

Nets DanID A/S
Lautrupbjerg 10
DK – 2750 Ballerup

T +45 87 42 45 00
F +45 70 20 66 29
www.nets.dk

CVR-nr. 30808460

Specifikationsdokument for OCSP

Indholdsfortegnelse

1	Formål og målgruppe	4
2	Introduktion til OCSP-responder	5
3	OCSP-responder-certifikater	6
4	Komponenter i et OCES-personcertifikat	7
5	OCSP Request profile	8
6	OCSP Response profile	9
7	OCSP-klienter	11

Versionsfortegnelse

30. november 2009	Version 1.0	CR
8. februar 2010	Version 1.1	TechniWrite
20. januar 2011	Version 1.2	MTV
3. juni 2014	Version 1.3	PHJER
5. juni 2014	Version 1.4	PHJER
9. marts 2015	Version 1.5	CRASK MMELI

1 Formål og målgruppe

Dette dokument er en del af NemID tjenesteudbyderpakken.



Dokumentet beskriver den OCSP-profil, som benyttes i NemID-systemet. Dokumentet er relevant for tjenesteudbyderen, hvis Nets DanIDs Sikkerhedspakke ikke indeholder den ønskede funktionalitet på dette område.



Dokumentet henvender sig til de personer, der er ansvarlige for implementeringen af NemID. Det forventes, at brugere har kendskab til OCSP-protokollen som beskrevet i RFC2650.

2 Introduktion til OCSP-responder

OCSP muliggør, at man kan spørge online på status af et aktuelt certifikats serienummer (eller flere serienumre). Dette sikrer, at man hurtigt får den status, man skal bruge, uden at hente den fulde spærrelisteinformation, som kan have en ganske betragtelig størrelse.

Nets DanID tilbyder OCSP til validering af certifikater som supplement til spærrelister (CRL).

Bemærk, at anvendelsen af OCSP-systemet er gratis for private brugere, men hvis man er en virksomhed, skal man have tegnet en aftale om anvendelse af OCSP. Dette kan gøres ved at kontakte Nets DanID Salg på salg@danid.dk.

OCSP-responderen udstilles over http. URL'en, der skal anvendes, er indeholdt i certifikatet og fremgår af Authority Information Access- extensionen.



OCSP er beskrevet i standarden RFC 6960 med yderligere krav fra OCES Certifikat Politikken.

3 OCSP-responder-certifikater

De certifikater, som OCSP-responderen benytter til signering, er standard OCES-virksomhedscertifikater, dog med følgende tilpassede profil:

Felt	Værdi/Beskrivelse
Validity	Gyldighedsperioden vil være kortere end for normale certifikater
Key Usage	Digital Signature
Extended Key Usage	OCSP Signing
OCSP No Check	Empty – dvs. at klienten bør stole på validiteten af certifikatet.
CRL Distribution Point	Ikke medtaget
Authority Information Access (AIA)	Ikke medtaget

4 Komponenter i et OCES-personcertifikat

OCES-personcertifikater indeholder en X.509 standard extension, der udpeger OCSP-responderen, så valideringsværktøjer kan kalde den:

Felt	Værdi
Authority Information Access (AIA), accessMethod OCSP	URL til OCSP-responderen, eksempelvis http://ocsp.oces-issuing01.trust2408.com/responder

Denne extension er markeret som non-critical. Der er ikke yderligere OCSP-relevante oplysninger i OCES-certifikater.

5 OCSP Request profile

De OCSP-requests, som OCSP-responderen accepterer, skal overholde følgende begrænsninger:

Felt	Værdi
Version	1
Requestor Name	Valgfrit felt. Bør indeholde navnet på den kaldende service
Request List Hash Algorithm	SHA1 understøttes
Request List Issuer Name Hash	SHA1 hash af TRUST2408 OCES CA n Name
Request List Issuer Key Hash	SHA1 hash af den offentlige nøgle for TRUST2408 OCES CA n's certifikat
Request List Serial Number	Kan indeholde ét serienummer der ønskes verificeret.
Nonce	Det er tilladt at angive en nonce, men Nets forbeholder sig ret til ikke at angive tilsvarende nonce i OCSP responset.

Bemærk, at:

- Der kun kan angives ét serienummer pr. request.
- Signerede requests behandles præcis som usignerede requests. Det vil sige, at signaturen ikke valideres.

6 OCSP Response profile

OCSP-responses har følgende profil i forhold til standard-OCSP-responses:

Felt	Værdi
OCSP Response status	Succesful, hvis et korrekt response kunne genereres. I andre tilfælde sættes en anden (undefineret) status
Response Type	Basic OCSP Response
Version	1
Responder ID	OCSP Responder'ens Distinguished Name
Produced At	Tidsstempel der fortæller, hvornår response er genereret
Response List <i>Hash Algorithm</i>	SHA1
Response List <i>Issuer Name Hash</i>	SHA1 hash af TRUST2408 OCES CA n Name
Response List <i>Issuer Key Hash</i>	SHA1 hash af den offentlige nøgle for TRUST2408 OCES CA n'ens certifikat
Response List <i>Serial Number</i>	Serienummer for det certifikat, der blev valideret
Response List <i>Cert Status</i>	Revoked eller Valid afhængig af certifikatets status
Response List <i>Revocation Time</i>	Revokeringstidspunkt – kun angivet hvis certifikatet er spærret
Response List <i>This Update</i>	Tidsstempel for sidste synkronisering med CA'ens spærreliste
Response List <i>Next Update</i>	Tidsstempel for næste synkronisering med CA'ens spærreliste. Synkronisering kan dog ske tidligere.

Response vil muligvis ikke indeholde Nonce Extensions, selv om requesten indeholder en Nonce extension.

Hvis request angiver andre udstedere end TRUST2408 OCES CA n, afvises requesten som malformed.

Hvis request angiver et serienummer, der ikke svarer til et certifikat dusted af TRUST2408 OCES CA n'en, sendes en response, der svarer til svaret for et gyldigt certifikat.

7 OCSP-klienter

OOAPI indeholder en OCSP-klient (OCSPCertificateRevocationChecker), som kan benyttes.

OCSP-klienten fra OpenSSL kan også bruges direkte.

Eksempel på opslag mod OCSP-responderen med OpenSSL:

```
$ openssl ocsf -issuer certs/oces2-ica02-pr.crt -serial  
0xA537332EC -url http://ocsp.pr.certifikat.dk/responder -  
CAfile certs/oces2-bundle-pr.crt
```

```
Response verify OK
```

```
0xA537332EC: good
```

```
This Update: Mar 3 14:44:35 2015 GMT
```

```
Next Update: Mar 4 02:45:21 2015 GMT
```

Bemærk at oces2-ica02-pr.crt indeholder certifikatet fra den udstedende CA, der har udstedt certifikatet, som ønskes valideret, men filen oces2-bundle-pr.crt indeholder både OCES II rodcertifikatet og certifikatet fra den udstedende CA.