
OCES digital signatur i sundheds sektoren (amtslig perspektiv)

Indledning	2
Digital Signatur udfordringer	2
Administration	3
Udstedelse (og opbevaring)	4
CD Kort signatur	5
USB og smartcard signatur.....	5
Anvendelse	6
TDC smartcard server.....	7
Administrative fordele ved implementation af TDC smartcard server.	8
Øvrige funktionalitetsønsker.....	10
Straks udstedelse af signatur	10
Automatisk godkendelse af brugeroprettelser	11
Bilag 1: Sikkerhedskrav.....	12
Administration af certifikater.	14
Manuel godkendelse af brugerændringer via. TDC's LRA applikation	14
Automatisk godkendelse af brugerændringer	15
Revisionsspor og historik.....	15
Administration af privilegerede brugere.....	15
Sikkerhed af brugerautentifikation.....	15
Udstedelse, opbevaring og anvendelse af nøgler	15
Udstedelse	15
Opbevaring	15
Anvendelse.....	16

Indledning

I forbindelse med udrulning af OCES Digital Signatur til medarbejdere i sundhedssektoren (under amterne) har der rejst sig en række juridiske og tekniske spørgsmål. Disse spørgsmål/problemformuleringer bliver behandlet i en projektgruppe under Amtsrådsforeningen og har bl.a. resulteret i, at en arbejdsgruppe er i færd med at afsøge mulige brugbare løsninger til brug i sektoren.

Dette dokument præsenterer resultatet af TDC's analyse med tilhørende oplæg til produktudvikling hos TDC.

Digital Signatur udfordringer

Der er tre overordnede projektførøb i forbindelse med udrulning af OCES medarbejder certifikater man nøje bør overveje:

1. Administration/oprettelse af medarbejdere, som skal have en Digital Medarbejder signatur – (oprettelse, spærring, etc.)
2. Udstedelse/installation af den enkelte medarbejders signatur
3. Anvendelse af medarbejder signaturer

De tre områder indeholder hver især såvel juridiske som tekniske aspekter, som kan have indflydelse på de endelige implementeringer og dermed også omfanget af henhv. Implementering, vedligehold og administration.

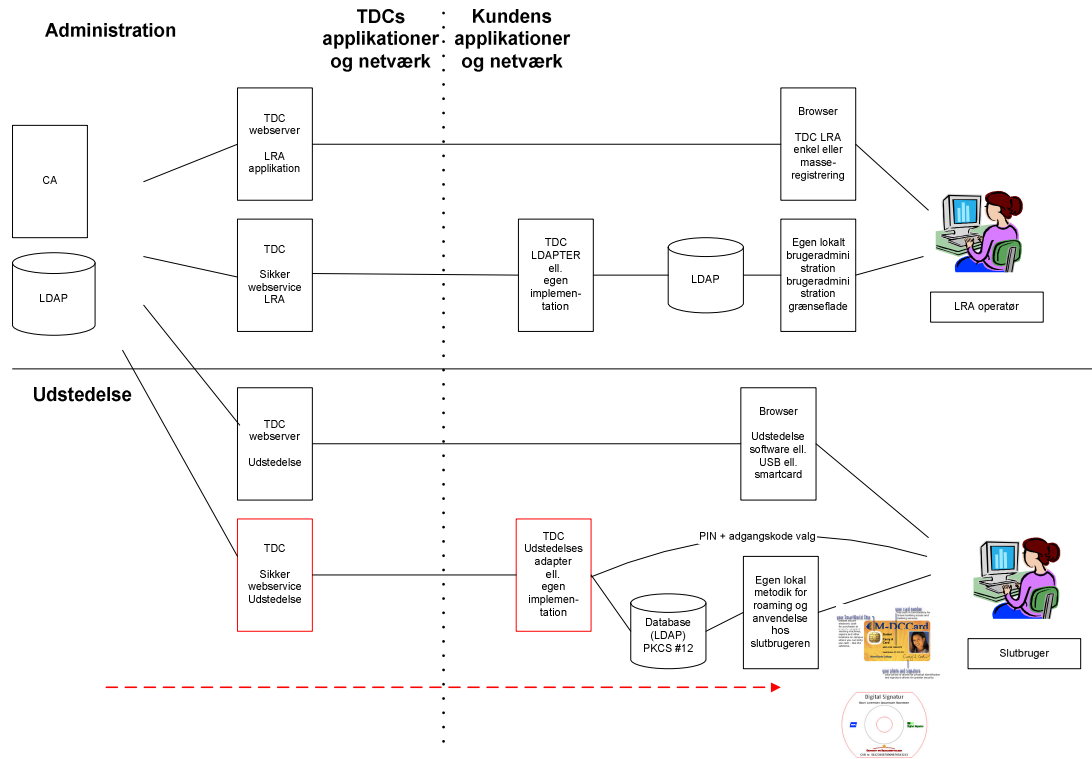


Fig: Illustration af de nuværende og fremtidige løsninger til administration og udstedelse af signatur.


