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 no. 30808460

Specification document for OCSP

Table of Contents

Version history

8 February 2010	Version 1.1	TechniWrite
20 January 2011	Version 1.2	MTV
4 June 2014	Version 1.3	PHJER
9 March 2015	Version 1.4	CRASK MMELI

1 Purpose and target group

This document is a part of the NemID Service Provider Package.

The document describes the OCSP profile that is used in the NemID system. The document is relevant for the service provider if Nets DanID's Security Package does not contain the desired functionality in this area.

The document is aimed at the people who are responsible for the implementation of NemID. It is expected that users are familiar with the OCSP protocol as described in RFC2650.

2 Introduction to OCSP responder

OCSP enables you to enquire online about the status of a current certificate's serial number (or several serial numbers). This ensures that you quickly obtain the status that you need without downloading the full certificate revocation list information, which can be quite considerable.

Nets DanID offers OCSP for the validation of certificates as a supplement to certificate revocation lists (CRL).

Please note that the use of the OCSP system is free for private users, but if you are a company you must have concluded an agreement on the use of OCSP. This can be done by contacting Nets DanID Sales at salg@danid.dk.

The OCSP responder is displayed via HTTP. The URL to be used is included in the certificate and can be seen in the Authority Information Access extension.

OCSP is described in the RFC 6960 standard, with additional requirements from the OCES Certificate Policy.

3 OCSP responder certificates

The certificates that the OCSP responder uses for signing are standard OCES company certificates, though with the following adapted profile:

Field	Value/Description
Validity	The period of validity will be shorter than for normal certificates.
Key Usage	Digital Signature.
Extended Key Usage	OCSP Signing.
OCSP No Check	Empty – i.e. the client should trust the validity of the certificate.
CRL Distribution Point	Not included.
Authority Information Access (AIA)	Not included.

4 Components in an OCES personal certificate

OCES personal certificates contain an X.509 standard extension, which designates the OCSP responder so that validation tools can call them:

Field	Value
Authority Information Access (AIA)	Online Certificate Status Protocol URL. For example: http://ocsp.oces-issuing01.trust2408.com/responder

This extension is designated as non-critical. There is no additional OCSP-relevant information in OCES certificates.

5 OCSP Request profile

The OCSP requests that the OCSP responder accepts must comply with the following limitations:

Field	Value
Version	1
Requestor Name	Optional field. Should contain the name of the calling service.
Request List Hash Algorithm	SHA1 is supported.
Request List Issuer Name Hash	SHA1 hash from TRUST2408 OCES CA n Name.
Request List Issuer Key Hash	SHA1 hash from the public key for the TRUST2408 OCES CA n's certificate.
Request List Serial Number	Can contain one serial number that you wish to verify.
Nonce	Allowed, but can be ignored by Nets.

Note that:

- Only one serial number can be specified for each request.
- Signed requests are processed in exactly the same way as unsigned requests. This means that the signature is not validated.

6 OCSP Response profile

OCSP responses have the following profile in relation to standard OCSP responses:

Field	Value
OCSP Response status	Successful if a correct response could be generated. Otherwise, a different (undefined) status is set.
Response Type	Basic OCSP Response.
Version	1
Responder ID	The OCSP Responder's Distinguished Name.
Produced At	Time stamp that defines when the response was generated.
Response List *Hash Algorithm*	SHA1.
Response List *Issuer Name Hash*	SHA1 hash from TRUST2408 OCES CA n Name.
Response List *Issuer Key Hash*	SHA1 hash from the public key for the TRUST2408 OCES CA n's certificate.
Response List *Serial Number*	Serial number of the certificate that was validated.
Response List *Cert Status*	Revoked or Valid, depending on the certificate's status.
Response List *Revocation Time*	Only specified if the certificate has been revoked.
Response List *This Update*	Time stamp of the last synchronisation with the CA's certificate revocation list.
Response List *Next Update*	Time stamp of the next synchronisation with the CA's certificate revocation list. Earlier synchronisation is possible.

Response might not contain Nonce Extensions, even if the request contains a Nonce extension.

If the request specifies issuers other than TRUST2408 OCES CA n, the request is rejected as malformed.

If the request specifies a serial number that does not correspond with a certificate dusted by the TRUST2408 OCES CA n, a response is sent corresponding to the response for a valid certificate.

7 OCSP clients

An example of OCSP client (OCSPCertificateRevocationChecker) can be obtained from OOAPI.

The OCSP client from OpenSSL can be used immediately. For example:

```
$ openssl ocsp -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
```

Please note:

- oces2-ica02-pr.crt contains certificate of that issuing CA, which issued the certificate we are validating
- oces2-bundle-pr.crt contains certificates of issuing CA and OCESII root CA.