

Digital signatur og PKI i sundhedsvæsenet

November 2003

Udgivelsesdato : 19. november 2003
Udarbejdet : Carl Bro & Sundhedsstyrelsen

Denne rapport er udarbejdet som et beslutningsgrundlag i forbindelse med brug af digital signatur i sundhedsvæsenet.

Web: www.sst.dk
Kontakt: sesi@sst.dk
Tlf. 7222 7400
Sundhedsstyrelsen,
Islands Brygge 67
2300 København S

Emneord: Digitalsignatur, PKI, signaturreport, adgangsstyring, autentifikation, kryptering

ISBN-elektronisk: 87-91361-75-3

Indholdsfortegnelse

Side

1	Indledning	3
1.1	Overordnede mål med digital signatur i sundhedsvæsenet	3
1.2	Resume og overordnede anbefalinger	4
1.3	Tidshorisont	5
1.4	Sundhedsportalen	6
2	Problemstillinger og anbefalinger	7
2.1	Mål og behov vedr. digital signatur i sundhedsvæsenet	7
2.1.1	Sikring af autenticitet	7
2.1.2	Sikring af fortrolighed	8
2.2	Digitale certifikater i sundhedsvæsenet	9
2.2.1	Certifikater til sikring af autenticitet	9
2.2.2	Certifikater til sikring af fortrolighed	13
2.3	Software- vs. hardware-certifikater	16
2.3.1	Alternative hw-tokens	17
2.4	Brugen af OCES-certifikater	18
2.5	Information i certifikater	19
2.6	Identifikation af virksomhederne i sundhedsvæsenet	20
2.7	Identifikation af medarbejderne i sundhedsvæsenet	21
2.8	Administration og procedurer omkring certifikater	22
2.8.1	De administrative roller	22
2.8.2	CA's rolle, opgaver og ansvar	23
2.8.3	LRA's rolle, opgaver og ansvar	23
2.8.4	Fornyelse af certifikater	24
2.8.5	LRA organisationen i sundhedsvæsenet	24
2.9	Brugerstyring og brugerkatalog	25
2.9.1	Et fælles brugerkatalog	25
2.9.2	Informationen i brugerkataloget	26
2.9.3	Administration af brugerkataloget	27
2.9.4	Udveksling af information om adgangsrettigheder	28
2.10	Single sign-on og sikker adgang til sundhedsapplikationer	29
2.11	Lovgivning og det formelle grundlag	30
2.12	Økonomiske aspekter	30
2.13	Eksterne relationer og projekter	30
2.14	Problemområder	31
2.14.1	Langtidsarkivering af signaturer og signerede data	31
2.14.2	Applikationernes understøttelse af digital signatur og certifikater	31
2.14.3	Brugen af forkant-teknologi og -tjenester	31
3	Pilotprojekter og initiativer	32
3.1	Vurdering af egnede hw-tokens	32
3.2	LRA-funktionalitet og LRA-procedurer	32
3.3	Retningslinier for håndtering af OCES-certifikater i nye applikationer	33
3.4	Biometriske metoders fordele og ulemper i forskellige arbejdssituationer	33
3.5	Brugerkatalog og brugerstyring	34
Bilag A	Referencer	35
Bilag B	Begreber og Forkortelser	36
Bilag C	Tekniske løsningselementer	48
C.1	Komponenter vedr. single sign-on med certifikat	48
C.2	Integritet og ægthed i data – krav til applikationerne	50
Bilag D	Eksempel på LRA web-tjeneste (OCES)	51
Bilag E	Omkostningselementer og økonomi	52

1 Indledning

Den digitale signatur er både pga. teknologiens større modenhed og via initiativer og projekter i flere sektorer på vej ind som en facilitet til både borgere, virksomheder og offentlige organisationer i Danmark.

Efter lanceringen i 2003 af det nationale OCES-koncept – ”Offentlige Certifikater til Elektronisk Service” (ref. 1) er der blevet yderligere fokus på at udnytte de muligheder, der ligger i at benytte elektroniske certifikater til opnåelse af bedre sikkerhed og erstatte papiret med elektroniske tjenester og arbejdsgange.

I sundhedsvæsenet vil den digitale signatur finde anvendelse for såvel sundhedsprofessionelle¹ som for borgerne, som vil kunne få adgang til fx egne journaldata og til booking mv. via elektroniske tjenester.

Denne rapport vurderer centrale problemstillinger og forskellige koncepter for brugen af digital signatur og elektroniske certifikater i sundhedsvæsenet og giver anbefalinger på området. Rapporten indgår som et led i forudsætningerne for gennemførelsen af ”Initiativ 24” vedr. informationssikkerhed og den generelle sikkerhed omkring IT-systemers patientdata i den nationale IT-strategi for sundhedsvæsenet 2003-2007 (ref. 7).

Rapporten er skrevet i perioden maj 2003 – november 2003 i samarbejde mellem Sundhedsstyrelsen, SESI og Carl Bro.

1.1 Overordnede mål med digital signatur i sundhedsvæsenet

Nogle af de fordele, der forventes for arbejdsgange og for sikkerhed ved indførelse og brug af digital signatur i sundhedsvæsenet, er følgende:

- single sign-on til de mange applikationer, som sundhedsprofessionelle dagligt skal have adgang til
- forøgelse af sikkerheden i forhold til fysisk underskrift
- forøgelse af sikkerheden i forhold til traditionel bruger-id- / password-baseret adgang
- sparet tid til administrative procedurer
- sparet tid til blanketudfyldelse (dødsattester mv.)
- mere tidstro opdatering af fælles registre
- opnåelse af en vigtig forudsætning for overgang fra papirbaserede arbejdsgange og papirbaseret information til digital forvaltning med fuld elektronisk betjening, sagsbehandling og arkivering mv.

¹ Jf. ordlisten i bilag B benyttes udtrykket ”sundhedsprofessionelle” om alle personer, som har autorisation i sundhedsvæsenet og/eller har adgang til at benytte og/eller skabe klinisk information, dvs. sundhedsprofessionelle omfatter læger, sygeplejersker, fysioterapeuter, lægesekretærer, SoSu-assistenten m.fl.

Det forventes principielt, at alle personalegrupper vil blive berørt af indførelse af digital signatur, men i første omgang vil det nok primært dreje sig om følgende:

- De fleste sundhedsprofessionelle på sygehuse
- Praktiserende læger
- Laboratorier
- Hjemmeplejen
- Apoteker

Arbejdsprocedurerne og dagligdagen på mange arbejdspladser i sundhedsvæsenet peger mod en løsning, hvor certifikat og nøgler er placeret på hardware – såkaldt ”hw-token” – fx chipkort. Såfremt dette bliver løsningen, vil der givetvis være andre anvendelser af den valgte hw-token end til opbevaring af certifikater, fx fysisk adgangskontrol. Dette kan medvirke til at fremme en kultur, hvor en hw-token er en naturlig fysisk og elektronisk ”adgangsnøgle”, som alle bærer på sig overalt, og som man husker at tage med sig efter at have benyttet den til systemadgang.

Set ud fra et sikkerhedsperspektiv vil indførelsen af en hardware-baseret digital signatur give såkaldt ”stærk” autentificering, dvs. at adgang til sundhedssystemer og klinisk information baseres på (mindst) to af følgende tre adgangsnøgler:

- 1) Viden – noget man ved (fx PIN-kode)
- 2) Hardwarenøgle – noget man har (fx chipkort)
- 3) Biometrisk identifikation – noget man er (fx fingeraftryk)

1.2 Resume og overordnede anbefalinger

Dette afsnit resumerer i kort form hovedpunkterne og de overordnede anbefalinger. Der henvises til ordlisten i Bilag B mht. forklaring af begreber og forkortelser.

Bruger-autenticitet for sundhedsprofessionelle

Det primære behov ifm. brugen af digital signatur og certifikater i sundhedsvæsenet er behovet for at sikre ”brugerautenticitet”, dvs. at den enkelte sundhedsprofessionelle er den, som han/hun giver sig ud for at være, og kun via verificeringen af denne autenticitet får vedkommende adgang til sundhedssystemer og klinisk information.

Medarbejdercertifikater knyttet til sundhedsautorisation

Verificeringen af brugerautenticiteten anbefales at ske ved brug af medarbejdercertifikater, som udstedes til sundhedspersoner sammen med deres erhvervelse af autorisation i sundhedsvæsenet.

OCES-medarbejdercertifikater på hw-tokens

Selve realiseringen af certifikaterne anbefales at ske i form af OCES-certifikater overvejende på hardware-tokens, fx chipkort. Alternativt kan software-certifikater anvendes, hvor dette understøtter arbejdsgangene i sundhedsvæsenet.

Samarbejde med TDC

For at opnå den bedste løsning anbefales det at indgå et samarbejde med TDC, som er certificeringscenter for OCES-certifikater, omkring en definition af medarbejdercertifikater og certifikatadministration (LRA-funktionalitet) i sundhedsvæsenet

og en løsning med certifikaterne på chipkort eller anden form for egnet hardware-token.

Brugerkatalog, brugerstyring og single sign-on

Som grundlag for at definere brugeradgangsrettigheder for de sundhedsprofessionelles adgang til systemer og klinisk information anbefales det at etablere et fælles brugerkatalog med tilhørende procedurer for brugerstyring. Indførelsen af certifikat-baseret autenticitet i sundhedsvæsenet vil eksponere behovet for et sådant fælles brugerkatalog. Dette brugerkatalog vil blive grundlaget for "single sign-on" scenariet og for administration af tværgående adgangsrettigheder i hele sundhedsvæsenet.

Vedligeholdelsen af roller og rettigheder

Brugerstyringen anbefales opbygget på et standardiseret grundlag, hvor sundhedsprofessionelle via deres certifikat knyttes til fælles definerede "generiske" roller og tildeles adgangsrettigheder i brugerkataloget. Vedligeholdelsen af informationen i brugerkataloget anbefales at ske lokalt i de enkelte sundhedsinstitutioner, der opdaterer ansættelsesoplysninger og har ansvar for adgangen til klinisk information, dvs. i princippet de samme funktioner, som varetager definitionen af brugerrettigheder i dag – blot (oftest) i lokale systemer.

Andre anvendelser af digital signatur og certifikater

Sundhedssystemerne vil også skulle anvende teknologien omkring certifikater og digitale signaturer til at sikre konfidentialitet og beskyttelse af mere systemteknisk art. Dette vil for den enkelte sundhedsprofessionelle ske usynligt bag faciliteter i systemerne, som skal designes og realiseres, så beskyttelsen af følsomme data ikke ganske overlades til den enkelte brugers eget initiativ og færdigheder.

Pilotprojekter

Det anbefales at iværksætte relevante pilotprojekter – såvel mindre pilotprojekter med fokus på teknologivurdering som større pilotprojekter med fokus på vurdering og omlægning af arbejdsgange. De emner, der i første omgang er peget på, er vurdering af egnede hardware-tokens, samarbejde med TDC vedr. certifikater og deres administration samt udvikling af retningslinier for justering af sundhedsapplikationer, så digital signatur understøttes.

1.3 Tidshorisont

Indførelsen af digital signatur i sundhedsvæsenet vil indebære en ny metode og teknologi for autentificering og sikkerhed og vil give nye arbejdsgange i forskellige situationer. Digitale signaturer vil åbne for nye muligheder, men vil også på kort og mellemlangt sigt supplere de eksisterende systemer og procedurer.

Tidshorizonten for indførelse og udbredelse af digitale signaturer i sundhedsvæsenet vil være en længere årrække. Hver enkelt af de følgende hovedaktiviteter må forventes at ske over en periode, der strækker sig fra i dag og et til flere år, for nogle aktiviteter vedkommende 5-10 år, fremover. Selve anskaffelsen af certifikater (listens pkt. 1) vil kunne ske på forholdsvis kort sigt, men den fulde udnyttelse i hele sundhedsvæsenet vil forudsætte, at alle aktiviteter er gennemført.

1. Anskaffelse af certifikater til alle sundhedsprofessionelle, herunder etablering af de administrative procedurer og de tekniske systemer til administration og vedligeholdelse af certifikaterne.
2. Opgradering af de lokale IT-infrastrukturer, så brugerne kan benytte (hardware-baserede) certifikater på sundhedsvæsenets pc'er og arbejdspladser.
3. Etablering af den nødvendige brugerstyring inkl. de administrative procedurer omkring definition og vedligeholdelse af rettigheder mv.
4. Implementering og ibrugtagning af nye applikationer, herunder EPJ-systemer, som understøtter brugen af digitale signaturer og certifikater samt udfasning af de "gamle" applikationer og systemer, som det ikke er formålstjenligt eller økonomisk forsvarligt at opgradere, så certifikat-baseret sikkerhed understøttes.
5. Gennemførelse af en standardisering og etablering af de nødvendige procedurer. Dette vil være en forudsætning for, at sundhedsprofessionelle kan benytte deres certifikat og signatur på tværs af hele sundhedsvæsenet og til alle sundhedssystemer i Danmark.

Der vil således komme en overgangsfase, hvor digitale signaturer på nogle områder benyttes parallelt med eksisterende systemer og traditionelle sikkerhedsprocedurer og parallelt med papirbaserede arbejdsgange. På længere sigt er det visionen, at digitale signaturer vil være en del af grundlaget for fuld overgang til "digital forvaltning" (ref. 5), hvor alle arbejdsgange og al information er baseret på elektronisk sagsbehandling. Mangfoldigheden af applikationer og IT-løsninger i sundhedsvæsenet samt kravet om døgn drift året rundt vil ydermere bidrage til, at overgangsfasen vil være en årrække og indebære en vis redundans og forskellighed i de daglige arbejdsgange for de sundhedsprofessionelle.

1.4 Sundhedsportalen

Amtsrådsforeningen har taget initiativ til at etablere en offentlig sundhedsportal i samarbejde med andre parter på sundhedsområdet, bl.a. Sundhedsministeriet, Sundhedsstyrelsen, H:S og Kommunernes Landsforening (ref. 8 og 9). Det er et mål, at denne sundhedsportal – kaldet "Sundhedsportalen" med web-adressen www.sundhed.dk – skal fungere som en ramme for den elektroniske kommunikation mellem sundhedsvæsenets parter og i kommunikationen med patienterne / borgerne. Sundhedsportalen forventes lanceret med de første tjenester omkring årsskiftet 2003/04.

Parterne bag Sundhedsportalen har besluttet at digitale signaturer og certifikater skal benyttes såvel af borgerne som af de sundhedsprofessionelle ved brugen af visse af sundhedsportalens tjenester, bl.a. ved tilgangen til klinisk information. Af denne grund har der under udarbejdelsen af nærværende rapport været afholdt møder med Amtsrådsforeningen omkring koncept for og indførelse af certifikater til sundhedsprofessionelle. Sundhedsstyrelsen har til disse møder i regi af nærværende projekt udarbejdet to notater, jf. ref. 10 og ref. 11.

2 Problemstillinger og anbefalinger

2.1 Mål og behov vedr. digital signatur i sundhedsvæsenet

Den digitale signatur kan generelt benyttes til at sikre

- autenticitet – af fx personer eller meddelelser
- ægthed og integritet af de af signaturen omfattede data
- uafviselighed – handlinger kan ikke senere benægtes
- fortrolighed omkring data – data kan ikke læses af uvedkommende

Funktioner, der gennemføres, eller data, der sendes af en person, som i forbindelse med funktionen er autentificeret med digital signatur, er med meget høj sandsynlighed ægte og uforfalskede og kan ikke senere afvises af den pågældende.

Endvidere kan informationer, som skal beskyttes mod læsning af uvedkommende, med meget høj sandsynlighed sikres mod uvedkommende ved brug af modtagerens certifikat ved afsendelse eller lagring.

Dette sikkerhedsniveau skabes gennem de procedurer, der omgiver udstedelse og vedligeholdelse af certifikaterne, og af den teknologi, der ligger under brugen af certifikater og digitale signaturer.

Dette afsnit beskriver kort de grundlæggende mål og behov vedr. digital signatur i sundhedsvæsenet. I afsnit 2.2 nedenfor vurderes koncepter for brugen af certifikater i sundhedsvæsenet.

2.1.1 Sikring af autenticitet

Brugen af digital signatur for medarbejdere i sundhedsvæsenet vurderes overvejende at have det mål at sikre medarbejderes ”autenticitet” i forbindelse med deres adgang til og brug af systemer, funktioner og information.