Administration

Der findes tre løsninger til administration af medarbejdere (brugere) der skal have eller har signatur.

- Et browserbaseret interface, hvor medarbejdere oprettes i et web interface (standard i LRA Pro)
- Via en komma separeret fil (eller XML fil format) også kaldet masse registrering (standard i LRA Pro)
- Automatisk online forbindelse mellem et eksisterende brugeradministrations system (eks. løn og personale system) og de systemer hos OCES CA'en (TDC), der håndterer selve signaturanmodningen. Der er 2 varianter af denne ydelse:
 - Via et webservice interface, hvor organisationen selv udvikler de applikationer/moduler, der på baggrund af det dokumenterede interface forestår opsamling og kommunikation med TDC CA via omtalte webservice interface
 - TDC har udviklet en applikation til opsamling og kommunikation med TDC CA, der installeres i netværket hos kunden. Denne applikation kan konfigureres via et XML filter som matcher bruger oplysninger til signatur administration mellem kundens systemer og TDC CA udstedelses systemer.

Udstedelse (og opbevaring)

Udstedelse er den proces, hvor selve signaturen bliver udstedt/installeret. Hertil kræves dels et reference nummer, der sendes via e-mail til signatur modtageren, og dels en engangs pinkode (8 cifre). Når disse 2 elementer anvendes mod TDC's CA udstedes selve medarbejder signaturen. Standard metoden herfor i dag er via en web applikation som installerer selve signaturen direkte på den computer medarbejderen aktuelt benytter eller direkte på et smartcard eller en USB eToken. Fordelen med smartcard eller USB eToken er mobilitet og øget sikkerhed.

Strategi	Karakteristika	Forudsætninger	Løsningens komponenter
Standard signatur installation	Medarbejdere har én eller få faste PC som de arbejder ved hver dag.	Installation af signatur fast på PC'erne. Manuel kopiering af signatur til de pågældende PC'er. Administrator rettigheder ved installation af CSP software på PC'en (evt. distribution af denne software fra centralt hold).	Administration via. TDC LRA eller via. eget administrativt system. Traditionel software udstedelse.
Citrix/NT Roaming signatur	Medarbejderne skifter imellem et større antal arbejdsstationer, men arbejder typiske på én arbejdsstation så lang tid, at man har tid til at logge på som bruger af PC og netværk	Citrix eller NT roaming implementeret i virksomheden. Der findes en vejledning i op-sætning af f.eks. Citrix,  11404_Digital Signatur.pdf (53... men ellers er det typisk noget ens teknologileverandør eller konsulenthus bør hjælpe med at planlægge.	Administration via. TDC LRA eller via. eget administrativt system. Traditionel software udstedelse imens brugeren er logget på som roaming bruger.
CD kort signatur	Medarbejderen bruger kun signaturen til logon, ved brug indlægges CD kort i CD bakke. Signaturen opbevares fysisk af medarbejderen selv	CD Rom læser i PC (ikke slot/slide in). Logon applikationer understøttende CD kort applet logon.	Administration via. TDC LRA eller via. eget administrativt system. Færdigproduceret CD kort fremsendes til medarbejderen.
USB/smartcard	Mange arbejdspladser evt. forskellige organisationer. Høj sikkerhed og fuld funktionalitet af signaturen.	PC'erne skal have de drivere der passer til hardware (og for kortenes vedkommende også kompatible læsere).	Administration via. TDC LRA eller via. eget administrativt system. Udstedelse i "blank" hardware lokalt eller færdig produktion (med billede) hos TDC med efter-

			følgende fremsendelse til slutbrugeren.
Speciel lokal roaming/ sikkerheds- kopi- løsning	Specielle applikatio- ner eller netværk, customiserede an- vendelser	Specialudvikles af kundens egen organisation.	Administration via. eget administrativt system. Udstedelse i lokalt cen- tralt directory via. lokal PIN/adgangskode dialog.

CD Kort signatur



CD kort signaturen leveres på en lille CD Rom, som lægges i CD Rom læseren når signaturen ønskes anvendt.

USB og smartcard signatur

USB med kryptochip, således at den private signeringsnøgle aldrig forlader denne USB, signaturen genereres altså på selve USB'en.



Smartcard med kryptochip, således at den private signeringsnøgle aldrig forlader kortet, signaturen genereres altså på selve kortet.



