DIGITALISERINGSSTYRELSEN



# Certifikatpolitik for NemLog-in

Version 1.2

Dette dokument beskriver certifikatpolitikken for NemLog-in løsningen. Politikken definerer hvilke typer certifikater, der må anvendes til kryptering og signering af meddelelser, samt etablering af sikre transportkanaler via SSL / TLS protokollen. Endvidere beskriver politikken retningslinjerne for validering af certifikater.

Målgruppen for dokumentet er teknisk personale hos it-systemudbydere eller disses it-leverandører, som skal planlægge, opsætte test- og produktionsmiljø og udføre integrationstest.

## Dokumenthistorik

| Version | Dato | Initialer | Indhold /ændringer |
|---|---|---|---|
| 0.80 | 19.02.2008 | TG | Første udkast udarbejdet. |
| 0.81 | 20.02.2008 | TG | Opdateret efter input fra EBS. |
| 0.82 | 25.02.2008 | TG | Opdateret med input for SPN. SSL certifikater må ikke være selvsignerede, spærrelistecheck er påkrævet, og politik for udløbet spærreliste tilføjet. |
| 0.83 | 07.03.2008 | TG | Reference til vejledning om signaturers bevisværdi indføjet. |
| 1.0 | 12.09.2008 | TG | Referencer opdateret; versionsnummer opdateret. |
| 1.1 | 02.12.2009 | TG | OCES funktionscertifikater tilladt på linje med virksomhedscertifikater. |
| 1.2 | 07.11.2012 | TG | Opdateret terminologi så den er konsistent med vilkår. Opdateret afsender til Digitaliseringsstyrelsen samt links til dokumenter i referenceliste. Udvidet scope med web service kald og kald til signeringstjeneste. |

# Indholdsfortegnelse

## Introduktion

Den fællesoffentlige føderation er baseret på en dansk profil af SAML 2.0 standarden [OIO-SAML]. Denne foreskriver brug af signering og kryptering af meddelelser samt etablering af SSL / TLS forbindelser med henblik på at opnå en række sikkerhedsmæssige egenskaber som autenticitet, integritet og konfidentialitet. Parternes offentlige nøgler udveksles via X509 certifikater, men profilen definerer ikke nærmere krav til certifikaterne, herunder de politikker, de skal udstedes under. Sådanne krav er overladt til de føderationer, der anvender profilen.

Nærværende dokument definerer derfor certifikatpolitikken for den fællesoffentlige føderation, som omfatter NemLog-in løsningen og de tilsluttede myndighedsløsninger. Der defineres både en politik for miljøer til integrationstest og produktion. Endvidere defineres kravene til certifikatvalidering i føderationen.

## Tilladte typer af certifikater

### Signering og kryptering af meddelelser

Til signering og kryptering af SAML meddelelser, kald mod NemLog-in's signeringstjeneste samt underskrift af lokalt-udstedte security tokens, som veksles af NemLog-in, skal anvendes:

- OCES virksomhedscertifikater eller funktionscertifikater i produktionsmiljøer
- OCES test virksomhedscertifikater eller test funktionscertifikater i integrationsmiljø (udstedt af et OCES test CA).

På denne måde kan validering af certifikater og certifikatkæder konfigureres og testes på samme måde i test- og produktionsmiljøer – blot med forskelligt rodcertifikat som udgangspunkt.

### SSL/TLS Servercertifikater

I forbindelse med etablering af sikre forbindelser mellem brugerens browser og web servere i føderationen er der behov for SSL / TLS servercertifikater. Endvidere anvendes SSL / TLS også til sikring af Single logout via SOAP protokollen (server-til-server kommunikation).

For produktionsmiljøer gælder:

- Der skal anvendes SSL/TLS certifikater udstedt af et CA, der kan valideres af gængse browsere defineret som seneste to versioner af Internet Explorer, Chrome, Safari samt Mozilla Firefox.

Identity Provideren (og evt. serviceudbydere) har behov for et servercertifikat til deres eget domæne samt til det fælles domæne (<servernavn>.fobs.dk) – altså to forskellige servercertifikater. For en illustration af de to domæner og brugen af dem henvises til [GUIDE].

