

KOM GODT I GANG

CERTIFIKATER

En trin for trin guide til dig, der skal bestille og konfigurere certifikater

1. Introduktion

I den fælleskommunale infrastruktur anvendes certifikater til [Fælleskommunalt Adgangsstyring for systemer](#) (ADGSYSTEM) og til [Fælleskommunalt Adgangsstyring for brugere](#) (ADGBRUGER). Certifikater anvendes til at sikre parters rette identitet, samt til at etablere sikker kommunikation mellem parterne. De anvendes når et fagsystem integrerer med [webservices](#) og [Fælleskommunal Beskedfordeler](#) (BFO), samt når brugervendte systemer og Identity Providers integrerer med Context Handler. De er således helt centrale for sikkerhedsmodellen i infrastrukturen.

Formålet med denne guide er at give dig en introduktion til de hyppigt forekommende emner ved ibrugtagning, så du kommer hurtigt og godt i gang. Guiden henvender sig primært til leverandører, der skal integrere med den fælleskommunale infrastruktur for første gang.

De første tre afsnit er generelle og beskriver forskellen på de offentlige/private versioner, den anvendte standard, samt hvordan du bestiller. De sidste tre afsnit beskriver specifikt, hvordan du registrerer og anvender et certifikat.

Guiden indeholder følgende afsnit:

1. [Offentlig vs. privat version](#)
2. [Funktionscertifikater](#)
3. [Bestilling hos Nets](#)
4. [Registrering i Fælleskommunalt Administrationsmodul \(ADM\)](#)
5. [Windows Certificate Store](#)
6. [Java Key Store](#)

Du må ikke anvende samme certifikat ved integration til infrastrukturens testmiljø og produktionsmiljø. Du skal i stedet bestille og registrere separate certifikater til hvert miljø. Funktionscertifikater er beregnet til specifikke formål, og du skal derfor anskaffe et dedikeret certifikat til hvert unikke system.

Guiden står ikke alene, men fungerer derimod blot som introduktion til de detaljerede vejledninger, som du finder i Digitaliseringskataloget.

2. Offentlig vs. privat version

Grundlæggende findes certifikater i to versioner; med eller uden en privat nøgle. De anvendes til kryptering, således at afsender er sikker på, at det kun er tiltænkte modtager, der kan læse informationen. Certifikater anvendes ligeledes til signering, således at modtager kan være sikker på, at det var rette afsender, der sendte data.

Indehaver af versionen med den private nøgle kan således læse information, som kun er tiltænkt certifikatets ejer, og indehaver af versionen med den private nøgle kan udgive sig for at være certifikatets ejer og sende information på dennes vegne. Det er derfor kritisk, at du er bevidst om forskellen på de to, samt at du beskytter den private version på behørig vis. Derudover er det vigtigt, at du ikke deler den private version med andre.

Da signering og kryptering foregår i begge retninger ved kommunikation mellem systemerne, skal hver part have registreret modpartens offentlige version af deres certifikater. Det er derfor, du skal registrere den offentlige version i [Fælleskommunalt Administrationsmodul](#) (ADM) for dit anvendelsesystem, brugervendte system eller Identity Provider. For de to sidstnævnte er certifikatet indlejret i SAML-metadata. Du skal registrere infrastrukturens offentlige version af dets certifikater på de systemer, som du kalder fra. Dem henter du i [Digitaliseringskataloget](#).

Hvis du kommer til at dele den private version ved en fejltagelse, skal du straks tilbagekalde den (revocation) og få et nyt udstedt.

3. Funktionscertifikater

Den offentlige standard for certifikater betegnes [OCES-standard](#), som er defineret af Digitaliseringsstyrelsen. Generelt anvendes FOCES, også kaldet funktionscertifikater. Det er også muligt at anvende virksomhedscertifikater (VOCES), men det anbefales at anvende FOCES ved systemintegrationer, da de er beregnet til dette specifikke formål.

