
TDCs Signaturserver

Indhold

Indledning	3
Teknisk projekt	3
Tekniske forudsætninger	3
Installation af klienten.....	4
Udstedelse af signatur.....	4
Anvendelse af signaturen.....	6
Eksport af signaturen	7
Skift af bruger.....	8
Start af klienten	9

Indledning

Dette dokument introducerer TDCs Signaturserver.

Teknisk projekt

Alle projekter som involverer Signaturserveren skal igennem nedenstående dele før almindelig drift er etableret:

Trin	Beskrivelse
Aftaleindgåelse	Formel aftaleindgåelse mellem Kunden og TDC omkring den ønskede ydelse.
Kontaktpersoner	Tilknytning af kontaktperson hos TDC til projektet
Netværkskonfiguration	Konfiguration af netværksadgang herunder åbning i TDCs systemet for adgang fra Kundens net, men også åbning i Kundens net for adgang med de relevante protokoller, porte og IP adresser.
LRA konfiguration	Konfiguration af LRA til brug af Signaturserver, herunder tilknytning af unikke brugerid.
Klient Software	Udlevering/Udrulning af nødvendig software på kundens klientmiljøer (.Net framework og TDCs Signaturserver CSP)
Bruger test	Oprettelse af første bruger.

Tekniske forudsætninger

Der er en række forudsætninger for anvendelse af Signaturserveren hos kunden. Udgangspunktet er at kunden ikke skal bruge andre Digital Signatur applikationer end dem der er eksponeret gennem Microsofts Crypto API (CAPI). I den forbindelse skal der installeres en såkaldt Cryptographic Service Provider (CSP) som danner interface mellem Signaturserveren og CAPI. Bemærk at det er en forudsætning for anvendelse af CSPen til certifikat udstedelse at klient PCen er udstyret med Microsofts .Net framework.

Fra kundens netværk skal der være adgang til en webservice hos TDC på tcp port 80 i forbindelse med udstedelsen og i forbindelse med brug skal der være adgang til tcp port 22346.

Endelig skal kundens LRA være sat op til at administrere brugere på Signaturserveren.

Installation af klienten

Komponenten installeres som en standard Windows applikation. Den kan installeres på alle platforme senere end Windows 98.

Det er en forudsætning for anvendelsen at der er åbent for almindelig TCP port 80 og 22346. Det er desuden en forudsætning af Microsoft .Net framework er installeret.

Udstedelse af signatur

Udstedelse er baseret på at en LRA i forvejen har oprettet brugeren og tildelt brugeren et unikt Signaturserver ID. Efter oprettelsen modtager brugeren velkomst e-mail og en PIN kuvert. Herunder er angivet et eksempel på en e-mail:

```
Fra: signatur-autosvar@tdc.dk Sendt: on 12-10-2005 15:20
Til: Niels Frimodt Sørensen
Emne: TDC Digital Signatur for medarbejdere: velkomst e-mail

Kære Bruger
Firma, CVR 12341234

Du har bestilt en Digital Signatur. I denne e-mail kan du læse, hvordan du kommer i gang.

1: Gem denne e-mail, eller print den ud!

2: Om et par dage modtager du en PIN kode med posten. Den skal du bruge til at installere dit medarbejdercertifikat på din computer. I brevet med PIN koden findes også en spærrekode. Gem den! Den skal du bruge, hvis du skal spærre din Digitale Signatur.

3: Når du har fået PIN koden, finder du denne e-mail frem igen, klikker på linket hér, og starter installationen.

https://test.lra.certifikat.tdc.dk/udstedelse/jsp/flexinstall.jsp?RENO=77302542&PIN=46789430&PROVIDER=SMARTCARDSEVER&RID=tdctestbruger

Følg forløbet, og indtast din PIN kode.

Vær opmærksom på, at din PIN kode udløber d. 11/11-2005 kl. 14:19. Installer din Digital Signatur inden da.

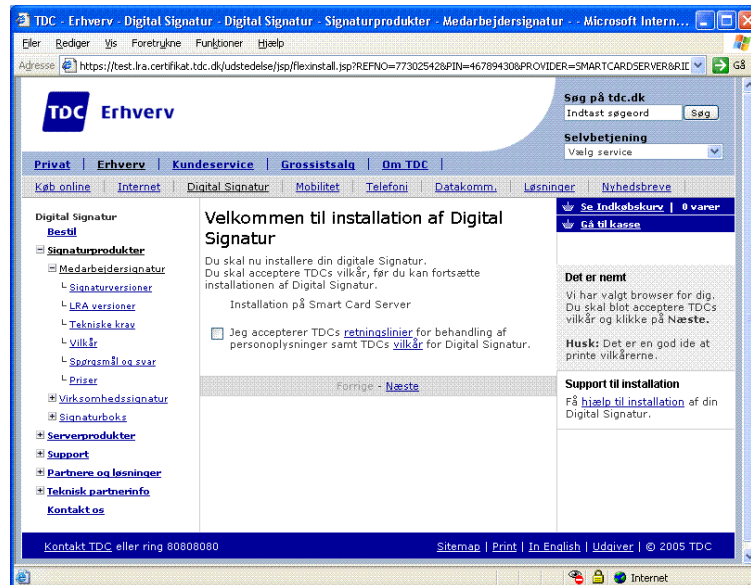
Hvis du får problemer med installation af certifikatet, kan du kontakte din lokale administrator.

Vi håber, du får glæde af Digital Signatur.

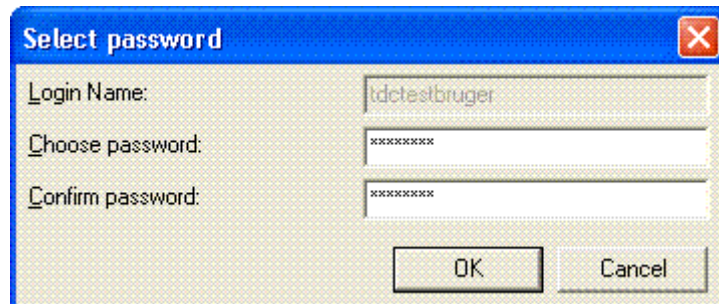
Venlig hilsen

TDC Totalløsninger A/S
```