For integrationstestmiljøet gælder:

- Certifikaterne skal udstedes under et test CA, hvis rodcertifikat tilføjes de browsere, der skal indgå i integrationstesten. Det er ikke tilladt at anvende selvsignerede certifikater, da disse kan medføre browseradvarsler og have uheldige sideeffekter, der forstyrrer testen.

Dette betyder, at miljøer til integrationstest og produktion ligner hinanden så meget som muligt.

#### SSL/TLS klientcertifikater

I forbindelse med Single Logout protokollen er der behov for SSL / TLS klientcertifikater, hvis SOAP protokollen anvendes. Her er politikken at anvende samme typer certifikater som til signering / kryptering af SAML meddelelser (se ovenfor).

## Certifikatvalidering

Nedenfor opstilles krav til certifikatvalidering for de forskellige typer certifikater.

#### OCES certifikater anvendt til signering og kryptering

Politikken for validering af certifikater anvendt til signering / kryptering af meddelelser er flg.:

- Der skal som udgangspunkt foretages alle de kontroller af signaturer og OCES certifikater, som er beskrevet i [SIGBEV] appendiks B.
- Der skal foretages spærrekontrol af modparternes certifikater for alle signerede meddelelser, der modtages. Både spærreliste (CRL) og on-line spærrecheck er tilladt.
- Hvis spærrekontrol ikke er mulig, skal meddelelsen / transaktionen afvises. Dette kan eksempelvis være tilfældet, hvis CA'et ikke er tilgængeligt eller aktuel spærreliste er udløbet.
- Hvis der anvendes spærrelister, skal en ny spærreliste hentes minimum en gang per time.
- Det skal kontrolleres, at det anvendte certifikat til signaturvalidering er identisk med det certifikat, der tidligere er oplyst via meta data.

#### SSL/TLS Server Certifikater

Disse valideres af brugerens browser i overensstemmelse med dennes sikkerhedsindstillinger, og særlige retningslinjer herfor gives derfor ikke.

#### SSL/TLS Klientcertifikater

Disse valideres efter samme retningslinjer som certifikater anvendt til signering / kryptering (se ovenfor).

## Fornyelse og spærring

Parterne i føderationen har selv ansvaret for at forny deres certifikater, inden de udløber, og i god tid notificere Digitaliseringsstyrelsen, hvis der er behov for udskiftning af SAML metadata. Dette er eksempelvis tilfældet, når OCES certifikater skal fornys.

Når NemLog-in's tilslutningssystem idriftsættes i 2013, vil serviceudbydere kunne anvende dette selvbetjeningssystem til at opdatere certifikater og metadata for de it-systemer, der er tilsluttet NemLog-in. Ligeledes giver tilslutningssystemet mulighed for at sende en påmindelse før de registrerede certifikater udløber. Dette fordrer dog, at myndigheder og it-leverandører har registreret korrekte e-mail adresser i systemet.

Endvidere er parterne ansvarlige for straks at spærre deres certifikat hos certifikatudsteder (DanID) samt notificere Digitaliseringsstyrelsen, såfremt der er mistanke om kompromittering af certifikatets tilhørende private nøgle.

## Referencer


[OIO-SAML] "OIO Web SSO Profile V2.0.9", Digitaliseringsstyrelsen.
http://digitaliser.dk/resource/2377872

[GUIDE] "Tilslutningsguide. Håndbog for serviceudbyderen som ønsker at tilslutte sig den fællesoffentlige log-in-løsning", Digitaliseringsstyrelsen.
http://www.digst.dk/Loesninger-og-infrastruktur/NemLogin/Tilslutning-til-NemLogin/Materiale-til-IT-leverandoerer

[LOGPOL] "Logningspolitik for den fællesoffentlige log-in-løsning", Digitaliseringsstyrelsen.
http://www.digst.dk/Loesninger-og-infrastruktur/NemLogin/Tilslutning-til-NemLogin/Tekniske-krav

[SIGBEV] "Signatur- og systembevis. Teknisk vejledning i sikring af digitale signaturers bevisværdi", IT & Telestyrelsen.
http://digitaliser.dk/resource/250820

## Øvrige relevante dokumenter og links

NemLog-in gruppen på digitaliser.dk
http://digitaliser.dk/group/2354775

Digitaliseringsstyrelsens web-side om NemLog-in:
http://www.digst.dk/Loesninger-og-infrastruktur/NemLogin