4. Bestilling hos Nets

Bestilling af funktionscertifikater foregår via Nets [hjemmeside](#) og kan kun foretages af en NemID-administrator fra virksomheden. Bestilling til test og produktion foretages i separate systemer:

- [Bestilling til produktion](#)
- [Bestilling til test](#)

Når du aktiverer et certifikat, får du udleveret versionen med den private nøgle. Du skal selv angive en adgangskode. Ved aktivering kan du vælge mellem tre formater:



I dette eksempel er valgt PKCS#12 (.p12/.pfx), da det er et generelt format, der fungerer på tværs af platforme. Ved at klikke på "Hent funktionssignatur" gemmer du den private version lokalt. Det er denne, der skal anvendes i koden ved kald til services på infrastrukturen, eller ved opsætning af Brugervendt system og Identity Provider. Husk at notere adgangskoden og gem den sikkert.

Bemærk, at du efterfølgende kun kan hente den offentlige version uden den private nøgle. Hvis du mister versionen med den private nøgle, eller mister adgangskoden til den, skal du anmode om at få et nyt certifikat udstedt.

I selvbetjeningen vælger du "Øvrige signaturer -> Administrér funktionssignatur":

Navn	FID	Kontakt	E-mail	Gruppe	Ret/Slet
TEST bestilling JGM	44815982	Jens Green Most	jgm@kombit.dk	Standard	

Her kan du fremsøge og vælge dit certifikat:



Genudsted signatur

Det er muligt at genudstede signaturen, hvis I har glemt adgangskoden. Genudstedelse betyder, at I udsteder et nyt funktionscertifikat. Prisen er 254,00 kr., som opkræves ved bestilling.

Ja, spær det nuværende certifikat.

2 **BESTIL GENUSTEDELSE** **1**

Offentliggørelse af certifikat

Vis certifikat i offentlig certifikatdatabase. **i** **GEM**

Detaljer om certifikater

Få overblik over de certifikater, der hører til funktionssignaturen:

Udstedt	Navn i funktionssignaturen	Status	Detaljer
29-05-2020 10:10:40	TEST bestilling JGM (funktionscertifikat)	UDSTEDT	Skjul
	Udløbsdato: 29-05-2023 10:08		
	Udstedt af: TRUST2408 Systemtest XXXIV CA		
	Serienummer: 1558771465		

[Spær certifikat](#) [Hent certifikat](#) **4** **3** **TILBAGE**

1. Her kan du bede om genudstedelse, hvilket genererer en ny version med ny udløbsdato.
2. Du kan ved genudstedelse samtidigt anmode om at få det gamle spærret.
3. Her henter du den offentlige version.
4. Du kan også vælge blot at spærre det nuværende certifikat.

Certifikaterne udløber automatisk ved udløbsdatoen og kan ikke benyttes herefter. Når man genudsteder et certifikat, så udstedes der en ny "version" af certifikatet, så begge certifikater er aktive på samme tid. Dette giver dig mulighed for i god tid at skifte certifikatet, inden det gamle udløber. Det gamle certifikat kommer således ikke automatisk på revocation-list, med mindre man specifikt anmoder om dette, i stedet udløber det blot.

Den offentlige version hentes som en CER fil (.cer) i PEM-format. Det er denne, du skal registrere på dit anvendelsesystem i ADM. I tilfælde af brugervendt system eller Identity Provider, da vil du efter lokal konfiguration med det private certifikat kunne udtrække SAML-metadata som har den offentlige version indlejret. Det er således SAML-metadata-filen du registrerer i ADM.



5. Registrering i Fælleskommunalt Administrationsmodul (ADM)

Når du har modtaget dit certifikat, skal den offentlige version registreres i ADM ([test](#) eller [produktion](#)). Hvis du skal integrere med webservices eller Beskedfordeler, skal certifikatet registreres på Anvendersystem. Her trækker du blot certifikatet (.cer/.pem) ind i boksen med den stiplede linje og klikker på ”Gem” knappen.