Den digitale signatur vil ud over medarbejderes autenticitet sikre ægthed og uafviselighed af information. Samtidig vil de funktioner, som den enkelte medarbejder udfører i systemerne, være ”signeret”, idet systemerne verificerer medarbejderens autenticitet via det digitale certifikat og registrerer handlinger og tidspunktet i logfiler.

Via verificering af medarbejderens autenticitet, dvs. at medarbejderen er den, som han/hun giver sig ud for at være, vil det være muligt at skabe et grundlag for at sikre, at medarbejdernes roller og adgangsrettigheder på ethvert tidspunkt er i overensstemmelse med det formelt ønskede og korrekte. Det grundlag, som skal sikre dette, er

- dels den digitale signatur,
- og dels information om den enkelte medarbejders rolle, autorisation, stilling og ansættelsessted, ansvar og adgangsrettigheder.

Definitionen af, hvad den enkelte medarbejders rolle og adgangsrettigheder mv. er, er en opgave, som kan sammenfattes under betegnelsen ”brugerstyring”. Brugerstyring beskrives yderligere i afsnit 2.9.

2.1.2 Sikring af fortrolighed

Brug af digitale certifikater til sikring af fortrolighed vurderes ikke generelt at være relevant for den enkelte medarbejder, men udelukkende for systemer og applikationer, således at fortroligheden kan sikres inden for den enkelte afdeling eller institution efter behov. Dette vil kunne ske med server-certifikater og sikkerhedsfaciliteter internt i systemerne og i applikationerne.

Det vil med et sådant koncept være uvedkommende for den enkelte medarbejder, hvorledes information holdes fortrolig internt i systemerne, således at kun de relevante personer får adgang hertil. Fortroligheden kan sikres såvel internt i det enkelte system som ved udveksling af information ved brug af kryptering med certifikater og nøgler, som er udstedt til det enkelte system.

Medarbejderne skal være opmærksomme på, at fortrolig information ikke generelt må trækkes ud af sundhedssystemerne og fx sendes i e-mails. Fortrolig eller følsom information i sundhedsvæsenets systemer bør kun i særlige tilfælde overføres til e-mails, disketter eller andre medier af den enkelte medarbejder. Dette kan være relevant ifm. behov for udveksling af klinisk information i mere administrativ sammenhæng og med eksterne parter i forhold til sundhedsvæsenet, såsom behandling af tværministerielle sager, klagesager og afregning. Medarbejderen vil i disse situationer i højere grad selv være involveret i at opretholde fortroligheden via brug af certifikater og kryptering, fx. af e-mails.

Adgang til sundhedssystemer mellem forskellige lokationer og fra fx hjemme-pc'er vil kunne ske sikkert via VPN (Virtual Private Network) eller via anden form for krypterede forbindelser (SSL-baseret eller tilsvarende).

Det vil til sikringen af fortrolighed være relevant, at der fx i brugerdialogen i systemerne indgår advarsler eller er spærret for visse funktioner, så ikke-autoriseret videregivelse eller kompromittering af fortrolig information undgås. Samtidig vil det være relevant at sikre, at uddannelsen, og herunder IT-uddannelsen, af de forskellige medarbejdergrupper også omfatter uddannelse vedr. fortrolige data i såvel papirform som i elektronisk form.

Styringen af fortroligheden og sikkerheden på systemniveau skal udføres af de IT-ansvarlige med udgangspunkt i brugerstyringen og i de generelle retningslinier for adgang til systemer og information.

2.2 Digitale certifikater i sundhedsvæsenet

2.2.1 Certifikater til sikring af autenticitet

Underskrift af dokumenter udføres af personer i den konkrete rolle, som de fungerer i ved underskriften. Ligeledes får personer i egenskab af deres rolle, herunder deres ansættelse og autorisation, adgang til funktioner, systemer og information mv.

Personer kan have flere roller, såsom job og andre faglige aktiviteter og kvalifikationer, og kan optræde i disse forskellige roller ved underskrift, herunder:

- et eller flere jobs,
- udvalgsarbejde, komiteer mv.,
- faglige foreninger og lign.,
- forskning og uddannelse,
- autoriseret sundhedsperson uden anden tilknytning.

Det certifikat og nøglesæt, der benyttes af en person til underskrift, er logisk set dels knyttet til personen og via den egentlige ansættelsesmyndighed knyttet til den rolle, som personen optræder i ved underskriften. Der vil være behov for, at både identiteten og rollen kan verificeres på et givet tidspunkt (aktuelt eller historisk) for en digital signatur (eller anden handling udført via et certifikats autenticitet).

Det er principielt et valg, hvorvidt certifikater til digital signatur skal være personlige eller ikke. Generelt må det dog vurderes som en fordel, og i visse tilfælde en forudsætning, at en digital signatur, ligesom det er tilfældet for papirbaserede forretningsgange, kan knyttes til en person og ikke (blot) til en virksomhed.

En række koncepter skitseres og vurderes i nedenstående skema.

Koncepter for certifikater til autenticitet / digital signatur	
P	<p>Et (enkelt) personcertifikat til hver person</p> <p>Et personcertifikatet rekvireres af hver enkelt person på eget initiativ, og certifikatet benyttes til signatur af personen i alle sammenhænge i rollen som "sig selv". Der er således hverken nogen specifik rolle eller nogen reference til ansættelse knyttet til certifikatet.</p> <p>Fordele:</p> <ul style="list-style-type: none">▪ Antallet af certifikater pr. person er begrænset til et enkelt.▪ Konceptet ligner umiddelbart de traditionelle fysiske papirgange. <p>Ulemper:</p> <ul style="list-style-type: none">▪ Certifikatet er ikke udstedt til personen i en bestemt rolle eller ifm. en bestemt ansættelse.▪ Konceptet indebærer en sammenblanding af sundhedsmedarbejders privatsfære og deres arbejde, bl.a. overlades certifikatadministration, fornyelse og spærring til privatpersonen.▪ Der skal vedligeholdes en database med oplysninger om ansættelsesforhold / roller.

M1	<p>Et enkelt medarbejdercertifikat til hver enkelt person</p> <p>Hver person modtager ifm. sin ansættelse et medarbejdercertifikat, som benyttes af personen i alle sammenhænge, hvor personen skal underskrive i rollen som ansat i det pågældende job. Personlige autoriseringer mv., som naturligt hører til ansættelsen, kan logisk knyttes til certifikatet og dermed indgå i den rolle, som personen vil benytte certifikatet i.</p> <p>I tilfælde, hvor en person har flere ansættelsesforhold (eller andre roller helt uden relation til ansættelsesforholdet), indebærer dette koncept formentlig, at personen vil få udstedt flere certifikater – ét for hvert ansættelsesforhold.</p> <p>Fordele:</p> <ul style="list-style-type: none"> ▪ Mange medarbejdere har kun behov for et enkelt certifikat (pr. ansættelsesforhold). ▪ Konceptet ligner i nogen grad de traditionelle fysiske papirgange og procedurer. <p>Ulemper:</p> <ul style="list-style-type: none"> ▪ Visse medarbejdere har behov for flere certifikater pga. flere ansættelsesforhold. ▪ Certifikater skal tilbagekaldes ved skift af ansættelsesforhold (på foranledning af den tidligere arbejdsgiver). ▪ Nyt certifikat skal udstedes ved skift af ansættelsesforhold (på foranledning af den nye arbejdsgiver). ▪ Certifikater skal tilbagekaldes og nyt udstedes ved skift af arbejdsopgaver / ansættelsesforhold hos samme arbejdsgiver.
Mn	<p>Et eller flere medarbejdercertifikater til hver enkelt person</p> <p>Hver person modtager ifm. sin ansættelse et medarbejdercertifikat – ligesom i koncept "M1". Endvidere udstedes efter behov yderligere certifikater ifm. eventuelle andre roller (og jobs), som personen bestrider.</p> <p>Fordele:</p> <ul style="list-style-type: none"> ▪ Hvert enkelt certifikat udstedes til en person i en specifik rolle. <p>Ulemper:</p> <ul style="list-style-type: none"> ▪ Mange medarbejdere vil have flere certifikater at holde styr på, og der kan i praksis opstå uklarheder om, hvilket der skal benyttes i en given sammenhæng. ▪ Dyrere og mere besværlig løsning end "M1". ▪ Certifikater skal tilbagekaldes ved rolle- / jobskift. ▪ Nyt certifikat skal udstedes ved påbegyndelse af ny rolle / nyt job.

MS	<p>Et enkelt "sundhedsvæsen"-certifikat til hver enkelt person</p> <p>Hver sundhedsprofessionel modtager sammen med sin autorisation som sundhedsperson et medarbejdercertifikat – ligesom i koncept "M1". Dette certifikat benyttes af medarbejderen i alle sammenhænge i sundhedsvæsenet.</p> <p>Fordele:</p> <ul style="list-style-type: none"> ▪ Konceptet er enkelt såvel at forstå som at håndtere af den enkelte medarbejder. ▪ Behovet for at tilbagekalde gamle og udstede nye certifikater minimeres. ▪ Konceptet ligner de traditionelle fysiske papirgange. ▪ Konceptet er i harmoni med fx autorisationer, som også følger personen uanset ansættelse. <p>Ulemper:</p> <ul style="list-style-type: none"> ▪ Der ligger en måske uønsket centralisering i konceptet. ▪ Autorisation dækker som udgangspunkt ikke alle sundhedsmedarbejdere i dag. ▪ Der skal vedligeholdes en database med oplysninger om ansættelsesforhold / roller.
V	<p>Et virksomhedscertifikat, som kan benyttes af medarbejdere</p> <p>Hver afdeling, organisatorisk enhed og rolle får udstedt et virksomhedscertifikat, som de ansatte benytter ifm. digital signatur i den pågældende afdeling, enhed eller rolle.</p> <p>Fordele:</p> <ul style="list-style-type: none"> ▪ Certifikatet er udelukkende knyttet til virksomheden og kan håndteres helt og holdent af denne. ▪ Certifikatet kan videregives til ny stillingsindehaver. <p>Ulemper:</p> <ul style="list-style-type: none"> ▪ Signaturen kan ikke relateres til en person – sporbarheden, og herunder den personrelaterede uafviselighed, forsvinder. ▪ Certifikatet og den private nøgle skal normalt benyttes af flere og skal derfor forefindes i flere (hardware) kopier, hvilket giver en øget risiko for kompromittering. ▪ Konceptet afviger væsentligt fra den traditionelle underskriftsmodel.

Anbefaling

Det anbefales, at der til digital signatur og sikring af autenticitet i sundhedsvæsenet vælges et koncept baseret på medarbejdercertifikater.

Hver sundhedsperson modtager sammen med sin autorisation som sundhedsprofessionel et medarbejdercertifikat. Dette certifikat benyttes af den pågældende i alle sammenhænge i sundhedsvæsenet.

Certifikatet har form af et medarbejdercertifikat, udstedt på vegne af en myndighed i sundhedsvæsenet. Denne myndighed optræder som en virksomhed, hvortil medarbejderen er knyttet, og hvorfra medarbejderen har sin autorisation. Sundhedsvæsenet opfattes i dette forhold som én virksomhed, mens certifikaterne i nogen udstrækning administreres lokalt.

I første omgang peges således på konceptet "MS" som det foretrukne løsningskoncept for digital signatur – med konceptet "M1" som fall-back løsning. Konceptet MS ligner i nogen grad den traditionelle papirbaserede personlige underskrift, og konceptet giver den enkelhed, som må prioriteres som væsentlig for dels de første pilotprojekter og dels den generelle accept og brug af digitale signaturer.

Konceptet "V" anses for uanvendeligt pga. de nævnte ulemper. "P" anses som uhensigtsmæssigt til formålet pga. de nævnte ulemper. Konceptet "Mn" anses for at være unødigt komplekst i forhold til "M1".

Fordelene ved det anbefalede koncept er, at

- konceptet er enkelt såvel at forstå som at håndtere af den enkelte medarbejder.
- behovet for at tilbagekalde gamle og udstede nye certifikater minimeres ved, at certifikater udstedes efter konceptet "medarbejdercertifikater i sundhedsvæsenet", således at hverken jobskift inden for sundhedsvæsenet eller daglige engagementer på fx flere sygehuse indebærer skift af certifikat.
- konceptet er i nogen grad analogt til de traditionelle fysiske papirgange.
- konceptet er i harmoni med fx autorisationer, som også følger personen uanset ansættelse.
- der vil gradvis opnås en standardisering af roller og rettigheder.

Ulemper ved konceptet er, at

- der ligger en måske uønsket centralisering i konceptet.
- autorisation dækker som udgangspunkt ikke alle sundhedsmedarbejdere i dag.
- der skal vedligeholdes en fælles database med oplysninger om ansættelsesforhold / roller, baseret på en enighed om, hvilke roller der er, og hvordan de repræsenteres.

Sidstnævnte punkt skal dog under alle omstændigheder tilgodeses i en eller anden form, enten lokalt eller som en fælles opgave.

De sundhedsmedarbejdere, som ikke er autoriserede sundhedspersoner, må benytte M1/Mn-konceptet. Disse personalegrupper har kun sjældent flere jobs / roller.

2.2.2 Certifikater til sikring af fortrolighed

Fortrolighed skal kunne sikres ifm. udveksling og lagring af dokumenter og klinisk information. Behovet for fortrolighed er ikke, som det er tilfældet med signaturen, knyttet til den enkelte medarbejder, men derimod til virksomheder, afdelinger og i nogen grad roller. Selvom der er høje krav til fortrolighed omkring information og dokumenter i sundhedsvæsenet, er kravene relateret til fx det enkelte hospital, den enkelte afdeling eller til en lægepraksis. Den enkelte medarbejder har ikke behov for at hemmeligholde information på personligt niveau, idet informationen skal kunne deles med kolleger eller med afdelingen eller ledelsen.

I de tilfælde, hvor en sundhedsprofessionel betros information, som ikke må videregives til andre personer, kan denne information beskyttes enten af systemet via særlige faciliteter hertil eller af den sundhedsprofessionelles nøgler fra dennes certifikat.

Det er, ligesom for den digitale signatur, principielt et valg, hvorvidt de certifikater og nøglesæt, som benyttes til opnåelse af fortrolighed, skal være personlige eller ikke.

En række koncepter skitseres og vurderes i nedenstående skema.

Koncepter for certifikater til opnåelse af fortrolighed	
P	<p>Et (enkelt) personcertifikat til hver person</p> <p>Et personcertifikat (og tilhørende nøglesæt) rekvireres af hver enkelt person på eget initiativ og benyttes af personen til modtagelse og til lagring af fortrolige dokumenter. Certifikatet og nøglesættet, og dermed hemmeligholdelsen, er begrænset til den pågældende person i rollen som "sig selv".</p> <p>Fordele:</p> <ul style="list-style-type: none">▪ Den enkelte person kan selv stå inde for hemmeligholdelsen af den fortrolige information. <p>Ulemper:</p> <ul style="list-style-type: none">▪ Hemmeligholdelsen er knyttet til den enkelte person uafhængigt af denne persons ansættelsesforhold og roller. Dette indebærer formentlig, at dette koncept er uanvendeligt i organisationer, der omfatter mere end én person.▪ Medarbejdere er "tvunget" til at anskaffe sig et personcertifikat og benytte dette ifm. sin ansættelse, hvilket ikke er intentionen med personcertifikater.▪ Konceptet indebærer en sammenblanding af personens rolle som borger og som ansat i sundhedsvæsenet.

