IT- og Telestyrelsen
Ministeriet for Videnskab
Teknologi og Udvikling

Digital Signatur Infrastrukturen til digital signatur

IT- og Telestyrelsen

December 2002

Infrastrukturen til digital signatur

Resumé: I fremtiden vil borgere og myndigheder ofte have brug for at kunne kommunikere nemt og sikkert med hinanden – fx udveksle personfølsomme oplysninger. Begge parter vil som minimum kræve sikkerhed for, at meddelelsen kommer fra den, der påstår at have sendt den, at den ikke er blevet ændret, siden den blev sendt, og at ingen uvedkommende har kunne læse den.

En sådan sikker kommunikation kan opnås ved brug af en såkaldt Public Key Infrastructure, PKI. Det vil sige en elektronisk infrastruktur, der består af følgende tæt forbundne elementer:

- Applikationer til kryptering og digital signering – PC baserede programmer, der sikrer uproblematisk anvendelse af krypterings- og signeringsnøgler
- Certifikater - en slags elektronisk pas til identificering af indehaveren, og som rummer den offentlige nøgle
- Et certificeringscenter - en pålidelig tredjepart, der udsteder og fornyer certifikater og f.eks. sørger for at spærre certifikater, der er blevet misbrugt
- Procedurer eller faciliteter til sikker generering og opbevaring af den private nøgle.

Med PKI-teknologien er det muligt for to parter at sikre deres indbyrdes kommunikation. Teknologien giver mulighed for, at parterne kan identificere sig entydigt over for hinanden, hemmeligholde deres kommunikation, samt signere meddelelser digitalt, så modtageren både ved, hvem den kommer fra, og at den ikke er ændret undervejs.

Denne vejledning uddyber disse begreber og sammenhængen mellem dem. Den er særlig henvendt til IT-chefer, projektledere og andre, der aktivt skal være med til at implementere digital signatur i en offentlig myndighed.

Indholdsfortegnelse

1 Formål og målgruppe

Denne vejledning introducerer læseren til de grundlæggende begreber, der knytter sig til infrastrukturen bag digital signatur. Det gælder især:

- Autenticitet, integritet og fortrolighed
- Kryptering og digital signatur
- Certifikater og sikker identifikation
- Certificeringscentre
- Sikker generering og opbevaring af den private nøgle

Målgruppen for vejledningen er IT-chefer, projektledere og andre, der aktivt skal være med til at implementere digital signatur i en offentlig myndighed.

Vejledningen er én blandt flere om digital signatur. De øvrige er:

- **OCES – en fælles offentlig certifikat-standard**
  Målgruppe: IT-chefer, projektledere og andre, der skal beskæftige sig indgående med digital signatur og implementeringen af denne i myndigheden

- **Digital signatur – forudsætninger og fordele**
  Målgruppe: Beslutningstagere i offentlige institutioner, der skal afveje forudsætninger mod de økonomiske fordele og mulige serviceforbedringer, der ligger i at implementere digital signatur

- **Sikker brug af digital signatur**
  Målgruppe: Beslutningstagere og projektledere, der skal arbejde med digital signatur-projekter

- **Juridiske aspekter ved at bruge digital signatur**
  Målgruppe: Projektledere, jurister og andre, der har et særligt behov for at kende de retlige aspekter af brugen af digital signatur

Alle ovenstående vejledninger findes på, IT- og Telestyrelsens, signatursekretariatets hjemmeside (https://www.signatursekretariatet.dk).

2 Public Key Infrastructure (PKI) – nøglebegreberne

Fundamentet for at udbrede digital signatur er en såkaldt Public Key Infrastructure, PKI. Det vil sige et sammenhængende system af signerings- og krypteringsnøgler, certifikater og certificeringscentre, hvor sidstnævnte fungerer som pålidelige tredjeparter.

Ved at bruge PKI kan man opnå en sikker elektronisk kommunikation. Sikkerheden har tre elementer:

- **Autenticitet** giver modtageren af en meddelelse garanti for, at den kommer fra den person, som påstår at have sendt den
- **Integritet** giver sikkerhed for, at en modtaget meddelelse er identisk med den meddelelse, som afsenderen sendte
- **Fortrolighed** giver sikkerhed for, at ingen uvedkommende kan få kendskab til meddelelsens indhold

Det gør PKI ideel til at understøtte en digital signering af meddelelser, der sendes gennem et åbent netværk som f.eks. internettet.

For at sikre autenticitet, integritet og fortrolighed skal PKI imidlertid indeholde en række nøgleelementer: Applikationer til kryptering og digital signering, certifikater, certificeringscentre og procedurer eller faciliteter til nøglegenerering og beskyttelse. Disse elementer gennemgås i det følgende.

3 Applikationer til kryptering og digital signering

Med henblik på at forstå betydningen af applikationer til kryptering og digital signering i et PKI, er det nødvendigt først at beskrive deres funktioner, nemlig kryptering og digital signatur.