The screenshot shows the 'KDI CTT Test System #2' interface. On the left is a navigation menu with 'It-systemer' selected. The main content area has tabs for 'Stamdata', 'Dataafgrænsningstyper', 'Anvendersystem', and 'Brugerven'. Under 'Anvendersystem', there is a 'Certifikat' section with a dashed box containing a file upload button and a table with one entry: 'KDI STS SFTP IBA Test2 (funktionscertifikat)' with an expiration date of '2023-02-20'. Below this is an 'SFTP' configuration section with fields for 'SSH brugernavn' (KDI_IBA_SFTP_TEST2), 'SSH nøgle' (ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAhD16REcaz6kowS), and 'Filudvekslingstype' (Simpel).


PEM-formatet er tekst der starter med ”----- BEGIN CERTIFICATE -----”. CER filer findes både i binært og PEM-format, så du kan ved at kigge i filen se hvilket format, det har. Den version du henter fra Nets er allerede i det rigtige PEM-format.

```
-----BEGIN CERTIFICATE-----
MIIGITCCBQmgAwIBAgIEW6uwOTANBg
SzESMBAGA1UECgwJVVFJVVU1QyNDA4MS
dGVzdCBYWE1JIEENBMB4XDTE5MDUyMT
CzAJBgNVBAYTAkRlMShwIQYDVQQKDE
NTFXMCAgA1UEBRMzQ1ZS0je5NDM1MD
bWJpdC1zcC1zaWduaW5nLXRlc3QgKg
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCg
c2xS8Dqz8ogw152N9cIW92GARM0Vo6
HrnQ7K2y+17gT0G5zaYFCudiRk6rA5
6oBxHKP3YMNCDTKsleBL/2WTLUo7rF
00WocyZ91pkBdK/yOqGo3XV1P0tobf
ahuc2dAdI1IgbWwTa7FLvQolie1rWE
o4ICzTCCAskwDgYDVR0PAQH/BAQDAg
-----
```

Det nemmeste er at hente den offentlige version fra Nets. Du kan også anvende OpenSSL til at generere den offentlige version, eller anvende Windows Certificate Snap-in.

For brugervendte systemer og Identity Providers bliver certifikatet automatisk registreret, når du uploader SAML-metadata filen, da det er indlejret i denne.

SAML metadatafiler: *

Træk SAML metadata fil herind		
Certifikat	Udløb [^]	
ADFS Signing - TEST (funktionscertifikat)	2020-11-09	

Opdateringer bliver automatisk provisioneret til Security Token Service (Adgangsstyring for systemer) eller Context Handler (Adgangsstyring for brugere). Dette sker næsten umiddelbart, og du vil inden for kort tid kunne bruge dit certifikat.

6. Windows Certificate Store

Håndtering af certifikater på Java-plattformen er beskrevet i efterfølgende afsnit. Du importerer et certifikat lokalt på en Windows-maskine ved at aktivere filen (dobbelt-klik eller <enter>). Dermed aktiveres Certificate Import Wizard:

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

Current User

Local Machine

Hvis du skal teste lokalt, så kan du anvende "Current User". Når koden skal afvikles fra en Windows-server, placerer du certifikater under "Local Machine", dermed er de tilgængelige for alle tekniske brugere, som programmer afvikles i context af. Du bliver derefter bedt om at indtaste koden til den private nøgle:



Password:

 Display Password

Import options:

- Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
- Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
- Protect private key using virtualised-based security(Non-exportable)
- Include all extended properties.

Som det næste bliver du spurgt om, hvor certifikatet skal placeres:

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

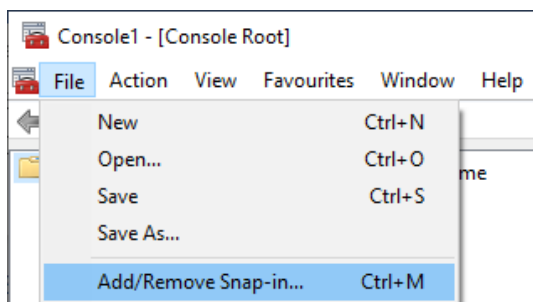
- Automatically select the certificate store based on the type of certificate
- Place all certificates in the following store