M	<p>Et medarbejdercertifikat til hver enkelt person</p> <p>Hver person modtager ifm. sin ansættelse et medarbejdercertifikat, som benyttes af personen til modtagelse og til lagring af fortrolige dokumenter. Certifikatet og nøglesættet, og dermed hemmeligholdelsen, er begrænset til den pågældende person i sit ansættelsesforhold.</p> <p>I tilfælde, hvor en person har flere ansættelsesforhold (eller andre roller helt uden relation til ansættelsesforholdet), indebærer dette koncept, ligesom med signaturen, formentlig, at personen vil få udstedt flere certifikater – ét for hvert ansættelsesforhold.</p> <p>Fordele:</p> <ul style="list-style-type: none"> ▪ Den enkelte person kan selv stå inde for hemmeligholdelsen af den fortrolige information. ▪ Hvert enkelt certifikat udstedes til en person i et specifikt ansættelsesforhold. <p>Ulemper:</p> <ul style="list-style-type: none"> ▪ Ved medarbejderudskiftning kræves procedurer, som sikrer, at medarbejderens fortrolige dokumenter kan læses af andre på afdelingen. ▪ Deling af fortrolig information fx mellem kolleger og på en afdeling er besværlig. ▪ Visse medarbejdere har behov for flere certifikater pga. flere ansættelsesforhold. ▪ Certifikater skal tilbagekaldes ved skift af ansættelsesforhold (på foranledning af den tidligere arbejdsgiver). ▪ Nyt certifikat skal udstedes ved skift af ansættelsesforhold (på foranledning af den nye arbejdsgiver). ▪ Certifikater skal tilbagekaldes og nyt udstedes ved skift af arbejdsopgaver / ansættelsesforhold hos samme arbejdsgiver.
V	<p>Et virksomhedscertifikat, som kan benyttes af medarbejdere</p> <p>Hver afdeling, organisatorisk enhed og eventuelt rolle får udstedt et virksomhedscertifikat med tilhørende nøglesæt, som de ansatte benytter til modtagelse og til lagring af fortrolige dokumenter.</p> <p>Fordele:</p> <ul style="list-style-type: none"> ▪ Dette koncept sikrer, at den fortrolige information er tilgængelig i den enhed el.lign., som formelt har adgang til informationen - uafhængigt af personudskiftning. ▪ Certifikatet er udelukkende knyttet til virksomheden og kan håndteres helt og holdent af denne. ▪ Konceptet svarer til de fysiske arbejdsgange i dag, hvor fortrolige dokumenter og informationer opbevares i afdelingsregi og lign. <p>Ulemper:</p> <ul style="list-style-type: none"> ▪ Brud på fortrolighed kan ikke (via certifikatet) relateres til en person. ▪ Nøglesættet skal benyttes af flere og skal derfor forefindes i flere (hardware) kopier. Dette sænker sikkerhedsniveauet.

S	<p>Et server- / applikationscertifikat, som håndteres på systemniveau</p> <p>Til hver server, applikation eller system, som skal hemmeligholde data, anskaffes et server-certifikat. Dette certifikat benyttes ved enten kommunikation (fx med SSL) eller ved lagring af data. Brugere er ikke involveret i brugen af dette certifikat, men tilgår udelukkende data via de relevante applikationer (med relevant adgangskontrol fx via digital signatur). Data må ikke udveksles og lagres uden for det sikre miljø (trusted domain) uden at være krypteret. Tilgang fra fx distance-arbejdspladser kan ske via VPN.</p> <p>Fordele:</p> <ul style="list-style-type: none"> ▪ Medarbejderne er ikke selv involveret rent teknisk i brugen af hemmeligholdelsesfaciliteter og certifikater. Certifikaterne kan håndteres af IT-afdelingen. ▪ Hemmeligholdelsen af fortrolige data afhænger i mindre grad af manuelle rutiner. ▪ Konceptet sikrer, at den fortrolige information er tilgængelig for præcis de medarbejdere, som er defineret at have adgang via de relevante applikationer. ▪ Konceptet svarer til de fysiske arbejdsgange i dag, hvor fortrolige dokumenter og informationer opbevares i afdelingsregi og lign. <p>Ulemper:</p> <ul style="list-style-type: none"> ▪ Det skal sikres, at applikationerne udvikles og drives, således at data ikke i de daglige arbejdsgange forlader det sikre miljø, samt at dette koncept er gennemgående for alle fortrolige data.
---	--

Anbefaling

I første omgang peges på konceptet ”S” som det foretrukne løsningskoncept for opnåelse af fortrolighed – med konceptet ”V” som fall-back løsning. Konceptet ”S” er på mange måder analogt til traditionelle fysiske og papirbaserede forhold. Endvidere kan konceptet medvirke til at sikre, at adgang til fortrolig information og procedurer omkring fortrolighed er uafhængig af medarbejdernes tekniske færdigheder og viden.

Konceptet ”P” anses for uanvendeligt, idet dette ville indebære, at hemmeligholdelse er knyttet til den enkelte person uafhængigt af dennes ansættelsesforhold og roller. Konceptet ”M” er i praksis mere proceduretungt og besværligt at bruge end ”V”.

Der kan i praksis være behov for flere måder at sikre fortrolighed på. I nogle tilfælde vil det, jf. afsnit 2.1.2, være relevant at udveksle klinisk information af fortrolig karakter fx via e-mails til andre myndigheder. Brugen af et medarbejdercertifikat eller en kombination af koncepterne V og M som supplement til ovenstående løsning vil således kunne være relevant for nogle sundhedsprofessionelle.

Faciliteter til at beskytte information, som den enkelte sundhedsprofessionelle er blevet betroet personligt under tavshedspligt, bør indgå i sundhedssystemerne. Sådan information kan eventuelt beskyttes af den sundhedsprofessionelles nøgler fra dennes certifikat.

2.3 Software- vs. hardware-certifikater

Der findes forskellige modeller for, hvorledes brugeren modtager og opbevarer sit certifikat og sine private nøgler ifm. brugen af digital signatur.

Certifikat og nøgler kan enten installeres på brugerens pc i form af filer (med tilhørende software til læsning og beskyttelse), eller de kan installeres på en hardware-token ("hw-token"), fx et chipkort eller en USB-token. En hw-token med certifikat og nøgler kan bæres af brugeren og benyttes på alle pc'er, som understøtter den pågældende type af hw-token og den anvendte type certifikat og nøgler.

For både software- og hardware-certifikater gælder, at brugen af certifikatet og nøglerne er beskyttet af en PIN-kode, som afkræves brugeren ved brug. Denne sikkerhed er lagt i det software, som giver adgang til og benytter certifikatet og nøglerne. Som et principielt alternativ til PIN-kode kunne biometrisk identifikation såsom fingeraftryk benyttes. Dette vil dog forudsætte, at de benyttede pc'er er udstyret med faciliteter til understøttelse af den valgte biometri.

Brugen af certifikater – såvel software-certifikater som hardware-certifikater – er i vid udstrækning en standardfacilitet i pc-software til web-tjenester i dag. Således er Microsoft Windows-pc'er (Windows 2000 eller Windows XP) og Microsoft Internet Explorer (version 6 eller senere) på klientsiden udstyret med faciliteter til understøttelse af både hardware- og software-certifikater, jf. bilag C.1 – dog kræves i de fleste tilfælde supplerende software fra leverandøren af certifikat-løsningen.

Software-certifikater kendes fra fx hjemmebank-systemer og VPN-løsninger, mens hardware-certifikater fx benyttes i visse adgangskontrolsystemer, hvor der er krav om stærk sikkerhed, og i de fremtidige chipkort-baserede betalingskort.

Mange arbejdspladser i sundhedsvæsenet, herunder på hospitaler og i klinikker, er karakteriseret ved, at medarbejderne ikke sidder ved den samme pc dagen igennem. På hospitaler er det ofte situationen, at læger og sygeplejersker i deres daglige arbejde er logget på ganske kort op til 30 gange på forskellige pc'er, afhængigt af hvor arbejdet foregår. Også praktiserende læger bruger ofte flere pc'er i deres daglige arbejde. Sundhedsprofessionelle er således "roaming" brugere mht. pc'er, dvs. brugere, som flytter rundt fra pc til pc og har behov for at flytte profil og rettigheder med til de forskellige pc'er.

Selvom et software-certifikat teknisk set godt kan installeres på flere pc'er, vil det i praksis dels være en relativt omfattende opgave løbende at installere hvert eneste medarbejdercertifikat på et stort antal pc'er og dels indebære en potentiel sikkerhedsrisiko, at disse certifikater (med tilhørende nøgler) forekommer i stort tal og måske ikke bliver fjernet, som de bør, når medarbejderen fratræder.

Som et alternativ kunne der teknisk set etableres software-baseret roaming, enten med certifikater placeret på en roaming-server eller med et koncept med tynde klienter (Citrix / Windows Terminal Server) med certifikater placeret på netværksserver. Sikkerheden i sådanne software-roaming-modeller er imidlertid ikke tilstrækkelig – basalt set reduceres autentificeringen til kendskabet til PIN-koden.

Brugen af hardware-baserede certifikater, dvs. med den ovenfor benyttede terminologi en ”hardware-roaming”-model, er af disse grunde det mest hensigtsmæssige i store dele af sundhedsvæsenet.

Anbefaling

Det anbefales at basere sundhedsvæsenets koncept for digitale signaturer på hardware-certifikater med brug af en egnet form for hw-token. Alternativt kan software-certifikater anvendes hvor dette understøtter arbejdsgangene i sundhedsvæsenet. Brugen af software-certifikater kan indebære en relativt omfattende arbejdsbyrde ved installation og afinstallation på et stort antal pc’ere. Desuden indebærer det en potentiel sikkerhedsrisiko pga. den omfattende kopiering og administration af certifikater og nøgler. Endvidere anses software-roaming for sikkerhedsmæssigt utilstrækkeligt.

2.3.1 Alternative hw-tokens

Det skal vurderes, hvilken form for hw-token der er mest egnet til brug i sundhedsvæsenet. Der er flere alternativer til valget af teknologi - først og fremmest følgende:

- USB-token
- chipkort
- trådløse chips (fx chipkort, badges eller lign.)

Fordele og ulemper ved disse alternativer er sammenfattet i skemaet nedenfor.

HW-token	Fordele	Ulemper
USB-token	<ul style="list-style-type: none"> ▪ USB-porte findes på alle moderne pc’er ▪ Indgår i TDC’s løsninger til OCES-konceptet 	<ul style="list-style-type: none"> ▪ Pc’er bør udstyres med USB-hub på desktop ▪ Kræver to-hånds betjening ▪ Antages at have dårlig mekanisk holdbarhed
Chipkort	<ul style="list-style-type: none"> ▪ Er generelt understøttet på markedet som hw-token ifm. digital signatur ▪ Nem (og velkendt) betjening for brugerne ▪ Vil (fra 2004) indgå i TDC’s løsninger til OCES-konceptet 	<ul style="list-style-type: none"> ▪ Pc’er skal udstyres med chipkortlæser
Trådløs teknologi	<ul style="list-style-type: none"> ▪ Er betjeningsfri, dvs. brugeren skal blot befinde sig i nærheden af pc’en ▪ Brugeren ”logges ud”, når han/hun forlader pc’en 	<ul style="list-style-type: none"> ▪ Brugeren risikerer, at hw-token læses (og derved uvidende at logge på excl. PIN), blot han/hun er tæt på en pc ▪ Brugeren ”logges ud”, hvis han/hun bevæger sig blot et par meter fra pc’en

Anbefaling

Det vurderes, at chipkort umiddelbart er den mest egnede form for hw-token til brug for certifikater i sundhedsvæsenet. Det anbefales at søge dette verificeret, fx gennem eksperimenter eller pilotforsøg.

2.4 Brugen af OCES-certifikater

I 2003 lancerede Ministeriet for Videnskab, Teknologi og Udvikling det nationale OCES-koncept – ”Offentlige Certifikater til Elektronisk Service” (ref. 1).

Brugen af OCES-certifikater er undersøgt nøje, dels fordi det fra regeringens side forventes, at OCES-certifikater skal kunne benyttes i offentligt regi, og dels fordi det vurderes at være en bekostelig affære at indføre og vedligeholde et ’nyt’ offentligt certifikat til brug i sundhedsvæsenet.

OCES-konceptet omfatter tre typer af certifikater: personcertifikater, medarbejdercertifikater og virksomhedscertifikater.

OCES er introduceret som et software-baseret certifikat. Dette vil kunne benyttes på de arbejdspladser, hvor medarbejderen har sin egen pc. Dette er imidlertid ikke tilfældet på et sygehus, hvor mange deles om de samme pc’er på en afdeling, og hvor mange sundhedsprofessionelle, fx læger, i dagens løb skal kunne benytte pc’er, der er placeret forskellige steder. I disse situationer betragtes et hardware-baseret certifikat som den mest realistiske mulighed, jf. afsnit 2.3.

OCES-certifikater forventes dog allerede fra 2004 at kunne benyttes på hw-tokens, og det er erfaret, at der allerede er flere pilotprojekter, der afprøver hardware-baserede OCES-certifikater (med brug af USB-token). Afprøvning af chipkort-løsninger er ligeledes under overvejelse, og en teknologisk løsning vil være enkel at implementere.

Anbefaling

Det anbefales at benytte OCES-medarbejdercertifikater i det i afsnit 2.2 anbefalede koncept, og det vurderes, at OCES-medarbejdercertifikater giver den tilstrækkelige funktionalitet, såfremt:

- der bliver mulighed for understøttelse af chipkort-baserede OCES-certifikater,
- der bliver mulighed for medarbejderidentifikation med CPR-nummer i tilknytning til udstedelse af certifikater².

Der har ifm. nærværende analysearbejde været afholdt møde med TDC, som har meddelt, at muligheden for understøttelse af chipkort til brug for OCES-certifikater

² Dette kræver medarbejderens udtrykkelige samtykke i henhold til udtalelse fra Datatilsynet, som er afgivet i dialog med IT&Telestyrelsen omkring OCES-medarbejdercertifikater. I forbindelse med certifikatudstedelsen skal dette samtykke således indhentes fra medarbejderen som en forudsætning for tilknytningen til CPR-nummeret. CPR-nummer benyttes rutinemæssigt ved udstedelsen af sundhedsfaglige autorisationer.

er nært forestående. Endvidere har TDC oplyst, at de vedligeholder CPR-numre i en beskyttet database.

2.5 Information i certifikater

Indholdet i et certifikat er (bevidst) meget begrænset og tjener i princippet kun det formål

- at identificere certifikatholderen entydigt (person og/eller virksomhed afhængig af certifikattypen),
- at vise certifikatholderens offentlige nøgle(r),
- at dokumentere, at certifikatet er udstedt af en CA.

Ud over disse basale certifikatinformationer indgår der også udløbsdato og nogle tekniske informationer om certifikatet og nøglerne. Der er endvidere mulighed for at lægge en begrænset mængde yderligere information i certifikatet, fx for medarbejdercertifikater medarbejderens stillings- og afdelingsbetegnelse.

Det kan vurderes, hvorvidt det er hensigtsmæssigt at lægge information i certifikaterne ud over den strengt nødvendige og krævede information. Følgende omstændigheder taler for at begrænse informationen i et certifikat mest muligt:

- Et certifikat og informationen heri er offentligt tilgængeligt og skal benyttes i enhver sammenhæng, hvor en digital signatur skal verificeres.
- Jo mere information, der ligger i et certifikat, jo hyppigere vil der være behov for at udskifte certifikatet, idet fx stillings- og afdelingsbetegnelser må forventes at ændres jævnligt.

Fordelen ved at have mere information i et certifikat end det strengt nødvendige kunne være, at det fx såvel på anvendelsestidspunktet som for arkiverede (historiske) certifikater direkte vil fremgå, hvilken stilling og afdeling certifikatholderen er tilknyttet. Principielt kunne man forestille sig, at certifikatet indeholdt den fuldt tilstrækkelige information om, hvilke systemer og informationer mv. certifikatholderen har adgang til. Dette er dog dels ikke tilsigtet med den begrænsede information, som er tiltænkt at ligge i et certifikat, og dels uhensigtsmæssigt pga. sundhedsprofessionelles hyppige ændringer i ansættelsesforhold mv., hvilket ville føre til hyppige udskiftninger af certifikater.

Et principielt alternativ er et benytte en særlig form for certifikater – attributcertifikater, som kan tilknyttes medarbejdercertifikatet og indeholde supplerende information om medarbejderen. Dette koncept indgår dog ikke i det nationale OCES-koncept, og det vil indebære både en mere kompleks certifikatmodel og en mere kompleks brugerstyring, herunder mere ressourcekrævende administrative procedurer ifm. ændringer i medarbejderes roller og adgangsrettigheder.

Der er således som supplement til informationen i et certifikat behov for at etablere brugerstyring i et ”bruger katalog”, hvor den enkelte medarbejders roller, beføjelser og adgangsrettigheder mv. registreres og vedligeholdes. Dette omtales i afsnit 2.9.

Anbefaling

Informationen i certifikater, som benyttes til digital signatur og autenticitet for medarbejdere i sundhedsvæsenet, skal begrænses til den minimale, nødvendige information til identifikation af medarbejderen.

Det forventes, at der kun er behov for ét certifikat (med 1 – 2 nøglesæt) til hver bruger. På et chipkort kan der i dag være 5 – 10 certifikater, men der er ikke indikationer for, at der er behov for denne kapacitet til de anvendelser, der skitseres i denne rapport.

