DIGITALISERINGSSTYRELSEN

National eID-gateway

Marts 2022
Version 1.1

Certifikatpolitik

Dette dokument beskriver certifikatpolitikken for den danske eID-gateway. Politikken definerer hvilke typer certifikater, der må anvendes til kryptering og signering af meddelelser, samt etablering af sikre transportkanaler via TLS-protokollen. Endvidere beskriver politikken retningslinjerne for validering af certifikater.

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

Indholdsfortegnelse

1. Introduktion

Autentifikation gennem den danske eID-gateway er baseret på en dansk profil af SAML 2.0 standarden kaldet OIOSAML [OIOSAML]. Denne foreskriver brug af signering og kryptering af meddelelser samt etablering af TLS-forbindelser med henblik på at opnå en række sikkerhedsmæssige egenskaber som autenticitet, integritet og fortrolighed. 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 DK eIDAS Connector i den danske eID-gateway. Der defineres både en politik for miljøer til integrationstest og produktion.

2. Tilladte typer af certifikater

2.1 Signering og kryptering af meddelelser

Til signering og kryptering af SAML-assertion, kald mod DK eIDAS Connector, 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.

2.2 TLS Servercertifikater

I kommunikationen med DK eIDAS Connector skal der anvendes TLS.

I forbindelse med etablering af sikre forbindelser mellem tjenesteudbyders it-system og DK eIDAS Connector er der behov for TLS-servercertifikater.

For produktionsmiljøet gælder:

- Der skal anvendes 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.

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.

3. Certifikatvalidering

Nedenfor opstilles krav til certifikatvalidering for de forskellige typer certifikater.

3.1 OCES-certifikater anvendt til signering og kryptering

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

- 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 online 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 metadata.

3.2 TLS Server Certifikater

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

4. Fornyelse og spærring

Tjenesteudbyder 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.

Ved overgang til nyt certifikat skal tjenesteudbyder meddele sine tekniske oplysninger til Digitaliseringsstyrelsen via e-mail til funktionspostkassen eidas@digst.dk, herunder angive dato og tidspunkt for, hvornår det nye certifikat skal tages i anvendelse.

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

5. Referencer

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

[SIGBEV] "Signatur- og systembevis. Teknisk vejledning i sikring af digitale signaturers bevisværdi", Digitaliseringsstyrelsen. https://www.digitaliser.dk/resource/250820

6. Versionshistorik

Version	Dato	Initialer	Indhold /ændringer
1.0	29-06-2018	OSBUH	Første version til offentliggørelse
1.1	09.03.2022	IDAWI	Mindre sproglige tilpasninger.