3.1 Kryptering

Når en borger og en myndighed kommunikerer elektronisk med hinanden, kan de have behov for at udveksle følsomme personlige data og informationer, som ikke må kunne læses af uvedkommende. Enhver myndighed eller organisation, som sender eller modtager følsomme personoplysninger, har pligt til at sikre, at uvedkommende ikke får kendskab til oplysningerne. Det kan blandt andet ske ved at kryptere kommunikationen.

Kryptering kan sikre, at en meddelelse kun kan læses af netop den modtager, den er tiltænkt – f.eks. den enkelte borger eller en bestemt medarbejder i den offentlige forvaltning.

Ved kryptering kodes meddelelsens indhold, så den fremstår som ulæselig. Denne forvanskning sker på en kontrolleret måde, så indholdet senere kan genskabes. Man siger, at meddelelsen først krypteres og senere – når den skal læses igen – dekrypteres.

En vigtig forudsætning for kryptering er såkaldte nøgler. Nøgler er den information, computeren bruger, når en meddelelse skal krypteres og dekrypteres. Læs mere om kryptering og nøgler i tekstboksen.

En simpel krypteringsnøgle
Kryptering er gennem flere tusind år blevet brugt til at sende meddelelser hemmeligt. En tidlig og simpel metode er at erstatte hvert bogstav i en meddelelse med det bogstav, der ligger f.eks. 5 bogstaver længere fremme i alfabetet. Dvs. at a bliver til e, b til f osv.

Nøglen er i dette eksempel "5". Meddelelsen "Hvad Gud har bundet" bliver krypteret til "møfilæimfxgæsijz", idet ordmellemrummene er fjernet for at gøre det sværere at bryde krypteringen. Man dekrypterer naturligvis meddelelsen ved først at erstatte hvert bogstav med det, der ligger 5 bogstaver før i alfabetet, og derefter ud fra indholdet fastslå, hvor mellemrummene skal placeres.

Den form for kryptering, der er beskrevet i tekstboksen kaldes symmetrisk kryptering, fordi man bruger den samme nøgle til at kryptere og dekryptere meddelelsen. Nøglen er "en fælles hemmelighed" og skal derfor være tilgængelig for både afsenderen og modtageren. Et forhold, der gør anvendelse af symmetrisk kryptering kompliceret, f.eks. i situationer hvor mange mennesker skal kommunikere med en myndighed. Det er desuden en meget stor udfordring at overføre den hemmelige nøgle sikkert mellem afsender og modtager.

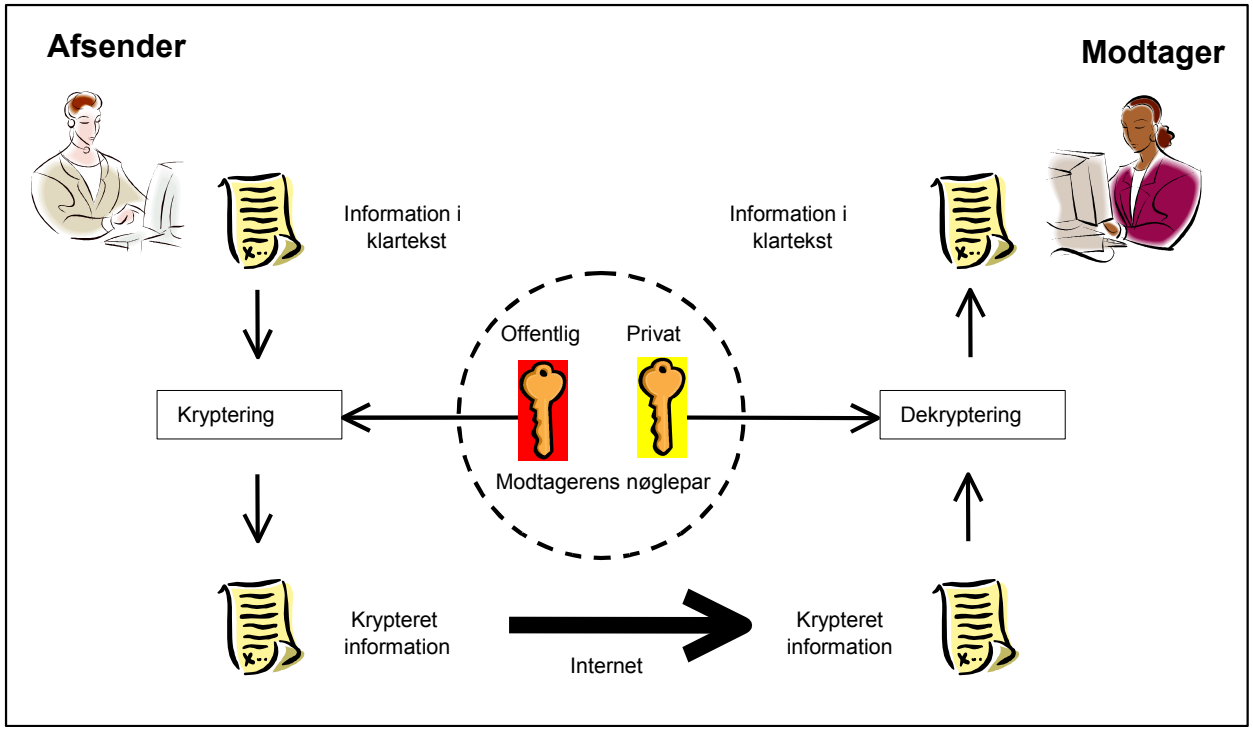
En PKI bygger derimod på asymmetrisk kryptering, hvor der bruges et nøglepar med to forskellige nøgler:

- En offentlig nøgle, som kan være frit tilgængelig for alle.
- En privat nøgle, som holdes hemmelig.