Anvendelse

Anvendelse af medarbejder signatur i sundhedssektoren er primært fokuseret på logon (adgangskontrol til web applikationer). Der er overordnet 3 anvendelse områder, hvor medarbejder signatur er oplagt som sikkerhedskomponent:

- a. Sikker e-mail hvor en medarbejder via en S/MIME kompatible e-mail klient (typisk Outlook, Notes eller Groupwise) får mulighed for at sende og modtage fortrolige oplysninger (signering og kryptering). De fleste offentlige myndigheder anvender de såkaldte eDag2 løsninger hertil og ikke den enkelte medarbejder signatur.
- b. Logon til adgangskontrol til bl.a. web applikationer, VPN, netværk, singel sign on, etc. Den mest benyttede standard til logon er SSL med klient autentificering.
- c. Dokument og transaktionssignering bygger på ikke eksisterende standarder og kræver som oftest den samme klient/komponent i såvel afsender som hos modtagende applikation.

Ens for de 3 nævnte anvendelsesområder er, at de applikationer (Outlook, Browser, etc.) der understøtter brugen af digital signatur naturligvis skal kunne tilgå selve signaturen. Findes signaturen ikke installeret lokalt på PC'en, forudsættes det at applikationen kan "fremfinde" signaturen på anden vis. En mulig løsning på denne problematik er gennem brugen af smartcards eller eToken, hvorpå selve medarbejdersignaturen ligger.

En anden løsning er central opbevaring af signaturen og en tilhørende lokal roaming løsning, her illustreret med TDC smartcard server, en løsning, som TDC ønsker at produktudvikle specielt til sundhedsområdet, som alternativ til de enkelte institutioners egenudvikling af tilsvarende løsninger.

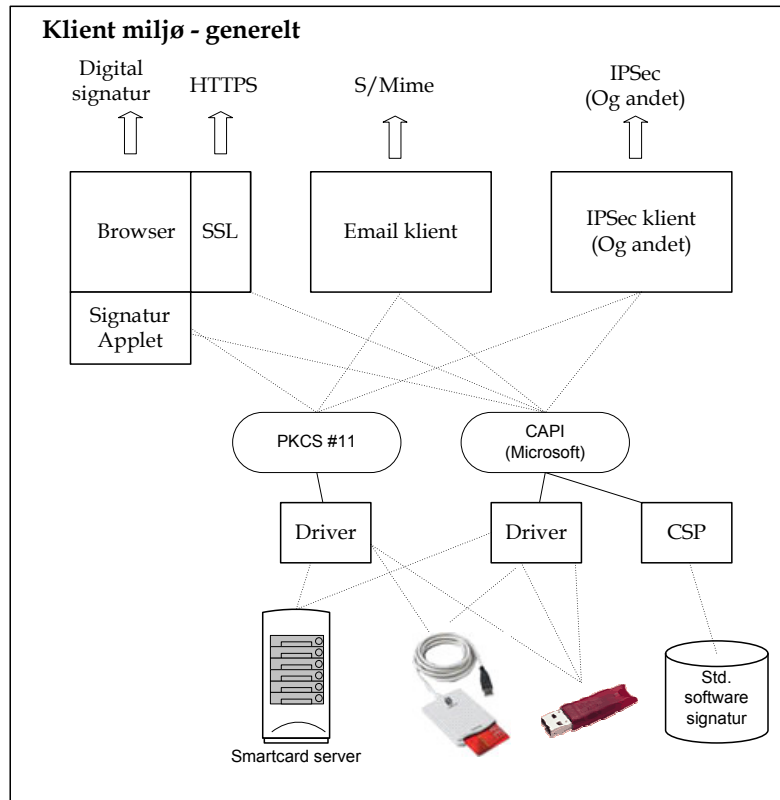


Fig: Generel arkitektur i klient miljøet. På Microsoft operativsystemer er CAPI primær grænseflade imens PKCS #11 er en generel grænseflade, oprindelig udviklet til smartcard, som primært anvendes af ikke-Microsoft applikationer (Netscape, Mozilla, etc.) eller ikke-Microsoft operativsystemer.

TDC smartcard server

Ud fra de ønsker og behov amterne har fremlagt i pilotforløbet har TDC identificeret et produkt, som TDC vurderer kan videreudvikles til et prisbilligt og funktionelt alternativ til distribution af hardware enheder til slutbrugerne.

Det videreudviklede produkt har fået arbejdstitlen *TDC smartcard server*, og bygger på et produkt oprindeligt udviklet af de danske krypteringseksperter Cryptomathic. TDC produktudvikler og implementerer smartcard server i samarbejde med Cryptomathic.

I forhold til anvendelsen af signatur i de enkelte applikationer som Browsers og mailklienter fungerer smartcard server på samme måde, som et personligt smartcard, som brugeren har stukket i en lokal kortlæser. Billedlig talt er "ledningen til smartcard'et bare lidt længere". Smartcard serveren har ikke enkelte personlige smartcards, men i stedet en krypteringshardware enhed som giver smartcard sikkerheden for alle brugere på én gang.

På den enkelte arbejdsstation installerer man en lokal sikkerhedssoftware kaldet SDC (signer desktop client). Det er denne software, som den lokale applikation kalder, når der er behov for digital signatur. Denne software afvikler al kommunikationen med smartcard server.

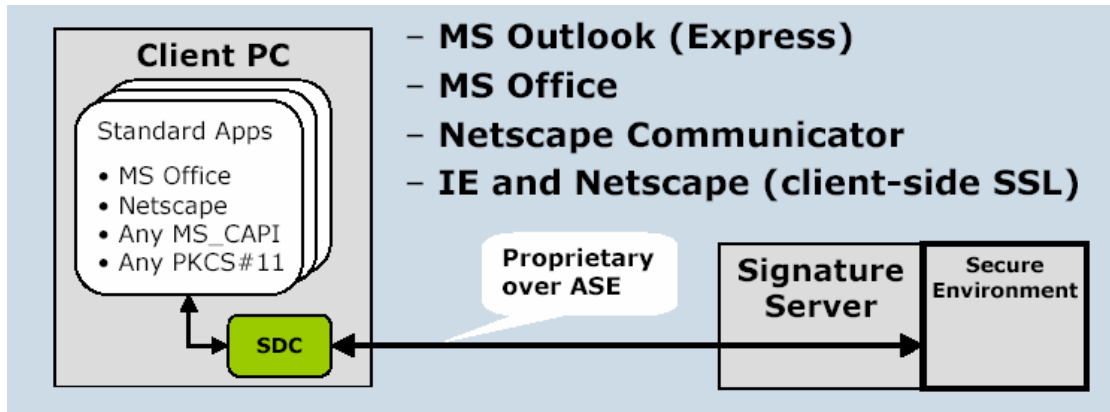


Fig: Smartcard server, anvendelse af signatur i lokale applikationer.

Administrative fordele ved implementation af TDC smartcard server.

Ved implementation af smartcard server står denne server for både nøglegenerering og nøgleopbevaring ifbm. den daglige anvendelse af digital signatur i organisationen.

Der er følgende fordele ved denne centrale mekanisme for udstedelse og opbevaring af digital signatur for medarbejderne i amtet.

- Digital signatur er tilgængelig alle arbejdspladser, som har SDC klienten installeret, og som netværksmæssigt hænger sammen med smartcardserveren. (For at opretholde to-faktor sikkerhed omkring OCES digital signatur, er smartcardserveren nødt til at være en del af et kontrolleret netværk, hvor brugeradgangen er begrænset af andre adgangskontrol mekanismer. Alternativt skal man implementere brug af engangskoder hver gang signaturen anvendes, dette er også en klar mulighed).
- Der er ikke et fysisk token eller smartcard, som brugeren kan glemme, ødelægge eller smide væk.
- Der er høj sikkerhed, idet brugerens private signaturnøgler aldrig forlader smartcard serveren.
- Der er central historik over anvendelse af den enkelte brugers signatur.
- Der er minimalt arbejde med etablering og vedligeholdelse af infrastrukturen, idet signaturen "leveres" direkte til den enkelte applikation fra smartcardserveren.
- Der er understøttelse af mange forskellige lokale applikation ud fra standarderne CAPI og PKCS#11.

Placering af smartcard server – mobilitet

Tænker man på smartcard serveren som en variant af citrix og NT roaming, er det mest logisk at opsætte smartcard serveren i det enkelte amts netværk.