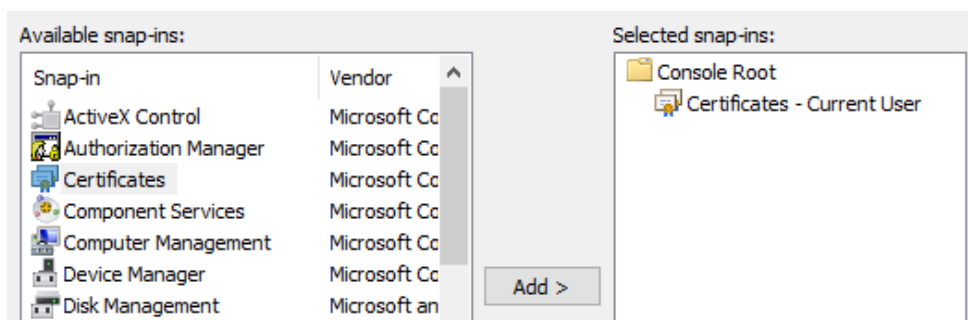
Certificate store:

Browse...

Placeringen i Certificate Store har ingen teknisk betydning, men det kan tænkes, at jeres virksomhed har en standard vedrørende dette, som skal følges.

For at tilgå Certificate Store startes Microsoft Management Console (mmc.exe). Dernæst tilføjes "Certificate" Snap-in:

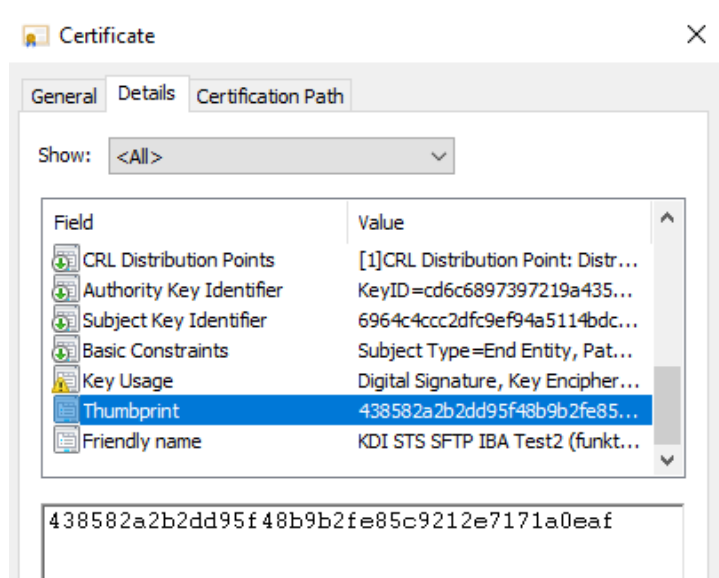




Herfra kan du:

- Eksportere et certifikat til offentlig version i PEM-formatet (.cer).
- Se detaljer for et certifikat.
- Se Certificate Authority (CA) Chain samt tjekke, at denne er valid.
- Se Thumbprint, som skal bruges i .NET kode.

Når du dobbelt-klikker på et certifikat og vælger detaljer, finder du Thumbprint på listen af attributter. Thumbprint anvendes ofte, når koden laver opslag i Certificate Store for at hente et certifikat (der kan laves opslag på andre attributter også).