De to nøgler i et sådant nøglepar kan kun fungere i sammenhæng. En meddelelse, som krypteres med den ene nøgle, kan således kun dekrypteres med den anden nøgle og omvendt. Samtidig er det i praksis umuligt ud fra kendskab til den offentlige nøgle at gætte eller beregne sig til den private nøgle.

Figur 1 viser et eksempel, hvor en borger sender fortrolige oplysninger til en bestemt medarbejder i en offentlig myndighed. Borgeren bruger medarbejderens offentlige nøgle

til at kryptere sin meddelelse med. Nu kan kun den person, som er i besiddelse af den private nøgle - altså den pågældende medarbejder - dekryptere og læse meddelelsen.



Figur 1: Asymmetrisk kryptering: *Kernen i asymmetrisk kryptering er, at modtageren har den unikke private nøgle, som kræves for at dekryptere meddelelsen. På den måde er afsenderen sikker på, at meddelelsen ikke falder i de forkerte hænder undervejs.*

3.2 Digital Signering

Anvendelse af asymmetriske nøglepar skaber mulighed for entydig identifikation af den private nøgle. Ingen nøglepar er ens og såvel den offentlige, som den private nøgle er derfor unikke. Digital signering fungerer således, at anvendes den private nøgle til kryptering af en meddelelse, vil denne alene kunne dekrypteres med den tilhørende offentlige nøgle. Modtageren af meddelelsen kan derfor være sikker på, at afsenderen har anvendt den unikke private nøgle, der er knyttet til den offentlige nøgle.

Kryptering med den private nøgle er således med til at sikre autenticitet, men alene for, at den private nøgle er anvendt. Reel autenticitet, dvs. sikkerhed for at en person er

den, han udgiver sig for, og at personen er den rette indehaver af den private nøgle, kræver involvering af et certifikat og et certificeringscenter, der behandles i henholdsvis afsnit 4 og 5.

Digital signatur handler dog ikke alene om autenticitet. Der skal også være sikkerhed for, at den meddelelse, der er underskrevet er identisk med den, der modtages. Denne integritet sikres ved at hashe meddelelsen, dvs. give denne et unikt digitalt fingeraftryk. Læs mere om hashing i tekstboksen.

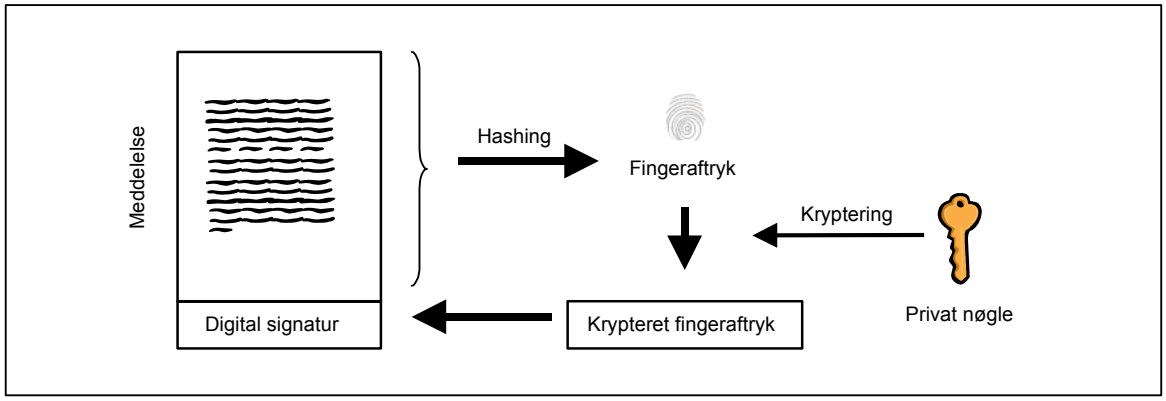
Hashing:
Hashing er transformationen af en meddelelse til en streng af en fast længde (kaldet hash værdien) via en bestemt algoritme. Hash algoritmen kaldes også for en hash funktion og skrives *H(x)*, hvor *x* er en meddelelse. Hash funktionen anvendes i kryptografiske sammenhænge for at effektivisere signatur og integritets mekanismer. Hash funktioner, der anvendes til kryptografiske formål har udover transformationsegenskaben følgende egenskaber:

- *H(x)* kan anvendes på en meddelelse af stort set vilkårlig længde
- Det er hurtigt at beregne *H(x)* for alle *x*
- *H(x)* er en en-vejs funktion, dvs. at det er usandsynligt at finde den meddelelse som svarer til en bestemt hashværdi
- *H(x)* er kollisionsfri, dvs. at det er usandsynligt at to forskellige meddelelser giver samme hashværdi. Hermed kan hashværdien simulere et "fingeraftryk" af meddelelsen

Kryptering med den private nøgle og hashing er fundamentet for at skabe en digital signatur. I det følgende gennemgås, hvorledes man i praktisk signerer en meddelelse digitalt og hvorledes modtageren kan kontrollere den.

