kun har ringe anvendelsesmuligheder. Virksomheder er villige til at betale den nødvendige pris, hvis blot anvendelsesmulighederne er tilstede.
- En nødvendig forudsætning for, at befolkningen investerer i udstyr til digital signatur er, at applikationerne er tilstede. Fokuser på udvikling af visionære applikationer, som befolkningen har ægte gavn af.

Transaktionsmængde

For at investeringen i digital signatur er rentabel, skal der være et vist antal transaktioner. Samtidig skal antallet af ydelser være højt.

Hvorledes sikres et tilstrækkeligt højt antal transaktioner og services?

- Initiativet "personlig internetadgang" vil stimulere brugen af digital signatur voldsomt.
- "Value for money"-produkter vil "trække" brugen af digital signatur i gang.
- Fokusering på specifikke målgrupper kan skabe en kritisk masse.
- Kommuner og andre offentlige organisationer kan udstede certifikater til medarbejdere for at skabe en kritisk masse og udbrede kendskabet til teknologien og dens anvendelse.

Teknik

Pilotprojekterne har vist, at brugen af digital signatur er vanskelig for uerfarne PC-bruger.

Hvordan kan brugen af digital signatur gøres enklere?

- Den teknologiske udvikling vil automatisk gøre brug af digital signatur simplere. Et eksempel er understøttelse af stærk kryptering, der nu er standard i alle produkter.
- Vælg simple løsninger baseret på standardprodukter. Undgå løsninger der ikke kan downloades og installeres "automatisk".
- Fokusér på rene software-baserede løsninger.