Brugeren følger linket i e-mail og installationen starter:



Betingelserne skal accepteres og der klikkes næste. (I produktionssystemet promptes man for indtastning af PIN koden – ikke vist her) Herefter promptes brugeren for at vælge og bekræfte sin adgangskode.



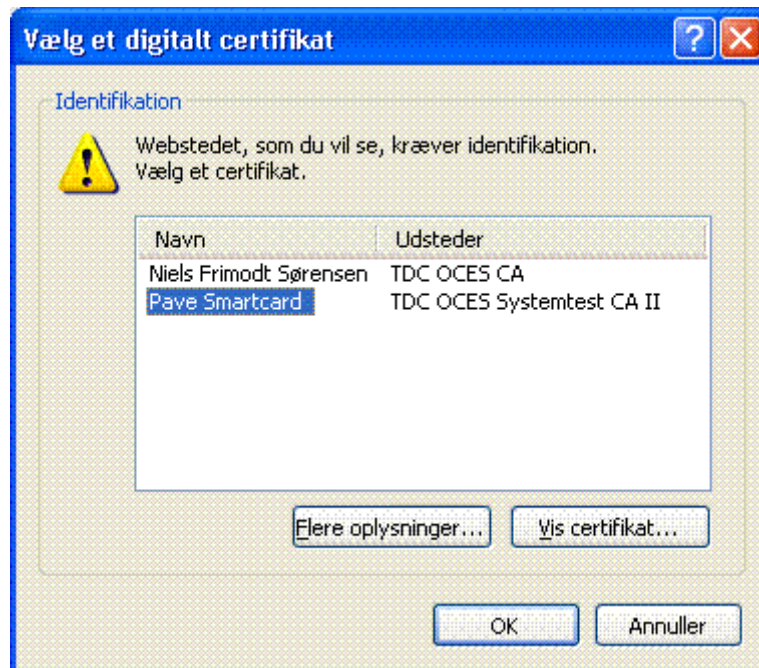
Installationen er tilendebragt og der vises en kvitterings-side



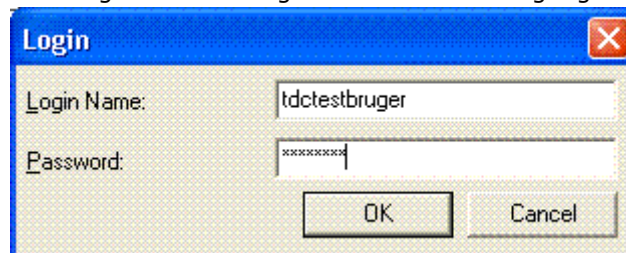
Anvendelse af signaturen

Signaturen kan anvendes i alle sædvanlige scenarier som understøttes af Microsofts krypto-standard CAPI. Herunder er angivet brugeroplevelsen ved SSL klient logon.