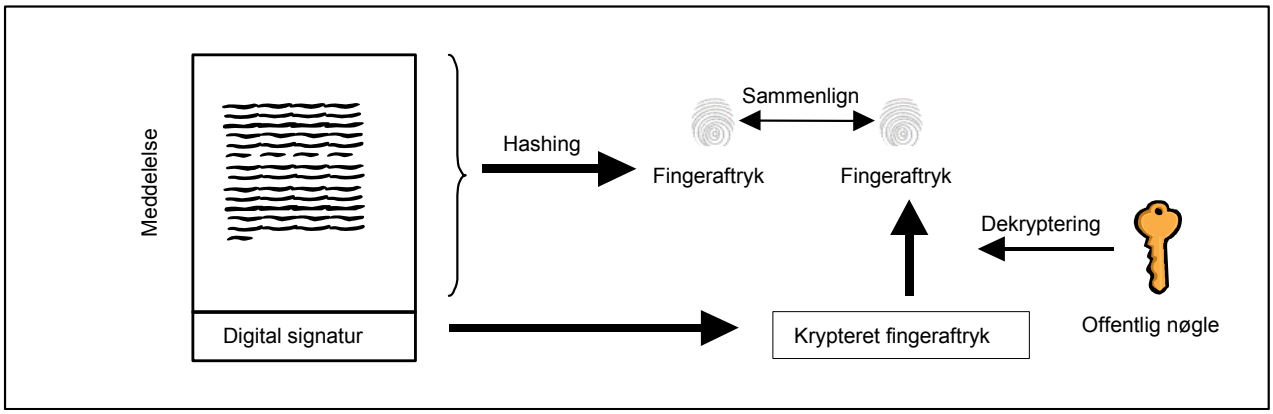
3.3 Fremstilling og kontrol af en digital signatur

En digital signatur fremkommer ved at hashe den meddelelse, som skal signeres. Resultatet bliver en unik værdi, som er baseret på indholdet i meddelelsen. Denne værdi kaldes også en tjeksum og kan betragtes som meddelelsens digitale fingeraftryk. Afsenderen af meddelelsen krypterer herefter fingeraftrykket med sin private nøgle. Den digitale signatur, der hermed skabes, vedhæftes den originale meddelelse, der nu er digitalt signeret. Da asymmetrisk kryptering er 100 gange langsommere end symmetrisk kryptering, er det kun tjeksummen og ikke hele meddelelsen, der bliver krypteret. Figur 2 viser princippet i, hvordan en digital signatur fremstilles.



Figur 2: Sådan fremstilles en digital signatur: *En digital signatur er et krypteret fingeraftryk af den meddelelse, man sender. Ens "underskrift" er altså forskellig fra gang til gang.*

En digital signatur har samme formål som en almindelig underskrift. Den garanterer over for modtageren af meddelelsen, hvem afsenderen er, og at den modtagne meddelelse er identisk med den, der blev signeret. Figur 3 viser, hvordan modtageren kontrollerer den digitale signatur på en meddelelse.



Figur 3: Sådan kontrolleres en digital signatur*: Modtageren af en signeret meddelelse bruger afsenderens offentlige nøgle til at genskabe den tjeksum, afsenderens computer beregnede for meddelelsen, og sammenligne den med sin egen beregning. Hvis de to tal er identiske, er meddelelsen uændret, og afsenderen identificeret.*

Først bruger modtageren afsenderens offentlige nøgle til at dekryptere det krypterede fingeraftryk, som er vedhæftet meddelelsen.

Dernæst lader modtageren meddelelsen gennemløbe den samme hashing, som afsenderen udførte. Resultatet er et fingeraftryk, som modtagerens computer sammenligner med det fingeraftryk, som afsenderen vedhæftede meddelelsen. Kun hvis de to fingeraftryk er helt identiske, kan der ikke være ændret i meddelelsen undervejs fra afsenderen til modtageren, og afsenderens identitet vil kunne fastslås med sikkerhed.

3.4 Applikationer

Kryptering og digital signering er komplekse funktioner, der kræver understøttelse af applikationer, hvis de skal gøres praktisk anvendelige. Derfor er applikationer til kryptering og digital signering en meget væsentlig del af PKI. Applikationerne skal kunne:

- Aktivere en eller flere krypteringsalgoritmer
- Gemme og anvende andres offentlige nøgler og certifikater
- Gemme og anvende rodcertifikater fra certificeringscentre
- Anvende den private nøgle
- Kontrollere gyldighed og tilladt anvendelse af certifikater
- Hashe meddelelser via en anerkendt hashing algoritme

Applikationerne skal også understøtte håndteringen af standardiserede nøgler og certifikater. De fleste certifikatpolitikker er baseret på, at certifikaterne inklusiv rodcertifikater fra certificeringcentrene skal opfylde kravene til et såkaldt standardiseret X.509 certifikat. Applikationerne skal derfor kunne håndtere certifikater af denne type. Se afsnit 4 for en gennemgang af certifikater og deres anvendelse.

Applikationerne skal endvidere kunne kryptere med en algoritme, der anses for at være sikker. Det tidligere IT-sikkerhedsråd angiver i deres vejledning "Praktisk brug af kryptering og digital signatur", at applikationer skal benytte en nøglelængde på mindst 1024 bits, når det drejer sig om RSA-nøgler (et eksempel på et asymmetriske nøglepar). RSA-algoritmen er en af de algoritmer, som benyttes til asymmetrisk kryptering. Det er muligt at benytte andre algoritmer. Valg af algoritme til såvel hashing, som kryptering er en del af den information, som findes i certifikatet.

I forbindelse med den digitale signering, krypteres som tidligere beskrevet, et fingeraftryk af meddelelsen. De to mest udbredte algoritmer til kryptering af dette fingeraftryk er MD5 og SHA-1, hvor SHA-1 anses for den mest sikre. Applikationerne skal derfor understøtte disse algoritmer.

4 Certifikater og sikker identifikation

Som nævnt bygger PKI på to forskellige krypteringsnøgler, en privat nøgle og en offentlig nøgle. Den private nøgle er det kun nøgleindehaveren, der har adgang til. Den offentlige nøgle kan distribueres til alle, som ejeren af den private nøgle ønsker at kunne kommunikere sikkert med. Den er normalt indlagt i et såkaldt certifikat – en datafil, som foruden den offentlige nøgle indeholder oplysninger, der entydigt kan identificere den person, som opbevarer den private nøgle.

Et certifikat er dermed en slags elektronisk pas, hvor det, at en person har adgang til den private nøgle, er et bevis for, at oplysningerne i certifikatet knytter sig til netop denne person – forudsat at den private nøgle er tilstrækkeligt beskyttet imod uvedkommendes (mis)brug.

Certifikatet er digitalt signeret af et såkaldt certificeringscenter, som derved bekræfter, at den indlagte offentlige nøgle svarer til en privat nøgle ejet af den person, der beskrives med f.eks. navn og adresse i certifikatet. Et certificeringscenter betegnes ofte som "en pålidelig tredjepart" og kaldes på engelsk Certificate Authority (CA). Deres funktion beskrives grundigere i afsnit 5.

4.1 Sikker identifikation (Autenticitet)

Når en myndighed tilbyder en tjeneste over internettet, vil den i mange tilfælde ønske eller kræve en sikker identifikation af tjenestens brugere. Det er netop, hvad PKI giver mulighed for gennem de certifikater, certificeringscenteret udsteder.

Figur 4 viser principperne i, hvordan det foregår rent teknisk. I praksis sker udvekslingen af informationer mellem systemerne automatisk på få sekunder. Forløbet er som følger:

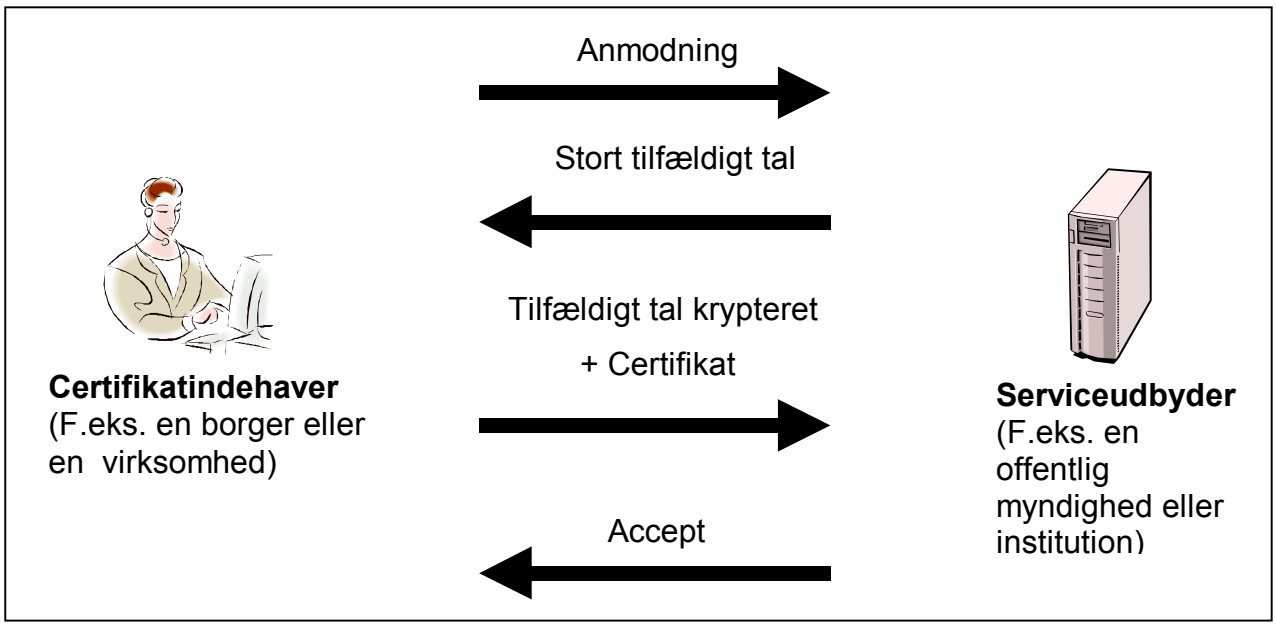
1. Myndighedens system sender et stort tilfældigt tal til brugeren, som bliver krypteret af certifikatindehaverens private nøgle.