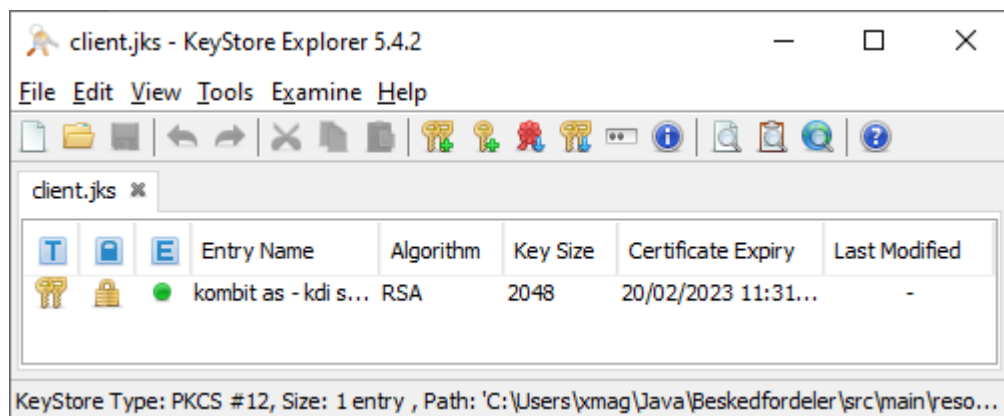
Som beskrevet tidligere skal du hente og registrere [infrastrukturens certifikater](#) på den maskine koden afvikles fra, på samme måde som dit eget certifikat. Der findes separate certifikater til Security Token Service (Adgangsstyring for systemer), Context Handler (Adgangsstyring for brugere), webservices og de fælleskommunale støttesystemer. Du behøver selvfølgelig kun at registrere de certifikater, der tilhører komponenter, du skal integrere med.



Eksempler på anvendelse af certifikater ved kald til webservices findes i [.NET client for Serviceplatformens DemoService](#).

7. Java Key Store

Til håndtering af certifikater på Java-plattformen anbefales <https://keystore-explorer.org/>. Certifikater gemmes i Java KeyStore filer (.jks).

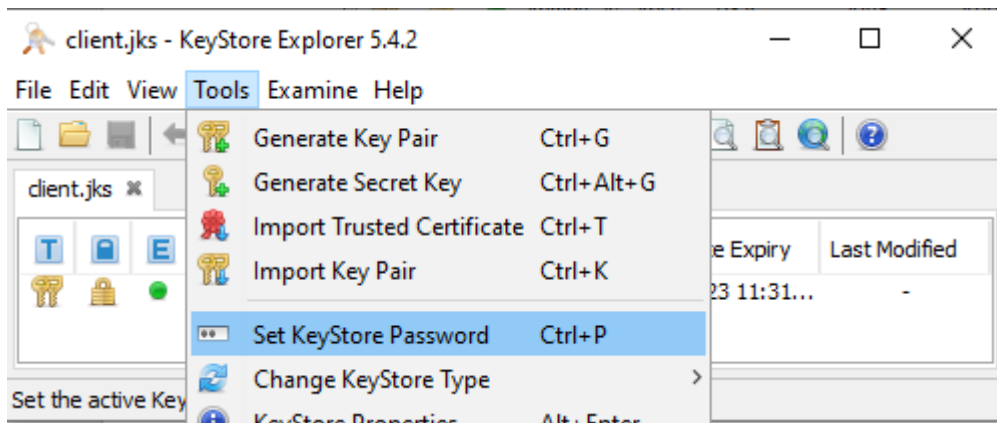


Eksempler på anvendelse af certifikater ved kald til infrastrukturen findes i demo-kode til [Besøgfordeler](#) (i dokumentationspakken) samt [Java client for Serviceplatformens DemoService](#). De anvender begge .jks filer, der kan genanvendes, blot man udskifter relevante certifikater.

Java > Besøgforderler > src > main > resources > token

Name	Date modified	Type
client.jks	21/02/2020 10:02	JKS File
trust.jks	21/02/2020 10:02	JKS File

Filen *client.jks* indeholder det private certifikat, der bruges ved kald til infrastrukturen. Dette skal du erstatte med dit eget. Vigtigt: Et keystore kan indeholde flere certifikater, men *client.jks* må kun indeholde et certifikat for dit anvendelsesystem. Det skal have samme adgangskode som selve certifikatet. Vælg "Tools" i menu og dernæst "Set KeyStore Password":



Filen *trust.jks* indeholder infrastrukturens certifikater for det eksterne testmiljø, og disse bør være gyldige, hvis du har hentet seneste version af demo-koden. Hvis de er udløbet, kan du hente seneste version fra [infrastrukturens certifikater](#). Dette Key Store har ikke behov for at få sat en adgangskode, da det kun indeholder offentlige certifikater.