Brugeren peger Internet Explorer mod et website der kræver SSL klient logon. Han bliver promptet for at vælge sin signatur:



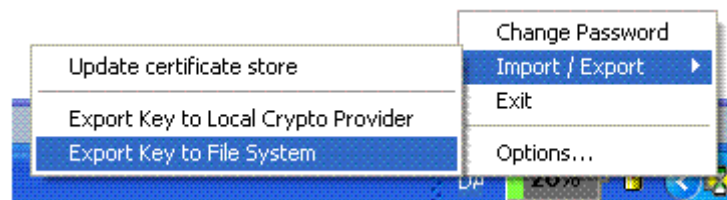
Efterfølgende skal brugeren indtaste sin adgangskode:



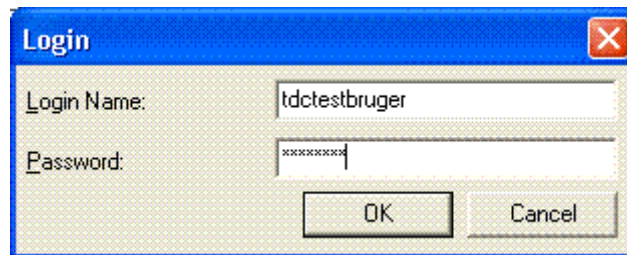
Eksport af signaturen

Hvis signaturen skal anvendes i scenarier der ikke er understøttet af CAPI standarden er der mulighed for at eksportere til PKCS#12 standard filformatet. Proceduren gennemgås herunder:

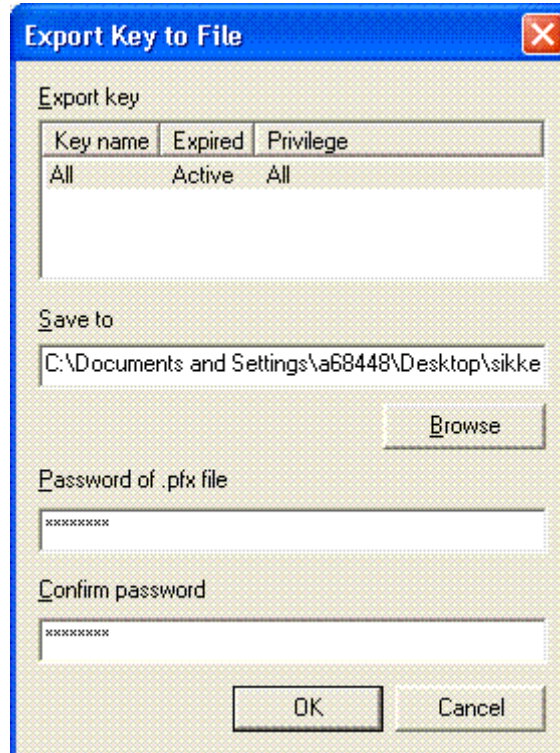
Brugeren højreklikker på Signaturserver ikonet i proceslinien og vælger Export to File:



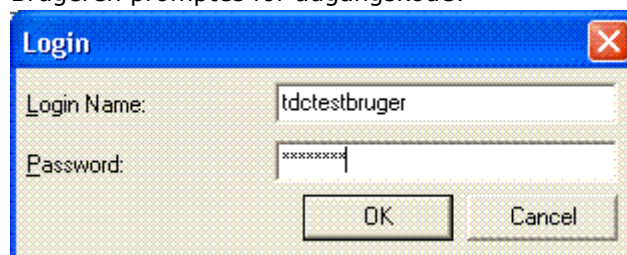
Brugeren promptes for adgangskode:



Brugeren promptes for placering af fil og adgangskode til PKCS#12 filen:



Brugeren promptes for adgangskode:

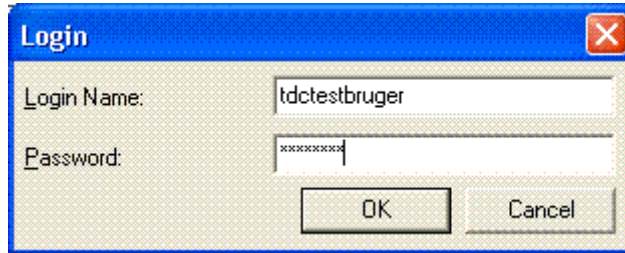


Skift af bruger

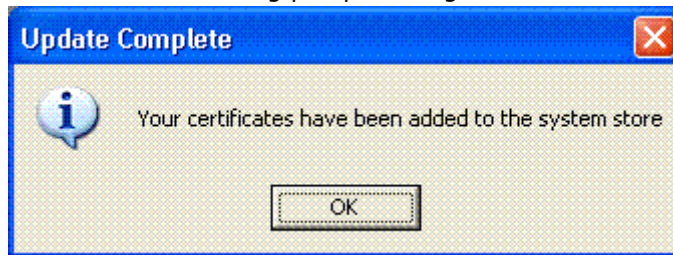
Hvis man kommer til en PC hvorfra en anden bruger senest har brugt Signaturserveren er det nødvendigt at opdatere certifikat store. Dette gøres ved at klikke på Signaturserverikonet i proceslinjen:



Brugeren promptes for brugernavn og adgangskode:



Der vises en kvittering på opdateringen:



Start af klienten

Hvis man ikke har signaturserver ikonet i proceslinien kan den startes fra programmenuen:

