Nets DanID A/S
Lautrupbjerg 10
DK – 2750 Ballerup

T +45 87 42 45 00
F +45 70 20 66 29
info@danid.dk
www.nets-danid.dk

CVR-nr. 30808460

Specifikationsdokument for OCSP

Indholdsfortegnelse

Versionsfortegnelse

25. maj 2009	Version 0.0	MOBO
26. november 2009	Version 0.1	JRF
30. november 2009	Version 1.0	CR
8. februar 2010	Version 1.1	TechniWrite
20. januar 2011	Version 1.2	MTV

1 Formål og målgruppe

Dette dokument er en del af Tjenesteudbyderpakken for NemID.

Dokument 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.

Oversigt over alle dokumenter i Tjenesteudbyderpakken:

Overordnet dokumentation

- Introduktion til NemID og Tjenesteudbyderpakken
- Anbefalinger til interaktionsdesign og brugervalg af applet
- Drejebog for migrering til NemID
- Termer og begreber i NemID

Implementeringsdokumentation

- Implementeringsvejledning for NemID
- Konfiguration og opsætning

Testdokumentation

- Vejledning i brug af test tools
- Anbefalede testprocedurer

Referencedokumentation

- Specifikationsdokument for servicen PID-CPR
- Specifikationsdokument for servicen RID-CPR
- Specifikationsdokument for LDAP API
- **Specifikationsdokument for OCSP**
- Specifikationsdokument for OCES II

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 er ganske betragtelig.

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 2560 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
Access Information Authority (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
Access Information Authority (AIA)	Online Certificate Status Protocol, som findes på: http://ocsp.certifikat.dk/ocsp/status

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'ens certifikat
Request List Serial Number	Kan indeholde ét serienummer der ønskes verificeret.
Nonce	Hvis der er angivet nonce extensions, ignoreres de.

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 (udefineret) 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 *Hash Algorithm*	SHA1
Response List *Issuer Name Hash*	SHA1 hash af TRUST2408 OCES CA n Name
Response List *Issuer Key Hash*	SHA1 hash af den offentlige nøgle for TRUST2408 OCES CA n'ens certifikat
Response List *Serial Number*	Serienummer for det certifikat, der blev valideret
Response List *Cert Status*	Revoked eller Valid afhængig af certifikatets status
Response List *Revocation Time*	Revokeringstidspunkt – kun angivet hvis certifikatet er spærret
Response List *This Update*	Tidsstempel for sidste synkronisering med CA'ens spærreliste
Response List *Next Update*	Tidsstempel for næste synkronisering med CA'ens spærreliste

Response vil ikke indeholde Nonce Extensions, heller ikke hvis 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

Der kan hentes et eksempel på en Java OCSP-klient på http://ocsp.certifikat.dk/ocsp/status

OCSP-klienten fra OpenSSL kan bruges direkte.

Eksempel på opslag mod OCSP-responderen med OpenSSL:

```
> openssl ocsp -issuer oces.cer  -CAfile oces.cer -
no_nonce -serial 123 –url
     http://ocsp.certifikat.dk/ocsp/status

Response verify OK
123: good
        This Update: Nov 29 11:19:36 2009 GMT
        Next Update: Nov 29 11:20:36 2009 GMT
```