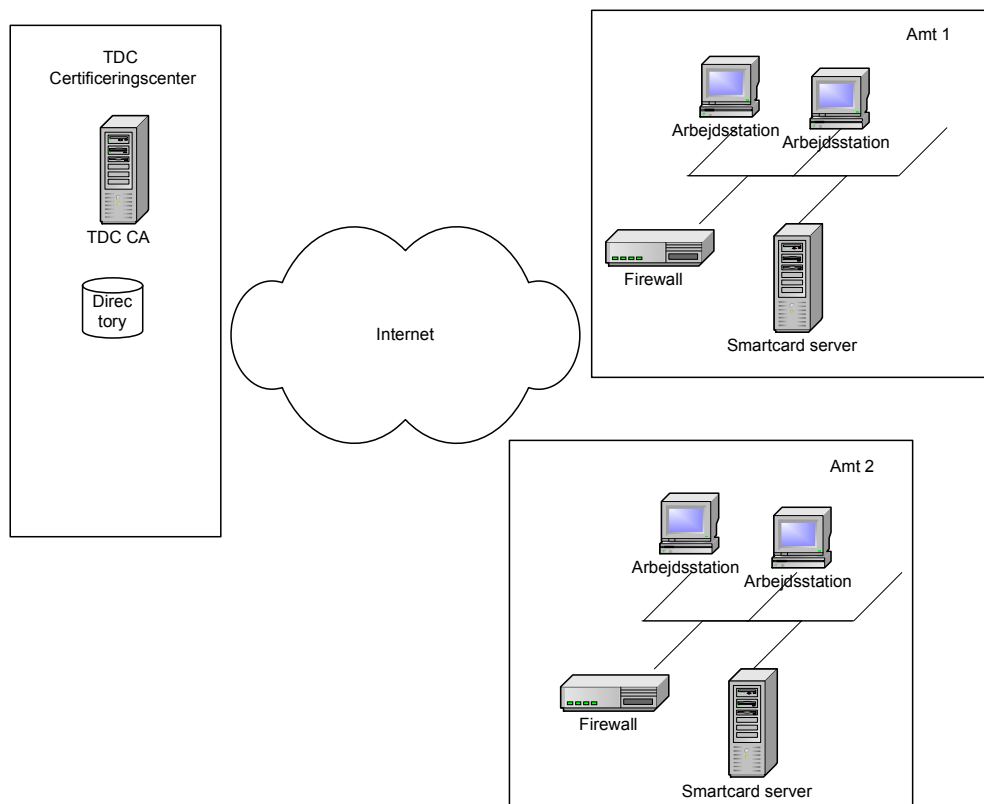


Fig: placering af smartcard serveren lokalt i det enkelte amts netværk

Lokal placering af smartcard server giver dog muligvis problemer ifht. læger og andet personale, som arbejder i flere amters netværk. Såfremt der er flere smartcard servere som skal tilgås fra de samme arbejdsstationer bliver der en forøget kompleksitet omkring brugerlogon.

Såfremt man kan finde en sikkerhedsmæssigt tilfredsstillende netværksopkobling til en centralt placeret server, ville dette give den største brugervenlighed ifht. mobilitet og brugeroplevelse.

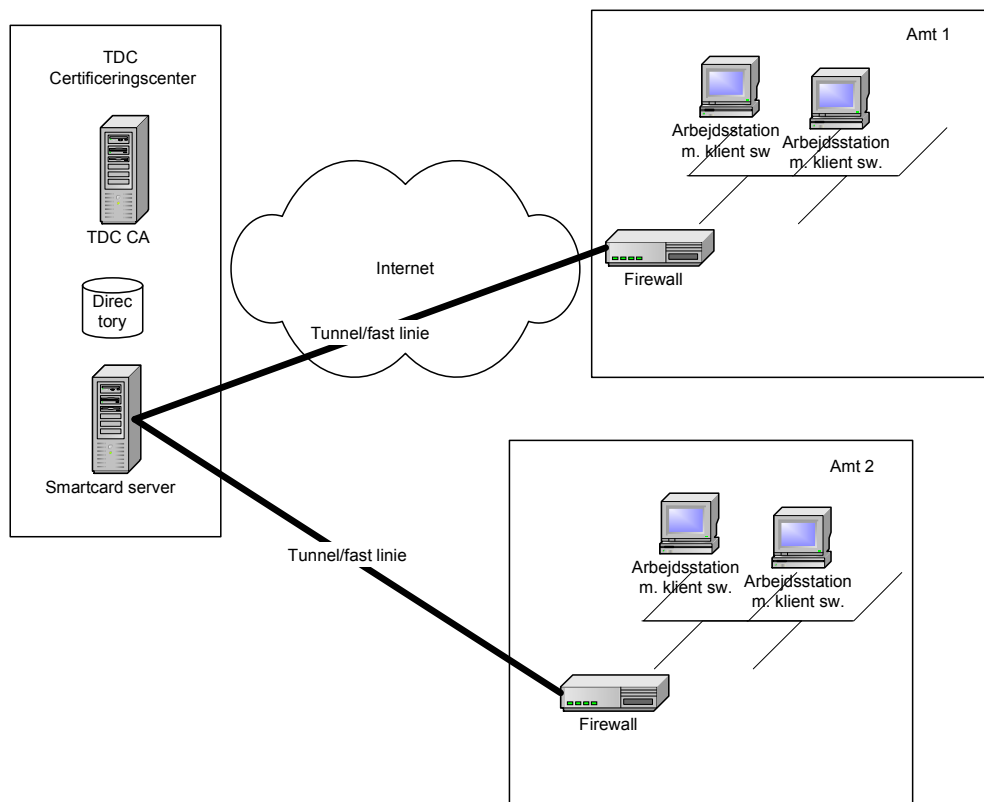


Fig: Smartcard server placeret centralt, tilgængelig fra alle amtsnetværk

Omkring selve sikkerhedsdiskussionen, som nok er den vigtigste ifht. arkitekturvalg, er der også mulighed for at overgå til engangskodeløsninger, således at afhængigheden af lukkede netværk kan elimineres. Engangskodeløsninger vil dog være dyrere at etablere og administrere og desuden give en mere knudret brugeroplevelse.

Øvrige funktionalitetsønsker

Udover de ovenfor skitserede produktudviklinger hos TDC, vil TDC arbejde på følgende områder

Straks udstedelse af signatur

Der arbejdes efter at en LRA administrator kan se PIN kode i LRA applikationen og overdrage denne direkte til brugeren, evt. med brugerens udstedelse og indlæsning i smartcard på stedet. TDC beskriver overfor IT- og Telestyrelsen konceptet som skal indmeldes til datatilsynet. Straks udstedelse vurderes at være den korrekte anvendelse til midlertidige medarbejdere fremfor tidsbegrænsede signaturer.

Automatisk godkendelse af brugeroprettelser

TDC beskriver udfra OCES certifikatpolitikken hvilke sikkerhedskarakteristika et administrativt system skal opfylde for at man kan undgå at en administrator eksplicit godkender og underskriver oprettelser af brugere.

Bilag 1: Sikkerhedskrav

OCES certifikatpolitikkerne (<https://www.signatursekretariatet.dk/certifikatpolitikker.html>) angiver sikkerhedskrav som TDC og Amterne skal overholdes ved implementation af komponenter til brug for administration, nøglegenerering og nøgleanvendelse hos et amt. TDC har udviklet en brugeradministrationsapplikation (LRA applikation) som sammen med TDC's "Forretningsbetingelser for oprettelse som Lokal Registrerings Enhed for medarbejdercertifikater" (<http://www1.certifikat.dk/repository/ForretningsbetingelserOCES.doc>) sikrer at TDC overholder de krav der har med registrering af certifikatholdere at gøre. TDC har desuden udviklet en udstedelsesmekanisme (udstedelses website) og en nøglegenererings- og opbevaringskomponent (TDC CSP), som sammen med TDC's vilkår for anvendelse af OCES certifikater" (http://www1.certifikat.dk/repository/Terms_and_conditions_OCES.pdf) sikrer, at TDC overholder de krav der har med nøglegenerering, -opbevaring og -anvendelse at gøre.

TDC er ansvarlig for alle krav udledt af OCES CP. Såfremt nedenstående liste over særlige krav organisationens løsning skal opfylde ikke er dækkende, er det OCES certifikatpolitikens krav der er gældende.

Det er TDC's ansvar dels at forsikre sig om, at organisationen vil være i stand til at leve op til sikkerhedskravene inden idriftsættelse, dels at følge op på efterlevelsen efterfølgende, evt. via revision.

Herunder gives udpluk fra OCES medarbejder certifikat politik 3.0. Den fulde tekst er tilgængelig på adressen: <https://www.signatursekretariatet.dk/certifikatpolitikker.html>

6.2 Certifikatindehaverens forpligtelser

CA skal ved aftale forpligte certifikatindehaveren til at sikre, at certifikatholder opfylder følgende betingelser:

- *at give fyldestgørende og korrekte svar på alle anmodninger fra CA (eller RA) om information i ansøgningsprocessen*
- *at generere, opbevare og anvende nøglepar som anvist af CA. Den private nøgle kan opbevares på harddisk, diskette eller lignende*
- *at tage rimelige forholdsregler for at beskytte den private nøgle mod kompromittering, ændring, tab og uautoriseret brug*
- *at beskytte den private nøgle med en aktiveringskode, der mindst består af 8 tegn og indeholder mindst et lille og et stort bogstav samt et tal*
- *anvendelse af anden aktiveringskode – f.eks. biometrisk – skal have en kompleksitet på mindst 128 bit*
- *aktiveringskode i miljøer, der effektivt kan spærre for udtømmende søgninger, kan dog være minimum fire cifre*
- *at beskytte aktiveringskoden, så andre ikke får kendskab til den*
- *at en evt. sikkerhedskopi af den private nøgle skal opbevares i krypteret form på betryggende vis*
- *ved modtagelse af OCES-certifikatet at sikre sig, at indholdet af OCES certifikatet er i overensstemmelse med de faktiske forhold*
- *alene at benytte OCES-certifikatet og de tilhørende private nøgler i henhold til bestemmelserne i denne CP*

- omgående at anmode den udstedende CA om spærring af OCES-certifikatet i tilfælde af kompromittering eller mistanke om kompromittering af den private nøgle
- omgående at anmode om fornyelse af certifikatet, hvis indholdet af OCEScertifikatet ikke længere er i overensstemmelse med de faktiske forhold

For så vidt angår private nøgler til brug for sikring af fortrolighed (krypteringsnøgler) kan certifikatindehaveren anvise certifikatholderen alternative procedurer til sikring af en fælles kontrol og anvendelse af nøgler. Certifikatindehaveren skal i givet fald informere certifikatholderen om konsekvenserne i forhold til fortrolighed.