Det har været overvejet, om medarbejdercertifikater skal indeholde separate nøglesæt til signatur (herunder sign-on med angivelse af PIN-kode) og til almindelig sign-on (uden angivelse af PIN-kode) til diverse IT-systemer. En sådan løsning ville give en enkel almindelig sign-on, da den alene baseres på en hw-token. Sikkerheden vil imidlertid være meget ringe i forhold til de sikkerhedsfordele, der kan opnås ved brug af sign-on med angivelse af PIN-kode. I øvrigt vurderes det, at flere og flere systemer i fremtiden vil kræve sikker identifikation af brugeren i form af stærk autentificering.

2.6 Identifikation af virksomhederne i sundhedsvæsenet

Virksomheder skal identificeres i medarbejdercertifikater (og i virksomhedscertifikater) på en entydig måde. OCES-konceptet lægger op til, at CVR-numre bruges til denne identifikation.

I den anbefalede model ”MS” (jf. afsnit 2.2.1), hvor medarbejdercertifikater udstedes af ”sundhedsvæsenet”, er der ikke i certifikaterne behov for en entydig virksomhedsidentifikation, men blot en identifikation af ”sundhedsvæsenet”. Der vil dog i såvel denne som i de øvrige modeller være behov for, at man i brugerkataloget identificerer ansættelsesstederne i relation til medarbejdere og certifikater.

CVR-nummersystemet er skabt til håndtering af økonomiske forhold vedr. virksomheder (handel, regnskaber m.v.). Dette system kan derfor på et senere tidspunkt let komme i konflikt med de behov, som opstår i relation til kommunikation af klinisk information. Sådanne konceptuelt forskellige formål bør principielt aldrig sammenblandes. En foreløbig undersøgelse viser endvidere, at brugen af CVR-numre er meget heterogen i sundhedsvæsenet. CVR-numre kan alene af denne grund ikke benyttes i brugerkataloget som identifikation af virksomhed (dvs. den enkelte medarbejders ansættelsessted).

Alternativt kan en kombination af sygehus- / afdelingsklassifikationen og partnerskabstabellen benyttes. Sygehus- / afdelingsklassifikationen og partnerskabstabellen er skabt til håndtering af klinisk information. Derfor er det grundlæggende mere hensigtsmæssigt, at disse benyttes til adgangsstyring til sundhedsvæsenets IT-systemer. Foreløbige undersøgelser viser, at partnerskabstabellens lokationsnumre let kan bruges til at dække det samlede behov for identifikation af organisatoriske enheder.

Anbefaling

Ved udstedelse af medarbejdercertifikater i sundhedsvæsenet skal benyttes en virksomhedsidentifikation, som entydigt identificerer "sundhedsvæsenet" som den virksomhed, hvortil medarbejderen er knyttet.

Anbefaling

En "virksomhedsidentifikationsmodel" skal udarbejdes på grundlag af sygehus- / afdelingsklassifikationen og partnerskabstabellen, således at alle ansættelsessteder i sundhedsvæsenet kan identificeres entydigt i et brugerkatalog (og i andre sammenhænge).

2.7 Identifikation af medarbejderne i sundhedsvæsenet

Det skal besluttes, hvorledes den enkelte sundhedsprofessionelle identificeres som "medarbejder" i forbindelse med udstedelse af et medarbejdercertifikat. Dels skal medarbejderen identificeres som person, og dels skal medarbejderen identificeres entydigt i medarbejdercertifikatet i forhold til den "udstedende virksomhed", dvs. i sundhedsvæsenet.

De mest almindelige former for medarbejderidentifikation ved ansættelser er identifikationer såsom:

- Medarbejderens (fulde) navn
- Initialer eller bruger-id
- Lønnummer
- Personnummer (CPR-nummer)

Alle ovennævnte medarbejderidentifikatorer, bortset fra navnet, er normalt entydige til et bestemt tidspunkt inden for rammerne af en mindre virksomhed. Ses derimod på hele sundhedsvæsenet, er det af disse identifikatorer kun CPR-nummeret, der kan forventes at være entydigt (og formatmæssigt kompatibelt) på tværs af alle ansættelsessteder.

CPR-numre skal imidlertid ikke indgå i certifikater, da informationen i certifikater er offentligt tilgængelig³. Der er derfor behov for at etablere en yderligere medarbejderidentifikation, som benyttes i certifikater, og som i et brugerkatalog el.lign. kan knyttes entydigt til den enkelte medarbejder.

En sådan medarbejderidentifikation kan for sundhedsprofessionelle baseres på den sundhedsfaglige autorisation – på autorisations-ID. Dette vil dog ikke kunne dække alle sundhedsprofessionelle, idet bl.a. lægesekretærer ikke har autorisation, hvorfor denne identifikation vil kræve, at autorisations-ID-systemet udvides til at omfatte også disse grupper.

³ TDC vil i OCES-konceptet understøtte, at CPR-numre registreres i tilknytning til udstedte medarbejdercertifikater på sikker måde, således at CPR-numrene ikke kan rekvireres af uvedkommende og til uvedkommende formål. Samme princip gælder i øvrigt for OCES-personcertifikater.

Ved opnåelse af autorisation foretages allerede i dag den for certifikatet krævede identifikation og sikring af medarbejderens identitet. Der er ikke krav om fremmøde ved udstedelse af sundhedsfaglig autorisation, men da OCES-certifikater ikke er kvalificerede certifikater, er der heller ikke krav om fremmøde ved udstedelse af disse. Autorisationssystemet kan derfor direkte bruges som grundlag for udstedelsen af OCES-certifikater for autoriserede sundhedspersoner.

Anbefaling

Der skal besluttes og defineres en entydig medarbejderidentifikation for sundhedsprofessionelle til brug for medarbejdercertifikater. Det anbefales, at sundhedspersonens autorisations-ID bruges som identifikation, og at autorisations-ID-systemet udvides til at omfatte også de sundhedsprofessionelle, som ikke i dag har autorisation, såsom lægesekretærer og SoSu-assistenten.

Det anbefales endvidere at samarbejde med TDC med henblik på at benytte autorisations-ID som medarbejderidentifikation i OCES-certifikater.

Det er essentielt, at der sikres en entydig og standardiseret medarbejderidentifikation, som kan benyttes i alle sammenhænge, herunder også i Sundhedsportalen. Alternativt vil det være nødvendigt at definere og etablere mapnings-tjenester, så identifikation af medarbejdere og deres roller og rettigheder mv. kan kommunikeres på tværs af systemerne. Sådanne mapnings-tjenester vil imidlertid være fordyrende og vil i praksis indebære sikkerhedsmæssige risici.

2.8 Administration og procedurer omkring certifikater

2.8.1 De administrative roller

Udstedelse og administration af certifikater sker i et samspil mellem en CA ("Certification Authority") og lokale administrative funktioner, der optræder i rollen som RA / LRA (Local Registration Authority). For OCES-certifikater optræder TDC og EuroTrust PKI Services i rollen som CA.

De primære opgaver for en CA og for RA / LRA'er er følgende:

- En CA er en identificeret og betroet part, som udsteder og administrerer certifikater. CA'en står, via sin egen digitale signatur, som garant for, at certifikater er ægte og sørger for at sætte certifikater på en spærreliste (CRL – "Certificate Revocation List"), hvis de er blevet kompromitteret, fx i tilfælde af tab / tyveri af de(n) tilhørende hemmelige nøgle(r). CA'en stiller endvidere de nødvendige tjenester for brugen og vedligeholdelsen af certifikaterne til rådighed, herunder katalogtjeneste og spærrelister.
- En RA / LRA har ansvaret for at verificere identiteten af en medarbejder forud for udstedelsen af et certifikat til vedkommende, samt for at sikre at kommunikationen med CA'en og udstedelsen sker korrekt og iht. kravene vedr. certifikatpolitik og -procedurer (CP og CPS).

I denne rapport vil termen "LRA" blive benyttet i stedet for "RA / LRA" for at fremhæve, at der er tale om funktioner, som i en vis udstrækning (kan) udføres lokalt. Ansvar og opgaver er uddybet i de følgende afsnit 2.8.2 (CA) og 2.8.3 (LRA).

2.8.2 CA's rolle, opgaver og ansvar

En CA

- definerer en certifikatpolitik (CP) og procedurer (CPS)
- udsteder og administrerer certifikater
- registrerer brugere og deres offentlige nøgler
- sikrer at certifikater er (offentligt) tilgængelige
- sikrer eventuel back-up af private nøgler (hvis ønsket – kun relevant for nøgler, der benyttes til at skabe fortrolighed)
- distribuerer spærrelister (CRL)
- varetager eventuel krydscertificering med andre CA'er
- gemmer historisk information om certifikater.

En CA kan være enten offentlig eller privat. En virksomhed har mulighed for at etablere sin egen CA, hvis dette ønskes. Pga. bl.a. de formelle krav til sikkerhed og procedurer er det dog en ressourcekrævende opgave at etablere og drive en CA. Det vil derfor normalt være en fordel at benytte en eksisterende (ekstern) CA, såfremt den tjeneste, der tilbydes, vurderes at være tilstrækkelig og har et acceptabelt prisniveau.

Brugen af en CA vil sikre kompatibilitet med andre certifikatbrugere af samme CA og af CA'er, som er krydscertificeret med den valgte CA.

For OCES-konceptet varetager TDC opgaven som CA i opdrag fra Ministeriet for Videnskab, Teknologi og Udvikling (VTU), jf. ref. 1, 2 og 3. Endvidere fungerer EuroTrust PKI Services som CA for OCES.

2.8.3 LRA's rolle, opgaver og ansvar

En LRA agerer i rollen som "forlænget arm" for CA'en og

- har ansvar for medarbejderidentifikation og forestår al kontakt med medarbejderne
- foranlediger generering af certifikat og nøgler, samt udleverer dette til certifikatholderen og sikrer registrering af certifikatet i CA'en
- fornyer certifikater
- spærrer certifikater, når behov
- varetager kommunikation med CA'en
- fører den relevante logning af de udførte funktioner.

I OCES-konceptet opererer TDC med flere typer af LRA og LRA-tjenester, men størrelsen og kompleksiteten af sundhedsvæsenet peger på, at "LRA Professionel" (den mest omfattende) vil være den mest hensigtsmæssige at benytte.

LRA Professional henvender sig først og fremmest til større organisationer, der ønsker at bruge digitale certifikater som en aktiv del af organisationen. Med LRA Professional kan der i samme organisation være udpeget flere LRA-administratorer, som kan arbejde parallelt og hierarkisk og har automatiske "logbøger". LRA Professional giver mulighed for selv at styre processerne omkring certifikaterne. TDC yder support til administratoren af LRA Professionel.

LRA-administratorer har under OCES-konceptet bl.a. adgang til følgende tjenester:

- Oprettelse af brugere, der skal have certifikat
- Inddeling af brugere i grupper
- Fremsendelse af e-mail og PIN-kode til brugere
- Spærring af certifikater
- Føring af bruger-logbog.

Et eksempel på, hvorledes en LRA-administrators web-adgang til certifikat-administration via CA'ens tjeneste kunne se ud, kan ses i Bilag D.

Anbefaling

TDC's LRA Professional for OCES vurderes at være det relevante valg af LRA-tjeneste for sundhedsvæsenet. Det anbefales at indgå i en dialog med TDC om sundhedsvæsenets behov for administration af certifikater, således at de konkrete procedurer, som skal udføres af LRA-administratorerne i sundhedsvæsenet, kan drøftes og fastlægges i et samarbejde.

2.8.4 Fornyelse af certifikater

Alle certifikater har en udløbsdato – for OCES-certifikaters vedkommende er udløbsdatoen sat til 2 år efter udstedelsen. Dette betyder, at der som en del af de regelmæssige procedurer skal etableres en procedure for fornyelse af et certifikat. Fornyelse af et certifikat indebærer udstedelse af et nyt certifikat med det samme navn og samme information som i det gamle certifikat, men med nye nøgler, ny gyldighedsperiode og et nyt certifikat-serienummer.

Det er relevant at sikre, at certifikatindehaveren – og derigennem certifikatholderen – i passende tid før udløb gøres opmærksom på, at certifikatet udløber. I OCES gælder (jf. OCES CP for medarbejdercertifikater), at CA senest 14 dage før udløb skal notificere certifikatindehaveren via e-post til ”den i certifikatet angivne e-postadresse eller til CVR-postadressen”. Den videre aktion er så op til certifikatindehaveren.

En præcis procedure for fornyelse skal besluttes og aftales med TDC.

2.8.5 LRA organisationen i sundhedsvæsenet

Varetagelsen af sundhedsvæsenets LRA-funktioner og de konkrete behov vedr. LRA-tjenesten tager udgangspunkt i det valgte koncept og i ovennævnte LRA-opgaver. Det i denne rapport anbefalede koncept indebærer en fordeling af LRA-opgaverne efter følgende princip:

Fælles LRA-funktion for sundhedsvæsenet:

- Håndterer kontakten med og indestår for identifikation af sundhedsprofessionelle (ifm. autorisering til IT-systemer)
- Foranlediger generering af certifikat og nøgler og udleverer hw-token til sundhedsprofessionelle (ifm. autorisering til IT-systemer)
- Fornyer certifikater og hw-tokens
- Kan spærre certifikater, når behov
- Varetager den administrative relation til CA'en (TDC)
- Fastlægger rammer for certifikater, LRA'er og procedurer

Lokale LRA'er / personalekontorer og (uden for kontortid) andre enheder / funktioner:

- Kan spærre certifikater, når behov
- Kan generere og udlevere midlertidige certifikater og hw-tokens, fx til brug i et døgn i tilfælde af bortkomst eller tekniske fejl på eksisterende hw-token mv.
- Kan generere nyt password / PIN-kode til hw-token (v. glemt password)

Følgende er en skitse til de konkrete LRA'er, der skal defineres i sundhedsvæsenet, baseret på det anbefalede koncept.

Fælles LRA-funktion for sundhedsvæsenet:

- Sundhedsstyrelsen.

Lokale LRA'er:

- Sygehusejere - lokal LRA for sundhedsprofessionelle på sygehusene, fx på sygehusets personalekontor.
- Sygesikringen i hvert amt/kommune - lokal LRA for sundhedsprofessionelle ved amts/kommunens praktiserende læger, speciallæger, laboratorier, klinikker og lægevagten.
- Kommunen - lokal LRA for hjemmeplejen, fx kommunens social- og sundhedsforvaltning.
- Lokal LRA, som kan fungere uden for kontortid, kan placeres i en institution med døgnåbent, fx skadestue eller vagtrum.

2.9 Brugerstyring og brugerkatalog

2.9.1 Et fælles brugerkatalog

Et fælles brugerkatalog i sundhedsvæsenet er, som omtalt enkelte steder tidligere, nødvendigt for at kunne definere og repræsentere de sundhedsprofessionelle, deres rolle og de rettigheder, den enkelte har ifm. adgang til systemer og information.

Denne "brugerstyring" er på den ene side en selvstændig og uafhængig opgave, som skal varetages af de instanser, der har med adgang til klinisk information at gøre, og på den anden side knyttet sammen med certifikaterne og deres administration, jf. afsnit 2.8 ovenfor, idet brugerstyringen baseres på brugeridentiteten repræsenteret via et certifikat. Behovet for et fælles brugerkatalog er ikke direkte en følge af brugen af certifikater og digital signatur. Et fælles brugerkatalog kunne også være relevant for andre og mere traditionelle former for autentificering såsom user-id og password, men det fælles brugerkatalog er et vigtigt led i opnåelsen af nogle af de fordele, som certifikaterne åbner mulighed for, herunder single-sign on og en stærkere autentificering for adgangen til klinisk information og fælles systemer på tværs af hele sundhedsvæsenet.

Baggrunden for, at der er behov for et brugerkatalog ved siden af certifikatadministrationen og den information, der ligger i selve certifikaterne (jf. afsnit 2.5), er

- at det er både administrativt og teknisk mere ressourcekrævende at vedligeholde supplerende informationer, herunder roller og rettigheder, i certifikater end i et fælles brugerkatalog,
- at undgå hyppige udskiftninger af certifikater pga. de sundhedsprofessionelles hyppige ændringer i ansættelsesforhold og tilknytning til flere arbejdssteder mv.

Brugerstyring sker allerede i eksisterende systemer i dag lokalt hos de enkelte systemansvarlige og på personalekontorer og ansættelsessteder. Med indførelsen af digitale signaturer i sundhedsvæsenet er der behov for at skabe en fælles platform for brugerstyring, således at verifikation af identitet og rettigheder og (historisk) kontrol kan ske på tværs af hele sundhedsvæsenet via digitale medier.