2. Det krypterede tilfældige tal sendes tilbage til modtagersystemet sammen med det certifikat, der viser brugerens identitet.

3. Først kontrollerer modtagersystemet ægtheden af brugerens certifikat ved hjælp af certificeringscentrets offentlige nøgle. Så kontrolleres det, at certifikatet ikke er udløbet eller spærret af certificeringscenteret.

4. Derefter benytter modtagersystemet brugerens offentlige nøgle, der er indlagt i certifikatet, til at dekryptere det tilfældige tal. Resultatet sammenlignes med det oprindelige tilfældige tal. Er de to tal ens, kan modtagersystemet gå ud fra, at

brugeren er den person, som er angivet i certifikatet. På tilsvarende måde kan brugeren identificere modtagesystemet.



Figur 4: Sådan tjekkes brugernes identitet: *Borgerens og myndighedens computere skal udveksle informationer fire gange. Først derefter kan begge parter være helt sikre på, hvem de kommunikerer med.*

5 Certificeringscentre

Hvis en PKI skal kunne virke, må alle involverede parter have tillid til den måde, nøgler og certifikater håndteres på. Det kræver et pålideligt certificeringscenter, der kan skabe tillid til infrastrukturen ved en sikker håndtering af certifikater og deres tilhørende offentlige nøgle.

I et certifikat "fastlåser" certificeringscentret oplysninger om en person til en bestemt offentlig nøgle. Det sker ved at forsyne certifikatet med certificeringscentrets digitale signatur.

Foruden at udstede certifikater har certificeringscentret også ansvaret for, at et certifikat, der ikke længere er gyldigt eller pålideligt, hurtigt kan spærres for brug. Det kan f.eks. være upålideligt, fordi den private nøgle er blevet brudt, spredt eller på anden måde kompromitteret. I så fald skrives certifikatets serienummer på en spærreliste, der svarer til de lister, bankerne fører over spærrede kreditkort.

Hvert certificeringscenter kan dog kun tage ansvaret for at opretholde en spærreliste over de certifikater, som det selv har udstedt. Brugerne bør derfor kun have tillid til certifikater, der er udstedt af et certificeringscenter, som de kender. Det er deres eneste garanti for, at kommunikationen har den sikkerhed, de forventer. Ofte vil der, f.eks. i en internetbrowser, være pre-installerede certifikater. Disse certifikater ligger alene i browseren, fordi, certificeringscentret har betalt producenten for det. Det er således ingen garanti for, at certificeringscentret er pålideligt. Den enkelte bruger vurderer selv, om certificeringscentret er pålideligt.

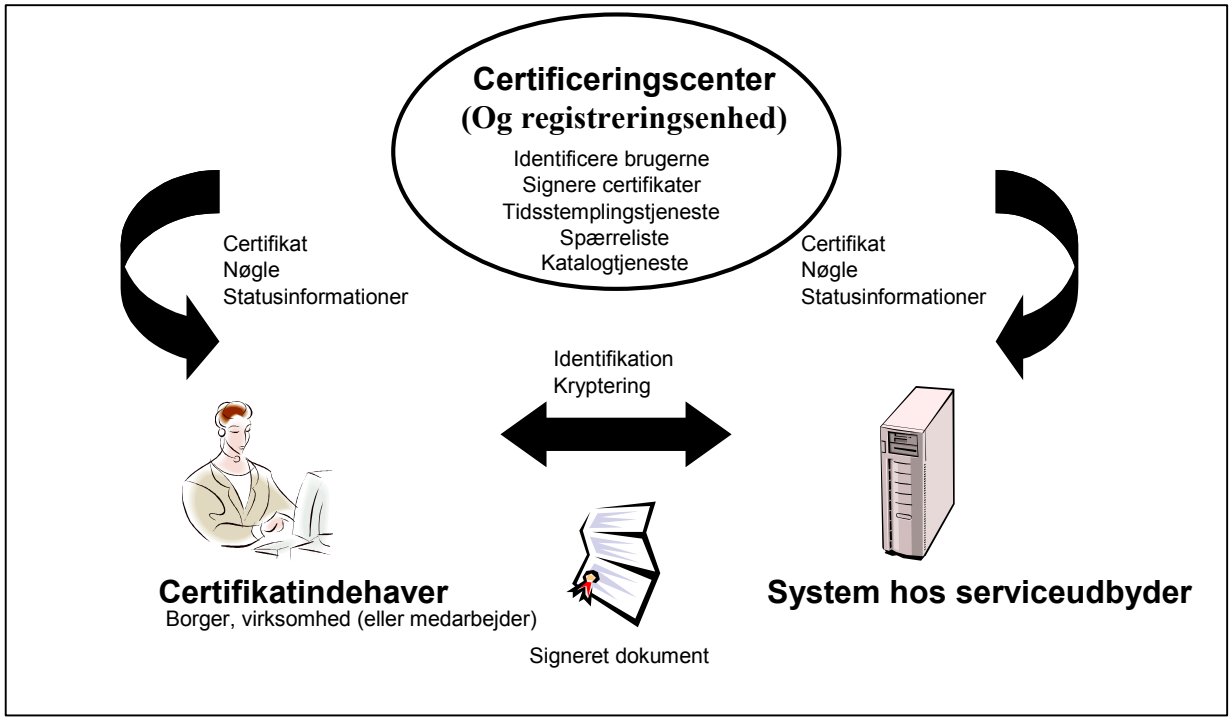
Tillid på tværs af certificeringscentre
Der findes i hvert fald tre forskellige løsninger på problemet med mange konkurrerende certificeringscentre:

- at brugerne og myndighederne i deres systemer skaber tillid til flere forskellige certificeringscentre
- at certificeringscentrene skaber tillid til hinanden ved krydscertificering
- at alle certificeringscentre har tillid til og er godkendt af en overordnet udsteder af certifikater

Ingen af de to sidstnævnte løsningsmodeller er endnu indført i Danmark.

Den "myndighed", som er ansvarlig for at identificere og behandle ansøgninger fra en kommende certifikatindehaver, kaldes registreringsenheden. I forbindelse med udstedelse af certifikater kan f.eks. posthuse blive anvendt, som registreringsenheder, hvor borgere som led i udstedelsesproceduren møder op og får kontrolleret deres

identitet baseret på et legitimationsdokument med billede. Certificeringscenteret og registreringsenheden kan godt være en og samme enhed, hvis certificeringscenteret også har ansvaret for at identificere certifikatindehaveren. Figur 5 viser de funktioner, et certificeringscenter skal udføre, og de informationer, der overføres mellem deltagerne i en PKI.



Figur 5: Et certificeringscenters opgaver: *Certificeringscenteret fungerer som en pålidelig tredjepart mellem afsender og modtager. Det udsteder certifikater, der garanterer parternes identitet over for hinanden. Og det sikrer, at certifikater kan spærres, når de misbruges. I figuren er certificeringscenteret og registreringsenheden den samme enhed.*

Udover certifikater til borgerne som privatpersoner kan der også udstedes andre typer af certifikater:

- **Virksomhedscertifikater** til myndigheder og firmaer
- **Medarbejdercertifikater** til medarbejdere i myndigheder og firmaer
- **Servercertifikater** til udstyr, der giver adgang til digitale tjenester

Certificeringscentrets kvalitetsstandarder
De procedurer og sikkerhedsmæssige foranstaltninger, som certificeringscentret skal følge og opretholde, når det udsteder og administrerer certifikater, er beskrevet i en certificeringspolitik. Certificeringscenteret beskriver i en Certificate Practice Statement (CPS), hvorledes det opfylder certifikatpolitikken. Af CPS'en fremgår alt fra rutiner og krav til sikkerhed ved fremstilling af nøgler og certifikater til en beskrivelse af, hvordan certificeringscenteret sikrer sig, at andre ikke får adgang til de private nøgler, som certificeringscenteret selv bruger ved signering af certifikater og spærrelister m.m..

Ved visse overførsler af information er det vigtigt senere at kunne fastslå nøjagtigt, hvornår den pågældende kommunikation fandt sted. Derfor kan det være nødvendigt at lade en betroet tredjepart tidsstemple den digitale signatur.

6 Sikker generering og opbevaring af den private nøgle

Sikkerheden i PKI er meget afhængig af den private nøgle og derfor også i høj grad af, at den private nøgle er beskyttet mod, at uvedkommende kan bruge den. Derfor er det almindeligt, at nøglen gemmes som en krypteret fil på en pc, en server eller på en diskette. Det kræver i så fald en adgangskode at kunne bruge nøglen Når den private nøgle er beskyttet på denne måde, kaldes det en softwarebaseret nøgle.

Man kan også beskytte den private nøgle ved at opbevare den på et chipkort. Det kaldes en hardwarebaseret nøgle og regnes for mere sikkert. Den private nøgle behøver nemlig aldrig at forlade chipkortet og er dermed godt beskyttet mod alle kendte former for "indbrud" så som virus, trojanske heste o.l. Problemet er, at hardwarebaserede nøgler er væsentligt dyrere og noget mere komplicerede at indføre. Eksempelvis kræver de, at brugerens pc er forsynet med en kortlæser.

I praksis genereres nøgleparret i en PKI af computerprogrammer ved hjælp af et tilfældigt tal. Kvaliteten af nøgleparret afhænger i høj grad af, at tallet er så stort og "tilfældigt", at ingen kan regne sig frem til den private nøgle (inden for en overskuelig tid).

I PKI'er, der bruger softwarebaserede nøgler, genereres nøglerne som regel på signaturindehaverens egen pc. Det betyder, at den pålidelige tredjepart, der skal garantere sikkerheden ved nøglerne, principielt ikke har fuld kontrol over de genererede

nøglers kvalitet. Desuden kan den pc, hvor nøglerne genereres, være inficeret med virus, der muliggør kompromittering af nøglen. Generelt kan der dog opnås en høj sikkerhed med softwarebaserede nøgler, hvis brugeren beskytter dem med adgangskode.

Bruger man hardwarebaserede nøgler, vil de normalt kunne genereres og lagres på chipkortet under tredjepartens fuldstændige kontrol – uden at tredjeparten dog kan få indblik i eller påvirke nøgleparret.

7 Andre sikkerhedsaspekter i PKI

7.1 Flere nøglepar kan øge sikkerheden

For at gøre brugen af digital signatur endnu sikrere, anbefales det ofte, at en bruger råder over flere nøglepar med tilhørende certifikater. Så kan et af disse nøglepar reserveres til at underskrive meddelelser eller til, når kommunikationen skal gøres uafviselig, dvs. sikring af, at afsenderen ikke senere kan benægte at have afsendt en meddelelse. Certifikatets anvendelse fremgår af certifikatet.

Det er nemlig langt fra al kommunikation, som det er nødvendigt at signere. Ofte vil brugeren blot have brug for at identificere sig, holde sin meddelelse hemmelig eller sikre dens integritet. For at adskille disse behov, kan det være fornuftigt med to eller flere forskellige nøglepar, f.eks. et par til signering samt et par til kryptering og dekryptering. Den private nøgle, der bruges til den kommunikation, som kræver særlig høj sikkerhed, anvendes herved i mindre omfang og risikoen for kompromittering reduceres.

Det kan være ønskeligt eller nødvendigt for brugeren at opbevare en ekstra kopi af den private nøgle, der skal anvendes til at dekryptere meddelelser, som er krypteret med den tilsvarende offentlige nøgle. Også dette aspekt taler for anvendelsen af flere nøglepar, idet det i så tilfælde alene vil være den private nøgle til dekryptering af meddelelser og ikke den private nøgle til signering, der skal opbevares en kopi af.

Der er desuden særlige problemer forbundet med at signere skemaer, der udfyldes direkte over internettet. Disse problemer vil blive behandlet i en senere vejledning, hvor problematikken vil blive belyst, og hvor der vil blive præsenteret konkrete løsningsforslag. Vejledningen forventes udarbejdet ultimo 2002.

7.2 Uafviselighed

Uafviselighed er efter autenticitet, integritet og fortrolighed et fjerde sikkerhedsaspekt i PKI.

At en meddelelse er uafviselig betyder, at den som har afsendt en meddelelse ikke efterfølgende kan benægte at have afsendt den, og at modtageren ikke kan benægte at meddelelsen er modtaget. Uafviselighed i PKI kan derfor sammenlignes med afsendelsen af et anbefalet brev, hvor afsender overfor en betroet tredjepart, postvæsenet, godtgør, at det er ham, der har sendt brevet, og hvor postvæsenet sørger for en kvittering på, at brevet er modtaget hos modtageren. Ligesom med et anbefalet brev, er sikring af uafviselighed således en tillægstjeneste til den almindelige kommunikation i PKI.

Det er naturligvis vigtigt at vide, at en meddelelse ikke er ændret undervejs fra afsenderen til modtageren (integritet), og at meddelelsen kommer fra den person, som påstår at have afsendt den (autenticitet). Sikring af uafviselighed kræver dog tillige en notarfunktion, dvs. en betroet tredjepart med tidsstemplingstjeneste og arkiveringsfunktion.

Tidsstemplingstjenesten skal sikre, at der ikke kan herske tvivl om, på hvilket tidspunkt meddelelsen er sendt henholdsvis modtaget. Det nøjagtige tidspunkt kan være meget væsentlig i f.eks. ansøgningssager med en konkret ansøgningsfrist. Ansøgningen vil måske alene kunne komme i betragtning, hvis den er modtaget inden ansøgningsfristens udløb. Her vil en tidsstemplingstjeneste kunne afgøre tvivlssager, idet denne som nævnt vil kunne fastslå det nøjagtige afsendelses- og modtagelsestidspunkt.

Arkiveringsfunktionen har en anden rolle, nemlig at registrere (logge) hændelsesforløbet i forbindelse med en transaktion. Konkret skal arkivfunktionen sikre, at logningen af opslag på spærrelisten, selve spærrelisten og afsenders certifikatet gemmes i krypteret form. Afviser modtageren f.eks. en ansøgning på grund af, at certifikatet er udløbet eller spærret, skal det i tvivlssager være muligt at bestemme, om det også var tilfældet.