Såfremt certifikatholder ikke længere har tilknytning til certifikatindehaver, skal certifikatindehaver omgående meddele CA dette og anmode om spærring af certifikatholderens certifikat.

CA skal desuden orientere certifikatindehaver og certifikatholder om, at den private nøgle anses for kompromitteret og skal spærres, hvis andre får kendskab til aktiveringskoden.

7.3.1 Registrering af certifikatindehaver

CA skal sikre, at certifikatindehaver, inden et OCES-medarbejdercertifikat tages i brug, gøres opmærksom på og accepterer vilkår og betingelser for anvendelsen af certifikatet.

Der er ikke krav om personligt fremmøde i forbindelse med udstedelsen af et OCESmedarbejdercertifikat.

CA skal etablere en procedure for verifikation af ansøgers identitet, der sikrer, at

- certifikatindehaveren angiver virksomhedens CVR-nr.
- OCES-certifikatindehaverens CVR-postadresse indhentes ved online opslag i CVR registeret i tilmeldingsprocessen
- den bemyndigedes engangskode fremsendes via pinkodebrev til virksomhedens ledelse på virksomhedens CVR-postadresse
- OCES-certifikatholderen udstyres med en engangskode fremsendt via pinkodebrev
- processen sker gennem en af virksomheden bemyndiget person, eller efter godkendelse fra en af virksomheden bemyndiget person
- bemyndiget er udpeget og godkendt af virksomhedens ledelse

Det er tilstrækkeligt, at CVR-postadressen verificeres én gang. Hvis virksomhedens adresse ændrer sig, skal CVR-postadressen verificeres på ny.

Såfremt CA på forhånd har kendskab til certifikatindehaverens identitet eller anvender andre betryggende procedurer til at foretage identitetskontrol, kan ovennævnte procedure for certifikatansøgning helt eller delvist fraviges.

Generering og installation af certifikatholders nøgler

Såfremt certifikatholders nøgler genereres hos certifikatholderen, skal CA etablere en installationsprocedure, der teknisk sikrer, at

- certifikatholder skal angive sin engangskode for at starte installation af den private nøgle og tilhørende certifikat
- nøglepar genereres hos certifikatholder
- certifikatholders nøgler er RSA-nøgler med en længde på mindst 1024 bit eller tilsvarende

- den offentlige nøgle overføres til CA sammen med oplysninger i en meddelelse signeret med den private nøgle
- den private nøgle er krypteret og beskyttet af aktiveringskode
- aktiveringskode til aktivering af den private nøgle genereres og indtastes i forbindelse med nøglegenereringen
- den private nøgle er aktiveret, når certifikatholderen har angivet aktiveringskode, der består af mindst 8 tegn og indeholder mindst et lille og et stort bogstav samt et tal
- anvendelse af anden aktiveringskode – f.eks. biometrisk – skal have en kompleksitet på mindst 128 bit
- aktiveringskode i miljøer, der effektivt kan spærre for udtømmende søgninger, kan dog være minimum fire cifre
- rodcertifikatet er installeret hos OCES-certifikatholder
- rodcertifikatet kan verificeres via anden kanal
- tidspunkt og dato for udstedelsen af certifikatet efterfølgende kan fastlægges

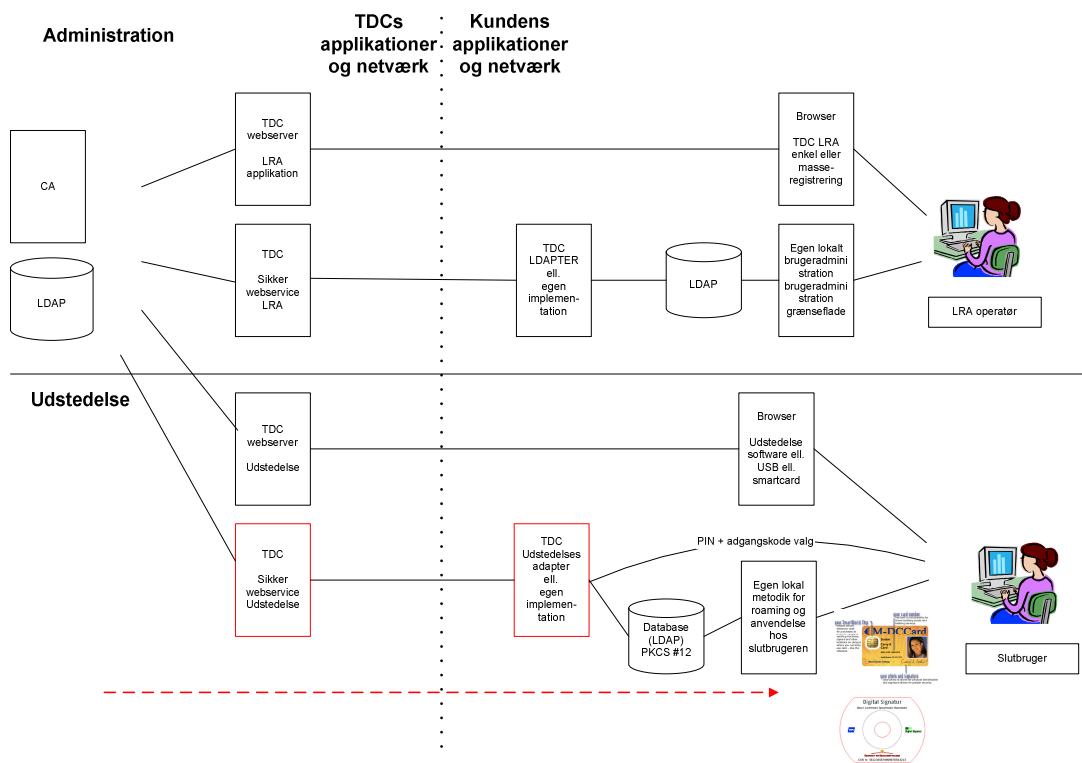


Fig: Illustration af de nuværende og fremtidige løsninger til administration og udstedelse af signatur.

Administration af certifikater.

Manuel godkendelse af brugerændringer via. TDC's LRA applikation

TDC sikrer efterlevelsen af kravene i OCES certifikat politikken dels ved at LRA operatøren anvender TDC's LRA applikation til brugerændringer, dels ved at anvise LRA operatøren " Forret-

ningsbetingelser for oprettelse som Lokal Registrerings Enhed for medarbejdercertifikater” (<http://www1.certifikat.dk/repository/ForretningsbetingelserOCES.doc>).

Automatisk godkendelse af brugerændringer

Såfremt brugerændringer opsamlet via TDC's sikker webservice LRA ønskes udført automatisk, uden manuel LRA operatør accept, skal de brugervilkår, processer og systemer som lokalt opsamler og indsender disse brugerændringer kompensere for den manglende direkte LRA operatør accept, ved at tilfredsstille alternative funktionalitets og sikkerhedskrav.

Revisionsspor og historik.

Ud fra en given brugerændring indmeldt til automatisk behandling på TDC's sikker webservice LRA, skal organisationen på TDC's forespørgsel kunne give et revisionsspor, som viser hvilken operatør, der op til seks år tilbage i tiden bemyndigede den pågældende ændring.

Administration af privilegerede brugere

Organisationen skal beskrive og dokumenterer processen for oprettelse og tildeling af rettigheder til operatører, som kan igangsætte en proces i organisationens systemer, som fører til en automatisk brugerændring på TDC's sikker webservice LRA.

Organisationen skal herunder tilse at forhold beskrevet i " Forretningsbetingelser for oprettelse som Lokal Registrerings Enhed for medarbejdercertifikater" efterleves af organisationens medarbejdere.

Sikkerhed af brugerautentifikation

Organisationen skal beskrive og dokumentere den sikkerhedsløsning som anvendes til autentifikation af brugere overfor de af organisationens interne systemer, som kan anvendes til at autorisere en automatisk brugerændring på TDC sikker webservice LRA.

Udstedelse, opbevaring og anvendelse af nøgler

Udstedelse

Der er i OCES medarbejder certifikatpolitikken kun åbnet mulighed for at nøglegenereringen og dermed udstedelsen af certifikatet kan ske hos udsteder (TDC) eller certifikatholder (medarbejderen). Nøglegenerering lokalt i organisationen kræver altså deltagelse af den enkelte medarbejder. Særlige forhold gør sig dog gældende, hvis nøglerne udelukkende skal anvendes til sikring af fortrolighed og ikke til signering af e-mails, logon og dokumentsignering.

Opbevaring

Opbevaring (herunder sikkerhedskopier) af de private nøgler skal ske i krypteret form under betryggende form. Krypteringen skal være sikret med et password, der ikke må komme til andres end medarbejderens kendskab. Det er organisationens ansvar at sikre, at medarbejderens nøgler opbevares under betryggende forhold. Organisationens skal være særlig opmærksom på disse forhold i forbindelse med løsninger, hvor medarbejdere anvender roamede profiler i terminalbaserede klienter.

Anvendelse

Det er KUN medarbejderen selv, der må anvende den private signaturnøgle. Der gælder dog særlige regler for anvendelse af private nøgler, som udelukkende anvendes til dekryptering af data og ikke til signering af e-mails, logon og dokumentsignering.

Det er organisationens ansvar at sikre, at medarbejdere opfylder betingelserne for opbevaring og anvendelse af medarbejdersignaturen, herunder at medarbejderen kun anvender signaturen på systemer, der ikke er kompromitteret med virus, trojanske heste eller lignende.