Sundhedsstyrelsen / MedCom har sammen med Oracle gennemført en analyse af etableringen af et lignende brugerkatalog ("Sundhedsstyrelsen / MedCom, Foranalyse til pilotprojekt til etablering af centralt brugerkatalog", ref. 4). Det antages, at resultaterne fra dette arbejde i et vist omfang kan benyttes som grundlag for et sådant brugerkatalog.

2.9.2 Informationen i brugerkataloget

Ifm. brugerstyringen vil alle sundhedsprofessionelle blive repræsenteret og få adgangsrettigheder via tre principielle parametre:

- Identifikation
- Rettigheder
- Personalisering.

Identifikationen tilknytter en identitet (samt andre informationer) til en given bruger. Identifikationen vil normalt være et certifikat, men man kan potentielt gøre identifikationen svagere (fx brugerid, password) eller stærkere (fx tvunget password tilknyttet certifikat eller hw-token).

Rettighederne vil være de ressourcer – systemer og data mv. – som denne bruger (identitet) kan tilgå på det aktuelle tidspunkt.

Personalisering er de aktuelle "profiler", der tilknyttes brugeren (identiteten), fx et tidspunkt ("rettigheden gælder fra kl. 7.00 til 16.00").

Konkret information for hver identitet vil omfatte:

- Entydig identifikation
- Certifikat
- Rolle
- Autorisation(er)
- Sundhedsprofession
- Ansættelse
- Rettigheder / adgang for de enkelte systemer (lokale og centrale)

Der henvises til ovennævnte Sundhedsstyrelsen / MedCom-rapport (ref. 4) vedrørende format af brugerkataloget med den tilføjelse, at der skal repræsenteres generiske roller og ikke ”reelle” roller. Disse generiske roller skal fastlægges i en standardiseringsproces i sundhedsvæsenet, således at enhver sundhedsprofessionel kan indplaceres heri.

Det er op til den enkelte virksomhed at mappe de generiske roller i brugerkataloget til reelle roller ud fra de faktisk gældende forhold på den enkelte virksomhed. Konsekvensen er, at visse informationer i det fælles brugerkatalog, fx rettigheder / adgang, kan være mere eller mindre relevant for forskellige virksomheder.

Mht. definitionen af brugeradgangsrettigheder må det forventes, at en del af rettighederne vil have form af ”regler”. Fx vil en sundhedsmedarbejder på en sygehusafdeling have adgang til information om de patienter, der er under behandling på den pågældende afdeling – udtrykt i form af en regel.

Det må endvidere forventes, at brugeradgangsrettigheder defineres som summen af de rettigheder, der er tildelt dels ved autorisationen og dels ved den eller de ansættelser, som den enkelte har på et givet tidspunkt. Ved fratrædelse af en stilling skal den pågældendes brugerrettigheder justeres, så de ved ansættelsen tildelte rettigheder annulleres. Tilsvarende vil de rettigheder, der er tildelt ved udstedelsen af autorisationen af en sundhedsperson være gældende lige så længe den pågældende har autorisation.

Der vil være behov for historik på brugerkataloget, således at roller og rettigheder mv. kan fremfindes for et givet tidspunkt og en given bruger og sag.

2.9.3 Administration af brugerkataloget

Vedligeholdelse af det fælles brugerkatalog er en løbende driftsopgave, som kræver koordinering med de lokale personale- og IT-kontorer.

Det fælles brugerkatalog skal opdateres lokalt af de institutioner i sundhedsvæsenet, som har ansvar for klinisk information. Hver gang en sundhedsprofessionel tiltræder, fratræder eller skifter ansvarsområde el.lign. skal brugerkataloget opdateres, så den pågældendes adgangsrettigheder er korrekt defineret.

Denne opgave løses allerede i dag overalt i sundhedsvæsenet – blot sker definitionen af brugeradgangsrettighederne for det meste i forskellige lokale systemer samt i de centrale sundhedssystemer og –registre. Og på grund af den eksisterende diversitet og mangfoldighed mht. sundhedsapplikationer må de sundhedsprofessionelle ofte håndtere et antal bruger-id'er og passwords til forskellige systemer og data.

Det fælles brugerkatalog vil kunne tilgås fra såvel lokale systemer som fra de fælles sundhedsapplikationer. En forudsætning for at en lokal applikation kan have fordel af at benytte brugerkataloget er dog, at applikationen benytter den anvendte standard for udveksling af information om adgangsrettigheder, jf. afsnit 2.9.4 nedenfor. Dette vil på langt sigt bl.a. give medarbejderne mulighed for at få adgang til alle systemer mv. på tværs af sundhedsvæsenet med en enkelt identitet.

Anbefaling

Det anbefales at påbegynde definitionen af ansvarsfordeling og procedurer vedr. brugerstyring og opdatering af sundhedsvæsenets fælles brugerkatalog. Disse opgaver vil formelt ligge hos alle lokale enheder, som har ansvar for at definere, hvem der skal have adgang til sundhedssystemer og til klinisk information.

Efterhånden som en større og større del af sundhedsvæsenets systemer understøtter brugen af certifikater og benytter det fælles brugerkatalog, vil de sundhedsprofessionelle opleve en migrering frem mod et "single sign-on" scenarium, jf. afsnit 2.10 nedenfor. I en overgangsfase over en årrække vil der dog være både lokale adgangssystemer og fælles brugerstyring, og det må forventes, at der vil være en vis redundans imellem disse i overgangsfasen.

2.9.4 Udveksling af information om adgangssystemer

Brugerstyringen og systemernes anvendelse af brugerkataloget vil indebære behov for opslag og udveksling af information om brugeradgangssystemer – såvel for brugere, der arbejder med web-applikationer som for brugere, der arbejder med ikke-web-baserede applikationer. Det forventede koncept for udveksling af brugeradgangssystemer er at benytte XML-baserede SAML (Security Assertions Markup Language) adgangssystem-udsagn (eng. "assertions") over SOAP (Simple Object Access Protocol). Endvidere bør standarden LDAP (Lightweight Directory Access Protocol) anvendes som kommunikationsprotokol til opslag af certifikater og så vidt muligt til alle opslag i brugerkataloget.

Understøttes disse og øvrige relevante åbne standarder, vil det betyde, at de virksomheder, som benytter det centrale brugerkatalog, kan benytte standard Web Services programmel til at realisere single sign-on på heterogene platforme samt til at realisere fortrolighed og signering i det omfang, der er behov for det. Med denne metode vil det i en overgangsfase i nogen udstrækning være muligt at undgå ændringer i eksisterende applikationer, såfremt der er tale om web-baserede applikationer.

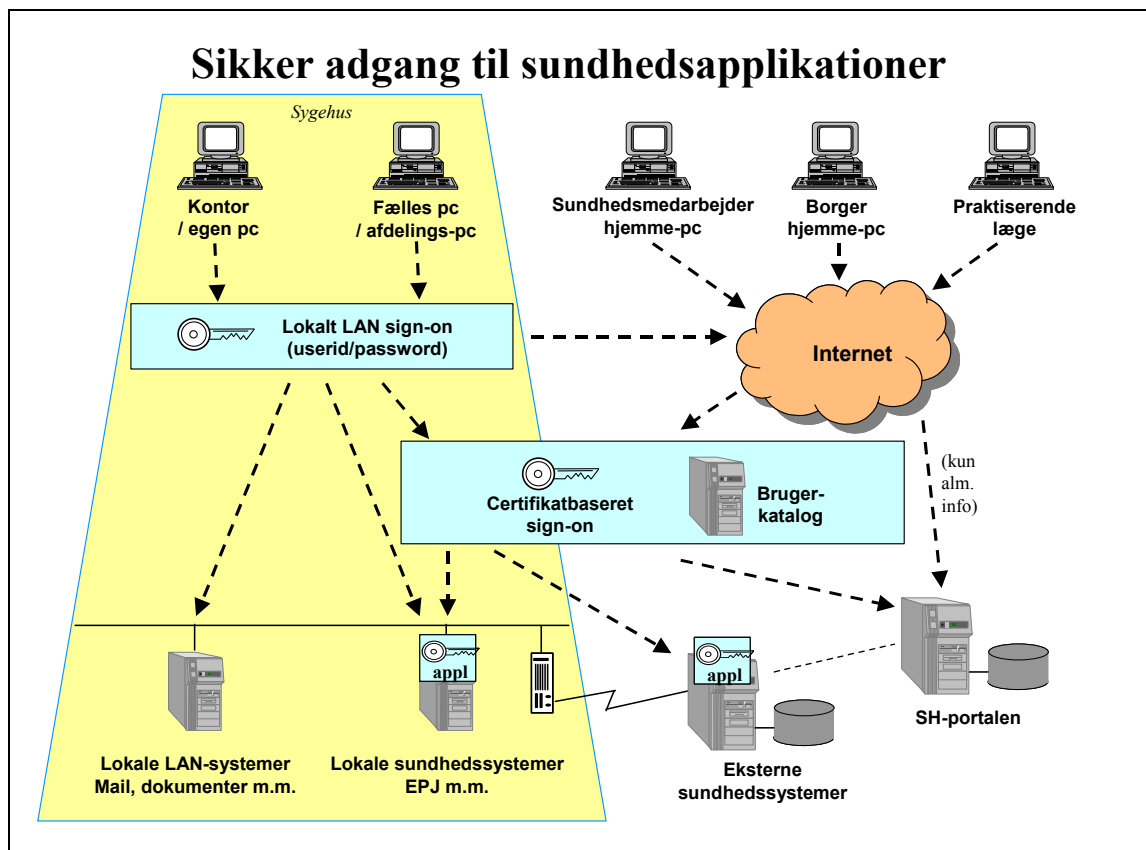
Anbefaling

Det anbefales, at brugerkataloget, systemernes adgang til brugerkataloget samt øvrig udveksling af information om brugeradgangssystemer og certifikater baseres på de åbne markedsanerkendte IT-standarder på dette område.

Specifikt bør definitionen og udvekslingen af adgangssystemer være baseret på XML-formatet og på XML-baserede SAML (Security Assertions Markup Language) adgangssystem-udsagn. Kommunikationen bør være baseret på SOAP (Simple Object Access Protocol) og på LDAP (Lightweight Directory Access Protocol) til opslag af certifikater og så vidt muligt til alle opslag i brugerkataloget.

2.10 Single sign-on og sikker adgang til sundhedsapplikationer

Nedenstående figur illustrerer nogle af de adgangsforhold og sikkerhedsniveauer, som vil være relevante ifm. indførelsen af digital signatur i sundhedsvæsenet.



Certifikatbaseret adgang til sundhedsapplikationer vil i første omgang kunne etableres via en "sign-on" tjeneste, fx på det enkelte sygehus eller på mere tværgående basis. Den sundhedsprofessionelle vil opleve certifikatbaseret sign-on som et "login" med hw-token og PIN-kode til en "sign-on" tjeneste, hvorigennem de relevante applikationer kan nås efter accepten af PIN-koden og så længe hw-token kan læses af klient pc'en, dvs. fx så længe chipkortet sidder i kortlæseren.

Den sundhedsprofessionelle vil dels have adgang til de lokale applikationer (typisk via lokalnettet og Windows-systemet) og dels have adgang til sundhedsapplikationerne, fx via "sign-on" tjenesten.

På kort sigt vil certifikatbaseret sign-on supplere de eksisterende adgangskontrolsystemer i lokalnet på sygehuse og i de enkelte applikationer mv. På længere sigt vil adgangssceneriet konvergere mod et koncept, hvor den digitale signatur (i form af en hw-token med medarbejdercertifikat) er det generelle adgangskontrolsystem overalt.

En mere teknisk beskrivelse af scenariet vedr. sign-on og adgang til sundhedsapplikationer med brug af certifikater kan ses i Bilag C.

2.11 Lovgivning og det formelle grundlag

Der har i forbindelse med udarbejdelsen af denne rapport ikke været foretaget en detaljeret vurdering af, hvorvidt der er behov for ændringer i lovgrundlaget eller det formelle grundlag på sundhedsområdet, herunder hvilke behov der måtte være for udarbejdelse af nye love, direktiver eller vejledninger.

Det er kendt, at der for en række dokumenter og arbejdssituationer i dag stilles formkrav i retning af underskrift el.lign., bl.a. for:

- recepter
- dødsattester
- ligpas
- kørekort, særlig lægeerklæring
- tvangsindlæggelsespapirer, jf. Psykiatriloven
- livstestamenter
- erklæringer
- anmeldelsesblanketter vedr. smitsomme sygdomme
- skriftligt samtykke i medfør af bl.a. patientretsstillingslov, forvaltningslov og persondatalov
- tilbagevisninger, bl.a. tandlæger opererer med dette begreb

Et tværgående arbejde i den offentlige forvaltning i Danmark under betegnelsen ”Den Digitale Taskforce” (jf. ref. 5) har iværksat en række initiativer og har bl.a. vurderet det formelle grundlag for digital forvaltning på alle ministerområder. Dette har ført til konkrete handlingsplaner for hvert enkelt ministerium, således at der allerede i dag foreligger en handlingsplan også for Indenrigs- og Sundhedsministeriet. Ministeriet har identificeret de formkrav, som unødigt hindrer digital kommunikation, og vil foretage de nødvendige ændringer.

Der er endvidere igangværende aktiviteter i Sundhedsstyrelsen på andre områder bl.a. vedr. etableringen af digitale registre og arbejdsgange til erstatning for traditionelle papirbaserede arbejdsgange og procedurer.

2.12 Økonomiske aspekter

Der henvises til vedlagte omkostningselementer og estimater i Bilag E.

2.13 Eksterne relationer og projekter

I forbindelse med udarbejdelsen af denne rapport er der afholdt møde med TDC og IT- og Telestyrelsen, primært med fokus på oplysninger vedr. OCES-certifikater. Disse parter har begge ytret interesse for at deltage i et pilotprojekt og ser initiativet som en løftestang for udbredelse af digital signatur i det offentlige.

Sundhedsstyrelsen har endvidere haft kontakt til parter i Tyskland, Frankrig og Sverige for at forhøre, om der i disse lande er relevante initiativer, som Danmark kan drage nytte af. De første forespørgsler til disse lande har ikke vist eksistensen af direkte anvendelige initiativer eller resultater.

2.14 Problemområder

Der er i dag enkelte uafklarede problemområder omkring brugen af digitale signaturer og af den teknologi, som benyttes hertil. Nogle problemområder med relevans for denne rapport gennemgås kort i dette afsnit.

2.14.1 Langtidsarkivering af signaturer og signerede data

Der er i dag ikke nogen etableret metode til arkivering, således at der skabes mulighed for at verificere signaturer og autenticitet mange år, fx 30 år, efter brugen af en digital signatur / autenticitet. Den teknologi, der benyttes om en årrække, kan være anderledes, og bagudkompatibilitet er ikke givet.

Ydermere vil der være behov for en metode til at sikre, at de arkiverede signaturer ikke forfalskes. Dertil kræves en pålidelig tidsstempling, som indgår i audit-records og i arkiveret materiale.

2.14.2 Applikationernes understøttelse af digital signatur og certifikater

Det er i dag uvist, i hvilket omfang eksisterende sundhedsapplikationer, såvel lokale som fælles applikationer, understøtter brugen af certifikater – både hvad angår bruger-autenticitet og hvad angår kryptering for at opnå fortrolighed. Det er ligeledes uvist, i hvilket omfang eksisterende applikationer kan benyttes via en ”sign-on server”, jf. afsnit 2.10. Brugen af sign-on server kræver, at applikationen giver adgang via en web-grænseflade, hvilket langt fra alle sundhedsapplikationer gør.

Det må forventes, at de fleste applikationer i et eller andet omfang skal revideres, før den fulde understøttelse af certifikater er på plads. Omfanget af dette arbejde er, så vidt det vides, ikke vurderet, og en sådan vurdering vil kræve en gennemgang af alle applikationer, som ikke forventes udfaset i løbet af få år. For nogle af de nyere, strategiske applikationer, herunder EPJ-systemer, er det sandsynligt, at der eksisterer foreløbige vurderinger af brugen af digitale signaturer og certifikater, men dette ligger ikke inden for rammerne af denne rapport's genstandsfelt.

2.14.3 Brugen af forkant-teknologi og -tjenester

Brugen af certifikater, herunder OCES-certifikater, og hw-tokens må klassificeres som et teknologisk og organisatorisk forkantområde. Erfaringerne med disse teknologier og tjenester er i dag begrænsede, og det må forventes, at dette forhold kan indebære et både tids- og ressourcemæssigt (mer)forbrug for de første projekter og faser og ligeledes med den bredere implementering.

3 Pilotprojekter og initiativer

Dette afsnit identificerer nogle områder, som vil være relevante at undersøge nøjere og vurdere i pilotprojekter – såvel mindre pilotprojekter med fokus på teknologi-vurdering som større pilotprojekter med fokus på vurdering og omlægning af arbejds-gange.

3.1 Vurdering af egnede hw-tokens

Jf. afsnit 2.3.1 er der fordele og ulemper ved de forskellige alternative hw-tokens, som kan benyttes til at holde certifikater og nøgler, såsom chipkort, USB-token og trådløs teknologi.

Det vil være relevant at foretage en vurdering af fordelene, ulemperne og egnetheden ved de nævnte hw-tokens ved daglig brug på fx et hospital og i en lægepraksis, hvor det daglige arbejde indebærer hyppige sign-on og –off ved skiftende pc'er.

Det er endvidere relevant at vurdere, hvorledes de forskellige typer af hw-tokens kan opbevares både tilgængeligt og sikkert af personalet på sådanne arbejdssteder, hvor arbejdsdragten og –miljøet giver visse restriktioner og vanskeligheder ifm. opbevaring og brug af sådanne genstande.

Endelig vil det være nødvendigt at samarbejde med TDC omkring brugen af hw-tokens aht. understøttelsen af OCES-certifikater.

Et pilotforsøg behøver ikke nødvendigvis at foregå i et realistisk miljø, men kan i nogen udstrækning gennemføres i et ”simuleret” miljø.

Formål

Formålet med pilotprojekter i dette område vil være at

- skabe grundlag for valg af egnet hw-token
- samarbejde med TDC om brugen af hw-token til OCES-certifikater

3.2 LRA-funktionalitet og LRA-procedurer

Konceptet for udstedelse og administration af OCES-medarbejdercertifikater i sundhedsvæsenet skal realiseres bl.a. gennem en LRA-funktionalitet, som er egnet til sundhedsvæsenets struktur og behov, jf. afsnit 2.8. Endvidere skal der etableres administrative procedurer både for den ordinære udstedelse af medarbejdercertifikater og for udstedelsen og anvendelsen af midlertidige certifikater og nøgler – dels til vikarer og dels til medarbejdere, som har mistet eller glemt deres hw-token.

I dialogen med TDC har TDC tilkendegivet åbenhed for at samarbejde med sundhedsvæsenet om den mere præcise definition og realisering af LRA-funktionaliteten. Dette samarbejde vil være et oplagt emne for et pilotprojekt, hvor LRA-funktionaliteten dels specificeres og implementeres med udgangspunkt i den allerede eksisterende LRA Professional og dels afprøves i en mere realistisk ramme. Samtidig bør dette arbejde omfatte de til LRA-opgaven knyttede procedurer, som skal ses og fungere i sammenhæng med LRA-funktionaliteten.

Formål

Formålet med pilotprojekter i dette område vil være at

- tilvejebringe den rette LRA-funktionalitet i samarbejde med TDC
- identificere de administrative procedurer for LRA-opgaverne

3.3 Retningslinier for håndtering af OCES-certifikater i nye applikationer

Jf. afsnit 2.14.2 ovenfor vil det for de applikationer, som ikke fases ud i løbet af få år, være nødvendigt at foretage en justering, så brugen af digital signatur og certifikater understøttes. Da der benyttes et stort antal forskellige applikationer i sundhedsvæsenet, vil udarbejdelsen af standardmetoder og retningslinier kunne bidrage til en mere effektiv justering af applikationerne.

Det vil derfor være relevant at vurdere muligheden for at udarbejde sådanne standarder og retningslinier for applikationer i sundhedsvæsenet. Dette vil fx kunne ske sammen med pilot-justering og -afprøvning for udvalgte applikationer.

Formål

Formålet med pilotprojekter i dette område vil være at

- vurdere forskellige typer applikationer mhp. understøttelse af digital signatur
- skabe og formulere retningslinier for, hvorledes applikationer i sundhedsvæsenet bør understøtte digital signatur og brugen af certifikater

3.4 Biometriske metoders fordele og ulemper i forskellige arbejdssituationer

Jf. afsnit 2.3 kan biometri benyttes som et alternativ – eller eventuelt som et supplement – til PIN-kodebaseret adgang til certifikat og nøgler.

Der kan i dag anskaffes biometrisk teknologi til pc'er, fx i form af mus med fingeraftryks-aflæser. Selvom sådanne teknologier også indebærer ulemper og i givet fald vil skulle anskaffes til alle arbejdsplads-pc'er, vurderes det at være relevant at etablere forsøg, hvor biometriske teknologier afprøves i forskellige arbejdssituationer med henblik på at vurdere deres anvendelighed i sundhedsvæsenet.

Formål

Formålet med pilotprojekter i dette område vil være at

- vurdere egnetheden af biometrisk adgangssikkerhed i sundhedsvæsenets IT-systemer ift. arbejdssituationerne og dagligdagen for sundhedsmedarbejderne

3.5 Bruger katalog og brugerstyring

Bruger katalog og brugerstyring samt opgaverne i denne sammenhæng er beskrevet i afsnit 2.9. Etableringen af et generelt bruger katalog for sundhedsvæsenet er en opgave, der må forventes at ske over en periode på flere år (forventet 2-4 år).

For et projekt af denne art, hvor løsningen skal anvendes af systemer på tværs af hele sundhedsvæsenet, og hvor mange parter er involveret, vil det kunne bidrage til en effektiv implementering, at de første erfaringer – såvel teknisk som proceduremæssigt – sker i mindre skala. Det vil fx være relevant at tage udgangspunkt i 1-2 udvalgte systemer på en hospitalsafdeling og etablere bruger kataloget for medarbejderne på den valgte afdeling for de pågældende systemer.

Valget af systemer kunne endvidere tilgodese, at der foretages forsøg med såvel en nyere web-baseret applikation som med en web-enabled, ældre applikation med traditionelle sikkerhedsfaciliteter.

Formål

Formålet med pilotprojekter i dette område vil være at

- få erfaring med brugerstyring i mindre skala / på pilotbasis, før en mere generel løsning implementeres i hele sundhedsvæsenet
- identificere eventuelle tekniske eller andre problemstillinger forud for en implementering af det fulde bruger katalog

BILAG A REFERENCER

1. ”OCES – Digital Signatur”; IT- og Telestyrelsen, Ministeriet for Videnskab, Teknologi og Udvikling; www.signatursekretariatet.dk (dato 10/9-2003)
2. ”TDC, Erhverv, Digital Signatur”, TDC; erhverv.tdc.dk/digital/ (dato 10/9-2003)
3. ”TDC Certificeringscenter”, TDC; www.certifikat.dk (dato 10/9-2003)
4. ”Foranalyse til pilotprojekt, til etablering af centralt brugerkatalog”, Sundhedsstyrelsen / MedCom i samarbejde med Oracle Danmark; Januar 2003; www.medcom.dk/mc4/inet/tekn/bruger/ (dato 10/9-2003)
5. ”Projekt Digital Forvaltning, Den Digitale Taskforce”; www.e.gov.dk (dato 10/9-2003)
6. ”IT-sikkerhedsvejledning for sygehuse”, Sundhedsstyrelsen, 17. juli 2002; http://www.sst.dk/publ/Publ2002/IT_sikkh_sgh_korr.pdf (dato 30/10-2003)
7. ”National IT-strategi for sundhedsvæsenet 2003-2007”, Sundhedsstyrelsen, Maj 2003; http://www.sst.dk/upload/nat_itstrategi03_07.pdf (dato 30/10-2003)
8. ”Etablering af national sundhedsportal”, Amtsrådsforeningen, Projektbeskrivelse 1. februar 2002; kan findes under <http://www.arf.dk/DigitaleAmter/SundhedsIt/Sundhedsportal/Materiale.htm> (dato 30/10-2003)
9. ”Den Fælles Offentlige Sundhedsportal”, Amtsrådsforeningen; <http://www.arf.dk/DigitaleAmter/SundhedsIt/Sundhedsportal/Index.htm> (dato 30/10-2003)
10. ”Notat vedr. digital signatur og brugerstyring”, Sundhedsstyrelsen, 12. august 2003
11. ”Vedr. udstedelse og vedligeholdelse af certifikater”, Arbejdsrapport, Sundhedsstyrelsen, 16. september 2003
12. ”OCES certifikatpolitikker”, bl.a. ”Certifikatpolitik for OCES-medarbejdercertifikater”, IT- og Telestyrelsen, Januar 2003 (jf. ref. 1)

BILAG B BEGREBER OG FORKORTELSER

Nedenstående liste omfatter en lang række begreber, som enten er benyttet i nærværende rapport eller som er beslægtet med de emner, som rapporten omhandler.

Der er anført kildeangivelse de steder i listen, hvor der er benyttet ordforklaringer fra andre kilder. I enkelte tilfælde, hvor det har været skønnet hensigtsmæssigt, er sådanne citerede ordforklaringer suppleret af yderligere forklarende tekst.

I alle ordforklaringer er de af listen omfattede ord angivet med *kursiv*.

A

Asymmetrisk kryptering
("Asymmetric encryption")

Asymmetrisk kryptering er betegnelsen for en familie af krypteringsmetoder og algoritmer, der kan benyttes til at skabe digital *autenticitet*, *uafviselighed*, *integritet* og *fortrolighed* – og dermed *digitale signaturer*.

Asymmetrisk kryptering er baseret på brugen af et nøglepar i form af hhv. en *privat nøgle* og en *offentlig nøgle*. Disse *nøgler* er hinandens inverse ifm. kryptering og dekryptering, og den ene *nøgle* kan ikke udledes ud fra kendskab til den anden *nøgle*. *Fortrolighed* opnås ved at kryptere med den *autoriseredes* / modtagerens *offentlige nøgle*, hvorved de krypterede data kun kan læses (dekrypteres) ved brug af den *autoriseredes* / modtagerens *private nøgle*. Omvendt opnås signering ved kryptering med den *private nøgle*, hvorved læsning (dekryptering) med den *offentlige nøgle* sikrer, at data stammer fra indehaveren af den *private nøgle*. Se også *digital signatur*.

Attributcertifikat
("Attribute certificate")

En elektronisk attest, som binder en given attributværdi til en bestemt *certifikatindehavers nøglecertifikat*. Attributværdien angiver en bemyndigelse (prokura). *Attributcertifikatet* er signeret af den enhed, som har givet denne bemyndigelse (kilde: *OCES, ref. 12*).

Autenticitet
("Authenticity")

Autenticitet (eller "ægthed") betyder at "noget" – fx en person eller data – er det, som den/det giver sig ud for at være. Sikring af "brugerautenticitet" i sundhedssystemer betyder således, at *identiteten* af den enkelte *sundhedsprofessionelle*, som får adgang til et system eller til data, er *verificeret* og at det derigennem er fastslået at personen er den, som han/hun giver sig ud for at være (se *autentificering*). *Autenticitet* benyttes også om ægtheden af fx software og udstyr, og at dette ikke er forfalsket.

Funktioner der udføres eller data der sendes af en person, som i forbindelse med funktionen er *autentificeret* med *digital signatur*, er med meget stor sandsynlighed ægte og uforfalskede og kan ikke senere afvises af den pågældende (se *uafviselighed*).

Autentificering
"Authentication"

At fastslå – at skabe sikkerhed for – *autenticiteten* (eller "ægtheden") af fx en person eller af data. Dette kan fx ske med brug af *digital signatur*, men også som i de fleste systemer i dag med brug af bruger-id / password eller *PIN-kode*. Bruger-id / password og *PIN-kode* giver svagere sikkerhed for *autenticiteten* end en *digital signatur*.

Autorisation
(generel IT-term)
("Authorisation")

Generelt ifm. IT-systemer og IT-sikkerhed betyder *autorisation* de rettigheder en bruger (eller et objekt) besidder i forhold til adgang til systemer, funktioner og data.

I denne rapport er denne term søgt undgået pga. sammenfaldet med begrebet sundhedsfaglig autorisation. I stedet er termer som "adgangsrettigheder" og i enkelte tilfælde "*autorisere*" benyttet.

Autorisation
(sundhedsfaglig autorisation)
("License")

Den sundhedsfaglige *autorisation*, som af Sundhedsstyrelsen tildeles *sundhedspersoner*, fx læger og sygeplejersker (se også *sundhedsprofessionelle*). Må i denne rapport ikke forveksles med *autorisering*.

Autorisere
("Authorise")

At tildele *autorisation* (rettigheder) til en person eller et objekt, dvs. at give personen (objektet) fx adgangsrettigheder til et system eller til at udføre en nærmere angivet form for behandling af nærmere angivne data. Se også *autorisation* (to betydninger). I denne rapport benyttes termen "*autorisere*" om tildeling af rettigheder ifm. IT-systemer.

B

Bemyndiget Person, der af virksomhedens ledelse er valgt og godkendt som kontaktperson, og som har prokura til på virksomhedens vegne at godkende og indsende certifikatansøgninger og/eller administrere virksomhedens *certifikater* (kilde: *OCES, ref. 12*).

Biometrisk identifikation *Identifikation* af en person ud fra dennes fysiske (biologiske) og unikke karakteristika, fx i form af fingeraftryk, stemme eller irismønstre.

C

CA ”Certification Authority” – se *certificeringscenter*.

Certificering (“Certification”) At udstede et *certifikat*, dvs. et bevis for, at en organisation, en person eller et objekt opfylder visse specificerede egenskaber og betingelser, som under *certificeringen* er blevet *verificeret*. *Certificering* kræver i sig selv, at omverdenen har tillid til den (normalt uafhængige) enhed, der udfører *certificeringen* (se også *certificeringsenhed* og *krydscertificering*).

Certifikat (“Certificate”) Et bevis for, at en person, en organisation eller et objekt opfylder visse specificerede egenskaber og betingelser, som er blevet verificeret i en *certificering*. Et *certifikat* identificerer ud over øvrige oplysninger i *certifikatet* såvel den certificerede persons (eller det certificerede objekts) *identitet* som den certificerende enheds *identitet*.

Termen *certifikat* benyttes i denne rapport synonymt med termen *nøglecertifikat*. Et *certifikat* kan også være et *attributcertifikat*. I denne rapport skrives *attributcertifikat*, når det er denne form for *certifikat*, der refereres til.

Certifikatindehaver (“Subscriber”) En fysisk eller juridisk person, der indgår aftale med det udstedende *certificeringscenter* (*CA*) for en eller flere *certifikatholdere*. For personcertifikater vil *certifikatindehaveren* være sammenfaldende med *certifikatholderen* (kilde: *OCES, ref. 12*).

Certifikatholder (“Subject”) Person eller afdeling, som i *certifikatet* er identificeret som den rette anvender af den *private nøgle*, der er associeret med den *offentlige nøgle*, der er givet i *certifikatet* (kilde: *OCES, ref. 12*).

Certificeringscenter (“Certification authority”) En fysisk eller juridisk person, der er bemyndiget til at generere, signere og udstede certifikater (kilde: *OCES, ref. 12*).

Certificeringspraksis ("Certification Practice Statement")	En specifikation af hvilke principper og procedurer, en <i>CA</i> anvender ved udstedelse af <i>certifikater</i> (kilde: <i>OCES, ref. 12</i>).
Certifikatpolitik ("Certificate policy")	Et sæt af regler, der angiver krav til udstedelse og brug af <i>certifikat</i> i et eller flere specifikke sammenhæng, hvor der findes fælles sikkerhedskrav (kilde: <i>OCES, ref. 12</i>).
Chipkort	Et <i>chipkort</i> – synonymt med et ”processorkort” og med et ”smart card” – er et plastkort med en mikroprocessor (en ”chip”). <i>Chipkort</i> kan lagre data og kan benyttes i kortlæsere, hvor data kan læses fra kortet og skrives på kortet, dvs. i chippens hukommelse. <i>Chipkort</i> benyttes bl.a. som betalingskort, adgangskort og som <i>identifikation</i> . <i>Chipkort</i> eksisterer både som kontaktfri kort, hvor læsning og skrivning kan ske trådløst, når blot kortet holdes i nærheden af kortlæseren, og som kort med kontakter, hvor læsning og skrivning sker ved, at kortet fysisk placeres i en kortlæser. Også kombinerede kontaktfri- / kontakt- <i>chipkort</i> kan fås.
CP	”Certificate Policy” – se <i>certifikatpolitik</i> .
CPS	“Certification Practice Statement” – se <i>certificeringspraksis</i> .
CRL	“Certificate Revocation List” – se <i>spærreliste</i> .

D

Digital signatur	En <i>digital signatur</i> er en digital <i>autentificering</i> , som benyttes i IT-systemer og IT-applikationer ifm. <i>autentificering</i> af fx brugere, meddelelser, systemenheder og –objekter og udførelse af funktioner. Termen <i>digital signatur</i> er i dag knyttet til den signeringsteknologi, der baserer sig på <i>asymmetrisk kryptering</i> . Gennem brugen af et <i>certifikat</i> og dannelsen af et ”fingeraftryk” – en slags checksum – af de data, der signeres, sikres ud over <i>autentificering</i> og <i>uafviselighed</i> også <i>integriteten</i> af de signerede data. Endvidere kan den samme teknologi benyttes til at skabe <i>fortrolighed</i> – se <i>asymmetrisk kryptering</i> .
------------------	---

E

Elektronisk signatur
("electronic signature")

Data i en elektronisk form, som er vedhæftet eller logisk tilknyttet andet elektronisk data, og som tjener til *autentificering* af data (kilde: *OCES, ref. 12*).

Den danske lovgivning benytter termen "*elektronisk signatur*" og ikke "*digital signatur*". De to termer bruges i en vis udstrækning som synonyme, men begrebet "*elektronisk signatur*" bør betragtes som bredere, idet begrebet "*digital signatur*" ofte refererer til den specifikke signeringsteknologi, som er baseret på *asymmetrisk kryptering*.

F

Fortrolighed
("Confidentiality")

Fortrolighed betyder, at uvedkommende ikke kan få adgang til eller mulighed for at benytte systemer, informationer og data, som de ikke er berettiget til. Det kan fx være væsentligt at sikre *fortrolighed* af følsomme persondata og økonomiske data.

Fortrolighed af en meddelelse sikres via kryptering. I forbindelse med *digital signatur* krypteres med modtagerens *offentlige nøgle*, således at kun besidderen af den tilhørende *private nøgle* (modtageren) kan dekryptere og læse meddelelsen.

G

H

I

Identifikation

At stadfæste *identiteten* af "noget" - typisk en person. Se også *biometrisk identifikation*.

Identitet

Normalt benyttes *identitet* om en person, dvs. hvem vedkommende er, normalt identificeret ved navn og fødselsdato og evt. CPR-nummer, adresse mv. Se også *identifikation*.

Integritet
("Integrity")

Integritet af data betyder, at data er komplette, korrekte og uforfalskede. En *digital signatur*, dvs. digital signering af data, skaber meget høj sikkerhed for *integriteten* af de signerede data.

Integritet kan fx også benyttes om det forhold, at et system fungerer, som det er defineret, og at det indeholder de korrekte hardware- og softwarekomponenter, brugerdefinitioner, adgangsrettigheder osv.

J

K

Klinisk information

Sundhedsrelateret oplysning om én person, der beskriver forhold ved dennes sundhedstilstand, sundhedsaktivitet eller interventionsresultat, herunder undersøgelsesresultat.

Krydscertificering

Gensidig *certificering* udført af to eller flere parter, fx *certificeringscentre*, med det formål at skabe tillid på tilsvarende måde, som en uvildig tredieparts *certificering* gør.

Kvalificeret certifikat
("qualified certificate")

Et *certifikat* udstedt i henhold til lov om *elektroniske signaturer*, lov nr. 417 af 31. maj 2000 (kilde: *OCES, ref. 12*).

I forbindelse med udstedelse af et *kvalificeret certifikat* kræves der personligt fremmøde af *certifikatholderen* af hensyn til *identifikationen*.

L

LDAP

"Lightweight Directory Access Protocol". En standardiseret kommunikationsprotokol for opslag af information i et katalog (et "directory"). *LDAP* bruges i vid udstrækning til opslag af *certifikater* i såkaldte "X.500-directories", dvs. kataloger baseret på X.500-standarderne. *LDAP* er en Internet standard.

LRA

"Local Registration Authority". En "lokal" *registreringsenhed*, dvs. en organisatorisk enhed, der udfører en del af en *registreringsenheds* opgaver fx i en virksomhed. En *LRA* er underordnet en *RA*.

Udtrykket "lokal" betoner, at der i en organisation kan være flere *LRA*'er, der tilsammen udfører organisationens *RA*-opgaver.

M

N

Nøgle ("Key")	I forbindelse med <i>digitale signaturer</i> en <i>privat nøgle</i> eller en <i>offentlig nøgle</i> , som benyttes i en krypteringsmetode (algoritme) til hhv. kryptering og dekryptering af data, som skal signeres og/eller hemmeligholdes. Se <i>asymmetrisk kryptering</i> .
Nøglecenter	Anvendes i nogen grad som synonym for <i>certificeringscenter</i> . Begrebet <i>nøglecenter</i> udtrykker dog implicit, at der er tale om generering af <i>nøgler</i> til et <i>certifikat</i> , hvilket kan ske såvel hos et <i>certificeringscenter</i> som hos en <i>RA/LRA</i> . Udtrykket benyttes ikke i denne rapport.
Nøglecertifikat ("public-key certificate")	En elektronisk attest, som angiver <i>certifikatindehaverens offentlige nøgle</i> sammen med supplerende information, og som entydigt knytter den <i>offentlige nøgle</i> til <i>identifikation</i> af <i>certifikatindehaveren</i> . Et <i>nøglecertifikat</i> skal signeres af et <i>certificeringscenter (CA)</i> , som derved bekræfter <i>certifikatets</i> gyldighed (kilde: <i>OCES, ref. 12</i>).

O

OCES	”Offentlige Certifikater til Elektronisk Service”. I 2003 lancerede Ministeriet for Videnskab, Teknologi og Udvikling det nationale <i>OCES</i> -koncept og <i>OCES</i> -initiativ, der skal være med til at fremme anvendelsen af <i>digital signatur</i> i Danmark (jf. ref. 1). <i>OCES</i> -konceptet blev i første omgang baseret på <i>software-certifikater</i> , der ikke har status af <i>kvalificerede certifikater</i> , men konceptet er efterfølgende udvidet til at omfatte <i>hardware-certifikater</i> . Der er p.t. 2 <i>certificeringscentre</i> knyttet til <i>OCES</i> -initiativet, hhv. TDC og Eurotrust PKI Services A/S.
Offentlig nøgle ("Public key")	En <i>nøgle</i> , som er knyttet til en tilhørende <i>privat nøgle</i> , og sammen med denne kan benyttes i <i>asymmetrisk kryptering</i> . Den <i>offentlige nøgle</i> indgår i et <i>certifikat</i> , hvor <i>certifikatholderens identitet</i> er angivet. Se også <i>asymmetrisk kryptering</i> .

P

PIN-kode ("PIN code")	Et (cifferbaseret) password til sikring af <i>autenticiteten</i> , knyttet til brugen af typisk en fysisk enhed fx et betalingskort. I forbindelse med <i>digital signatur</i> er der knyttet <i>PIN-kode</i> til brugen af et <i>certifikat</i> – uanset om der er tale om <i>hardware-</i> eller <i>software-certifikater</i> . ”PIN” står for ”Personal Identification Number”.
PKI	”Public Key Infrastructure” – se denne.
Public Key Infrastructure	En sammenhæng af organisationer og infrastruktur, der kan tillade brug af <i>digital (elektronisk) signatur</i> ved at stille anerkendte krypteringsnøgler og attester for disses validitet og tilhørsforhold til rådighed (kilde: IT-sikkerhedsvejledning for sygehuse, ref. 6). I <i>OCES</i> -konceptet skabes denne infrastruktur ved Ministeriet for Videnskab, Teknologi og Udvikling’s initiativ bl.a. gennem udarbejdelsen af en <i>certifikatpolitik</i> og etableringen af <i>certificeringscentre</i> for <i>OCES-certifikater</i> (se ”OCES”).
Privat nøgle ("Private key")	En <i>nøgle</i> , som er knyttet til en tilhørende <i>offentlig nøgle</i> , og sammen med denne kan benyttes i <i>asymmetrisk kryptering</i> . Den <i>offentlige nøgle</i> indgår i et <i>certifikat</i> . Kun <i>certifikatholderen</i> må kende og benytte den <i>private nøgle</i> , og tilgangen til den <i>private nøgle</i> er beskyttet med <i>PIN-kode</i> . Se også <i>asymmetrisk kryptering</i> .

Q

R

RA	"Registration Authority" – se <i>registreringsenhed</i> .
Registreringsenhed ("Registration authority")	Den fysiske eller juridiske person, der er ansvarlig for <i>identifikation</i> og <i>autentificering</i> af en (kommende) <i>certifikatholder</i> (kilde: <i>OCES</i> , ref. 12 – dog er i <i>OCES</i> benyttet ordet "autentifikation" i.st.f. "autentificering").
Rodcertifikat ("Root certificate")	Et <i>nøglecertifikat</i> udstedt af en <i>CA</i> til brug for signering af andre <i>certifikater</i> . Et rodcertifikat er signeret med sin egen <i>nøgle</i> (egensignering ("self signing")) (kilde: <i>OCES</i> , ref. 12).

S

Sundhedsperson	Ved <i>sundhedsperson</i> forstås en person, der er <i>autoriseret</i> i henhold til særlig lovgivning til at varetage sundhedsfaglige opgaver og personer, der handler på disses ansvar (kilde: Lov om patienters retsstilling, § 4). <i>Sundhedspersoner</i> , eksempelvis læger, sygeplejersker og fysioterapeuter, har i kraft af deres <i>autorisation</i> adgang til, skaber og/eller benytter klinisk information.
Sundhedsprofessionel	En <i>sundhedsprofessionel</i> er en person, som har adgang til, skaber og/eller benytter klinisk information. <i>Sundhedsprofessionelle</i> omfatter alle <i>sundhedspersoner</i> samt eksempelvis lægesekretærer og SoSu-assistenten, som ikke i dag har en formel <i>autorisation</i> . Der kan tænkes indført en form for <i>autorisation</i> til alle <i>sundhedsprofessionelle</i> i det danske sundhedsvæsen.
Sundhedsmedarbejder	En <i>sundhedsmedarbejder</i> er en person, som enten er <i>sundhedsprofessionel</i> , eller som er ansat i det danske sundhedsvæsen, fx i en administrativ eller tilsvarende funktion såsom administrations-, kantine- eller IT-medarbejder. <i>Sundhedsmedarbejdere</i> , som ikke er <i>sundhedsprofessionelle</i> , har oftest ikke behov for at have adgang til klinisk information.
Signaturmodtager ("verifier or relying party")	En fysisk eller juridisk person, der modtager en <i>elektronisk signatur</i> , som er dannet ved signering af data fra en <i>certifikatholder</i> (kilde: <i>OCES</i> , ref. 12).
Smart card	Se <i>chipkort</i> .

Spærreliste ("Certificate Revocation List" - CRL)	En liste over <i>certifikater</i> , som ikke længere anses for gyldige, fordi de er permanent spærret (kilde: <i>OCES, ref. 12</i>).
SSL	”Secure Socket Layer”. En Internet-standard, oprindeligt udviklet af Netscape, til opnåelse af sikker kommunikation mellem to parter (fx klient og server) over en TCP/IP forbindelse. Normalt benyttes i <i>SSL</i> de faciliteter, der sikrer <i>fortrolighed</i> (via kryptering) og <i>autenticitet</i> af tjenesten/serveren over for klienten. <i>SSL</i> giver også mulighed for, at serveren kan <i>autentificere</i> klienten. <i>SSL</i> er generelt understøttet af markedets Internet-produkter, herunder af de mest benyttede browsere og af et stort antal web-tjenester.
Stærk autentificering	<p><i>Stærk autentificering</i> forudsætter, at (mindst) to af følgende tre adgangsnøgler benyttes:</p> <ol style="list-style-type: none"> 1) Viden – noget man ved (fx password eller PIN-kode) 2) Hardwarenøgle – noget man har (fx en nøgle eller et chipkort) 3) Biometrisk identifikation – noget man er (fx fingeraftryk) <p><i>Stærk autentificering</i> giver større sikkerhed for <i>autenticiteten</i> end almindelig (svag) <i>autentificering</i>, der baserer sig på blot en enkelt af ovenstående – typisk ”noget man ved” i form af fx. password.</p>

T

Tidsstempling	<p>En digital <i>tidsstempling</i> af fx data eller udførte funktioner, der kan benyttes, således at det senere når som helst kan fastslås, hvornår en bestemt handling eller oplysning er gennemført / afgivet.</p> <p>For at sikre imod forfalskning kan der være behov for i nogle sammenhænge at benytte <i>tidsstempling</i> fra uafhængige eksterne tjenester – såkaldte ”Time Stamping Services” (TSS).</p>
---------------	--

U

Uafviselighed
("non-repudiation")

Uafviselighed betyder sikkerheden for, at en person, der har udført en handling eller funktion eller er ophav til information, ikke siden kan afvise sin handling eller korrektheden og ægtheden af informationen.

Uafviselighed kan sikres gennem brugen af *certifikater* og *digital signatur*. Fx vil en person, der har udført en funktion eller indtastet data og bekræftet dette med sit *certifikat* og sin *private nøgle* (via brugen af *PIN-koden*) ikke senere kunne afvise handlingen.

I papirets verden sikres *uafviseligheden* traditionelt v.hj.a. underskrifter, stempler, kvitteringer o.lign.

V

Verifikation
("Verification")

Verifikation betyder eftervisning, fx af en persons *identitet* (*verifikation* af *autenticitet*) eller af en digitalt signeret meddelelses ægthed (*verifikation* af *autenticitet* og *integritet* samt evt. *tidsstempel*). *Verifikation* af en *digital signatur* indebærer bl.a. at sikre, at det benyttede *certifikat* (og dermed de tilhørende *nøgler*) ikke var spærret på det tidspunkt signaturen blev dannet.

X

Y

Z

Æ

Ø

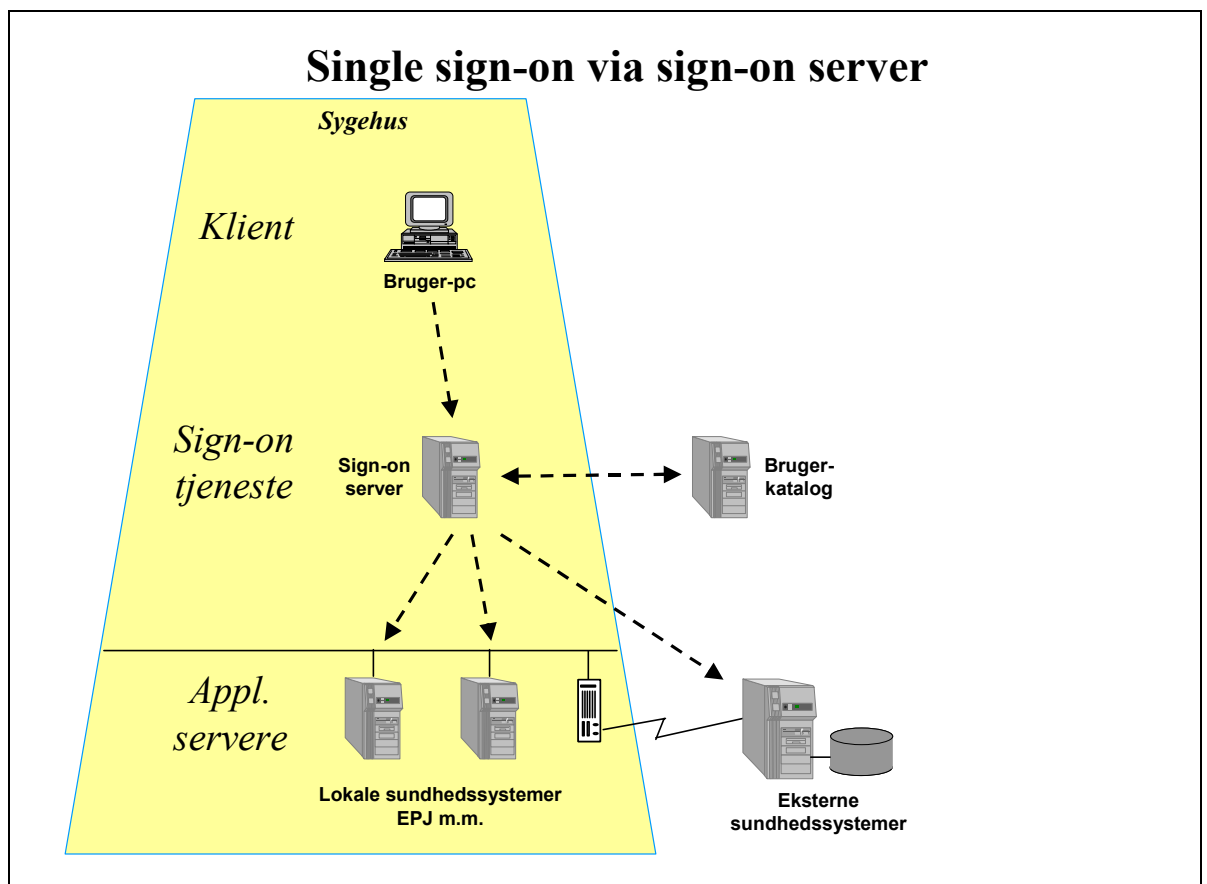
Å

BILAG C TEKNISKE LØSNINGSELEMENTER

C.1 Komponenter vedr. single sign-on med certifikat

Dette bilag giver en mere teknisk beskrivelse af scenariet omkring single sign-on og adgang til sundhedsapplikationer med brug af certifikat på hw-token og med brug af sign-on server og bruger katalog, jf. afsnit 2.10.

Figuren nedenfor illustrerer, med udgangspunkt i figuren i afsnit 2.10, nogle af de i det følgende omtalte komponenter.



Klientsiden

På klientsiden (brugerens pc) skal håndtering af certifikater understøttes. Denne funktion ligger normalt i web-browseren (fx Microsoft Internet Explorer) og er en del af "crypto store". Crypto store tilbyder dels et interface (Crypto Application Programmers Interface – CAPI) mod applikationer på klient-pc'en og dels et interface mod håndtering af certifikater. Sidstnævnte interface, der kaldes CSP (Cryptographic Service Provider), er specifikt for den leverandør, hvis produkt er benyttet til at beskytte brugerens digitale ID (den krypterede fil, der indeholder brugerens sikkerhedsdata, herunder den private nøgle), fx leverandøren af hw-tokens.

CSP er endvidere betegnelsen for den software, der bl.a. genererer det offentlige / private nøglepar. CSP'en udfører ligeledes de kryptografiske operationer så som kryptering og digital signatur.

Microsoft leverer en standard CSP til håndtering af moduler, der leveres af Microsoft, mens fx leverandører af chipkort-løsninger har udviklet deres egen CSP, der skal benyttes for at kunne bruge chipkort'et.

Crypto store kan indeholde flere CSP'er samtidig. Disse kan aktiveres uafhængigt af hinanden.

Når en bruger ønsker adgang til en applikation, der er understøttet af single sign-on, indlæser han sin hw-token (fx chipkort) og vil herefter blive bedt om PIN-kode. Brugerens identitet vil dernæst blive verificeret af sign-on tjenesten, hvorefter der, så længe brugeren har sin hw-token i pc'en, vil være adgang for brugeren til de applikationer, som brugeren har fået adgangsrettigheder til.

Indgangen til applikationerne kan enten være via en adgangsmenu, som præsenteres for brugeren af sign-on tjenesten efter autentificeringen, eller, alternativt, transparent for brugeren, således at brugeren ikke oplever tilstedeværelsen af en sign-on server.

Serversiden

På sign-on serveren verificeres brugerens autenticitet ved sign-on (og ved andre funktionskald afhængig af opsætning) via brugerens medarbejdercertifikat og den ifm. request'et modtagne signatur. Herefter checkes i et brugerkatalog, om brugeren må få adgang til den applikation, der bedes om – alternativt (i tilfælde af opsætning med menu), hvilke applikationer, brugeren har adgang til. Der kan her være tale om et lokalt brugerkatalog og/eller et fælles brugerkatalog, som tilgås via SAML-standarden for udveksling af oplysninger vedr. adgangsrettigheder ("assertions"), jf. afsnit 2.9.4.

Sign-on serveren videresender nu brugerens request til applikationen samt brugerens ID i form af medarbejderidentifikationen angivet i certifikatet.

Afhængig af den pågældende applikation og det sikkerhedsniveau, der ønskes i den videre kommunikation mellem bruger og applikation, kan brugeren udføre funktioner direkte i applikationen uden om sign-on serveren eller via sign-on serveren. En fordel ved at lade kommunikationen gå via sign-on serveren er, at der kan etableres en fælles sikker kommunikationsforbindelse mellem bruger og sign-on server (typisk SSL – Secure Socket Layer) som opretholdes lige så længe brugeren har sin hw-token i pc'en. Kommunikation mellem sign-on server og applikation foregår oftest i et sikkert servermiljø.

Herudover er det muligt for applikationen selv at udføre yderligere styring af adgang til funktioner og information ved brug af et brugerkatalog eller gennem applikationsspecifik rettighedsstyring. Det er endvidere muligt for applikationen at afkræve brugeren signering af specifikke transaktioner eller data, hvilket kan være særdeles relevant ifm. handlinger som de i afsnit 2.11 nævnte.

De tilgængelige sign-on server-løsninger fungerer primært mod web-applikationer.

En særlig problemstilling knytter sig til ”multi-domain services”, dvs. hvor brugere får adgang via en sign-on tjeneste i et (Internet-)domæne til applikationer i andre domæner. Konceptuelt skal ”multi-domain services” være understøttet i alle sign-on servers – på tværs af domæner, således at brugeren ikke behøver at bekymre sig om, hvor en bestemt applikation er placeret, og så sikkerheden ikke bliver ringere (eller unødigt skærpet) ved tilgang til applikationer i andre domæner. Markedets produkter gør dette muligt i nogen udstrækning, men det kan ikke antages, at der i dag er fuld kompatibilitet mellem forskellige produkter. Ligeledes må det forventes, at konfigureringsmæssige forskelle vil kunne medføre forskelligheder på brugergrænsefladen ved sign-on på tværs af domæner. Multi-domæne situationer vil i sundhedsvæsenet fx opstå, hvis forskellige sygehuse etablerer hver deres sign-on server og –løsninger. En imødegåelse af inkompatibilitetsproblemer i denne sammenhæng er at basere løsningerne på de åbne markedsstandarder, herunder SAML og SOAP.

C.2 Integritet og ægthed i data – krav til applikationerne

Et kendt problem ifm. digitale signaturer er, at brugere ved signering af data eller funktioner signerer, hvad de ”kan se”. En (ondsindet) applikation kan principielt snyde brugeren ved at lægge skjult information eller skjulte handlinger ind under signaturen, uden at brugeren har mulighed for at opdage det. Ligeledes vil en hacker kunne ændre på skjulte data (skjult for øjet, fx detaljer i et billede), som signeres, uden at brugeren ved det.

For at undgå sådanne kompromitteringer af dataintegritet og –ægthed skal det sikres, at applikationerne i sundhedsvæsenet dels er sikret i tilstrækkelig grad mod uautoriseret indtrængen og brug og dels er konstrueret, så data og funktioner er ”ægte”, dvs. fremstår som det de er, og som det de præsenterer sig for til brugeren. Normalt vil applikationer altid konstrueres, så dette er tilfældet, men det vil være relevant at fokusere på særligt følsomme data og funktioner, hvor ægtheden skal sikres i stærkere grad end normalt.

En af de mekanismer, som kan være nyttige at benytte ved sikring af ægthed og integritet, er ved behandling af særlige følsomme eller kritiske funktioner at bede brugeren om at bekræfte sin signatur (med PIN-koden, forudsat at hw-token allerede er tilgængelig, fx i form af et chipkort i kortlæseren på brugerens pc). En tilsvarende facilitet er kendt fra hjemmebanksystemer, hvor brugeren bedes bekræfte hver eneste pengeoverførsel i et særligt skærmbillede med de indtastede data.

BILAG D EKSEMPEL PÅ LRA WEB-TJENESTE (OCES)

Nedenstående skærbillede viser et eksempel på, hvorledes en LRA-administrators web-adgang til certifikat-administration hos en CA kunne tænkes at se ud. Skærbilledet er blot et eksempel og skal ikke tages som et præcist udtryk for de funktioner, som tilbydes LRA-administratorer ifm. OCES-certifikater (kilde: TDC).

The screenshot shows the 'weblRA' web application in a Microsoft Internet Explorer browser window. The user is logged in as 'Bruger: WEBLRA Testbruger 3' with the company 'Firma: TDC Internet Pro Advo Service// CVR:14773908'.

Detaljer om bruger

Navn	Systemnavn	Email	Gruppe	Udstedt ?
Testbruger nummer 1	cn=Testbruger nummer 1+serialNumber	jame@tdcinternet.dk	TESTBRUGERGRUPPE	1

Status på certifikat

Status	Gyldigt fra	Gyldigt til
SPERRET	2002-09-11 21:38:46	2003-09-11 22:08:46

Status for korrespondance

Type	Skabelon	Status	Tid	Ekstra info
EMAIL	All URL encoded mail	AFSENDT	2002-09-09 11:30:43	afleveret til
PINKODE BREV		VENTER	2002-09-09 11:30:41	sendt til Testbruger nummer 1

weblRA

- Returnere til søgefunktion.
- Viser alle brugerens "bevægelse" mht. udlevering af PIN-koder og oprettelser af certifikater.
- Giver mulighed for at angive ny e-mail adresse.
- Giver mulighed for at angiver ny post adresse.
- Kan flytte brugere til anden gruppe.
- Spærre brugerens certifikat.
- Fjerner bruger (når certifikat er spærret).
- Opstøder nye koder (nyt certifikat) til bruger.

Tilgængelige værktøjer for operatøren

BILAG E OMKOSTNINGSELEMENTER OG ØKONO- MI

Tabellerne nedenfor giver en oversigt over forventede omkostningselementer – dels for et sygehus og dels fælles for sundhedsvæsenet. Hvert af omkostningselementerne er klassificeret som hhv. varer eller tid og estimeret mht. antal og pris.

Omkostningselementer for et sygehus

Initielt	Varer	Tid	Antal	Est. omk.	Kommentarer
Etablering af lokal LRA-fkt. (PC)	1 PC m. kortlæser (10 kkr + 2 kkr)	1 dg	1-2 arb.pladser	12 - 24 kkr 1-2 dg.	Denne pris kan reduceres, hvis eksisterende arbejdspladsudstyr kan benyttes
Uddannelse af LRA-adm.		1 dg.	2-5 pers.	2-5 dg.	
Eventuel deltagelse i standardisering af roller og adgangsrettigheder		(X)		0 - 3 mdr.	Er ikke et krav til det enkelte sygehus
Oprettelse af lokale stamdata og funktionsdata i brugerkataloget		X		3-12 mdr.	Kan være meget omfattende - et antal person-mdr
Uddannelse ifm. brugen af brugerkataloget		1 uge	5-10 pers.	5-10 uger	Deltagere er IT-folk, systemejere og sikkerhedschef Der medgår tid til konceptfastlæggelse for sygehuset
Anskaffelse af kortlæsere til PC'er	0,5 kkr. pr. PC			Fx. 125 tkr.	Disse kortlæsere er kun til læsning (ej skrivning). Vurdering for 250 pc'er.
Evt. opgradering af PC'er	0				Bør indgå i løbende opgradering af IT-udstyr
Anskaffelse og opsætning af (lokal) sign-on server	HW 100 kkr. SW 300 kkr.	X		400 kkr. 3-6 mdr.	Arkitektur og evt. fælles server for flere sygehuse bør vurderes. Der kan være besparelser på 50% på SW+HW ved at flere sygehuse benytter samme server.

For hver applikation	Varer	Tid	Antal	Est. omk.	Kommentarer
Definition af applikation i brugerkataloget		2 dage/appl.	10 appl.	20 dage	
Definition af applikation i (lokal) sign-on server		0,5 dag/appl.	10 appl.	5 dage	
Applikationsunderstøttelse af certifikatbaseret autentificering		X		X mdr.	Skal vurderes for hver af de eksisterende applikationer. Der vil formentlig være tale om dels en minimumsløsning og dels en mere grundig revision, hvor appl. får fuld understøttelse af certifikatet, herunder signering af specifikke funktioner. Kan være meget omfattende for ikke-web-baserede applikationer (omskrivning af applikation).
Understøttelse af fortrolighed med brug af servercertifikat(er) (ikke en ny opgave)	Server-certifikat	X			Indgår allerede i applikationsudvikling

Løbende	Varer	Tid	Antal	Est. omk.	Kommentarer
Udførelse af LRA-opgaver (jf. rapporten)		1 t./dag		2 mdr./år	For et mellemstort eller stort sygehus.
(Lokal) sign-on server, licenser og vedl.	HW 10 kkr. SW 60 kkr.			70 kkr./år	
Anskaffelse af chipkort til midlertidige certifikater	20-50 kr. pr. kort (afh. af mængde)			<10 kkr./år	Der regnes med 50 kr. pr. kort og en forventet levetid på 1 år pr. kort (for midlertidige kort). Den estimerede omkostning svarer til at der permanent er 100 midlertidige kort i omløb på sygehuset.
Uddannelse af medarb.		X			Bør indgå i det normale uddannelsesforløb for alle medarbejdere
Definition og vedligeholdelse af medarb. i brugerkataloget		0,5 person		6 mdr./år	For et mellemstort eller stort sygehus.

Omkostningselementer fælles for sundhedsvæsenet

Initielt	Varer	Tid	Antal	Est. omk.	Kommentarer
Udvikling af koncept		X		1000 kkr. 12-24 mdr.	Der vil være behov for såvel udvikling af koncept, standardiseringsindsats, evaluering ifm. pilotprojekter og udarbejdelse af vejledninger igennem en længere migreringsperiode over nogle år. Der vil også være behov for at inddrage ekstern assistance.
Oprettelse af certifikater inkl. første års abonnement	(TDC OCES priser)	X	35.000 sh-professionelle	3500 kkr.	Anskaffelse af certifikater til 35.000 sundhedsprofessionelle.
Oprettelse af LRA inkl. første års abonnement	(TDC OCES priser)	X		0 kr.	Inkluderet i ovennævnte.
Etablering af løsning for lokale LRA-administratorer inkl. procedurer og uddannelse		X		6-12 mdr.	Omfatter aftaler og samarbejde med TDC
Etablering af brugerkataloget inkl. procedurer, uddannelse mv.	HW 200 kkr. SW 4000 kkr.	X		4200 kkr. 12-24 mdr.	Tilgængelighedskravene til det centrale brugerkatalog er meget høje, hvilket gør løsningen dyr. SW-prisen omfatter såvel basissoftware (database) som katalogudvikling (den største post) og tilpasning.
Standardisering af roller, adgangsrettigheder og medarbejderopl.		X		12-24 mdr.	Vil strække sig over en lang kalenderperiode, formentlig i størrelsesordenen 3-5 år.
Koordinering med lokale parter		X		6-12 mdr.	Bl.a. vedr. standardisering.
Standardisering af IT-løsning for dig.sign.	(X)	X		6-12 mdr.	Såfremt der initieres udvikling af specialløsninger, vil der på dette område også indgå omkostninger til systemkomponenter (HW og/eller SW). Dette bør dog minimeres, idet standardprodukter bør foretrækkes.

Løbende	Varer	Tid	Antal	Est. omk.	Kommentarer
Udførelse af LRA-opgaver (jf. rapporten)		X			
Abonnement for certifikater	(TDC OCES priser)		35.000 sh-professionelle	800 kkr./år	For 35.000 sundhedsprofessionelle
LRA abonnement	(TDC OCES priser)			0 kr.	Inkluderet i ovennævnte.
Nye certifikater	(TDC OCES priser)		2000/år	160 kkr./år	80 kr. pr. bruger for første år. Estimeret 2000 nye brugere pr. år
Anskaffelse af chipkort til sundhedsprofessionelle	20-50 kr. pr. kort (afh. af mængde)			1000 kkr.	For 35.000 sundhedsprofessionelle (pris ca. 30 kr. pr. kort)
Uddannelse af medarb.		X			Bør indgå i det normale uddannelsesforløb.
Vedligeholdelse af koncept		X			Der vil gå en årrække før der er tale om ren vedligeholdelse af konceptet.
Registrering og statistik		X		6 mdr./år	Sv. til en halvtidsopgave.
Løbende koordinering med og support til lokale LRA'er		X		6 mdr./år	Indsatsen vil være størst i de første år og kan derefter forventes at falde.
Licenser og vedligeholdelse af brugerkataloget	HW 40 kkr. SW 500 kkr.			540 kkr./år	
Drift af brugerkataloget	500 kkr.			500 kkr./år	