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 OCES II

Versionsfortegnelse

3. juni 2014	Version 1.5	PHJER
12. december 2016	Version 1.6	KMAIB

Indholdsfortegnelse

1 Formål og målgruppe

Dette dokument er en del af NemID tjenesteudbyderpakken.

Dokument beskriver OCES II, som benyttes i NemID. Dokumentet er relevant for tjenesteudbyderen, hvis Nets DanIDs Sikkerhedspakke ikke indeholder den ønskede funktionalitet på dette område.

Dokumentet henvender sig til de personer hos tjenesteudbydere, der er ansvarlige for implementeringen af NemID. Bemærk at dokumentet fra Afsnit 2 og frem er på engelsk.

2 Preface

This document details the contents of OCES II certificates issued by Nets DanID. This includes content specifics for the different types of certificates namely Personal, Employee, Company and Functional certificates defined in the OCES certificate policy.

Some of the content is regulated by the X.509v3 standard or the respective certificate policy, and the reader should consult these documents for further details.

It is assumed that the reader has adequate knowledge of the X.509 technology.

3 Components of a certificate

The contents of a certificate can be divided into the following components:

Field	Value/Description
Formalia	509 version, Certificate Serial Number, Validity period
Issuer	DN of issuer
Subject	DN of subject
Public Key	The subjects public Key
Extensions	Subject Alternative Name, Key Usage, Certificate Policy, CRL Distribution Point, Basic Constraints, Authority Information Access, Private Key Usage Period, Issuer Key Identifier, Subject Key Identifier
Signature	The CA’s signature confirming the correspondence between the identity of the subscriber and the key pair

Formalia, Issuer DN, Subject DN and the extensions will be described in detail.

Note that in the following, the ASN1 encoding types are given in parenthesis where applicable.

4 Formalia

Formalia are characterized by the following details:

Field	Value/Description
X.509 Version	3 (Integer) Note that the actual integer value is 2 according to the X.509 standard
Serial Number	Serial number of the issued certificate (Integer) Note that this number should not be mistaken for the Subject serialNumber.
Validity Period	The notBefore and notAfter fields specifying the validity of the certificate (UTCTime)

5 Issuer Distinguished Name

Nets DanID has several CA issuing OCES II certificates. Note that Nets DanID is using the officially registered alternative name 'Trust2408' in the certificates.

The content of the **Issuer DN** are characterized by the following details:

Field	Value/Description
Country	DK (PrintableString)
Organisation	TRUST2408 (UTF8String)
Common Name	TRUST2408 OCES CA n (UTF8String)

Where n is a number (represented by roman numerals) to distinguish between the different issuing CA. E.g. the fourth OCES issuing CA will be named:

"CN=TRUST2408 OCES CA IV, O=TRUST2408, C=DK"

6 Subject Distinguished Name

6.1 Personal certificates

The contents of the **Subject** field are characterized by the following details:

Field	**Value/Description**
Country	DK (PrintableString)
Organisation	Ingen organisatorisk tilknytning (UTF8String)
Common Name	Common Name of user, i.e. Registered Name or Pseudonym (UTF8String)
Subject SerialNumber	The PID of the subscriber, e.g. PID:9208-2002-2-123456789012 (PrintableString). The last component is the serial number, while the start is CA specific stuff. The serial number is at present time 12 digits. The total PID string can be considered unique. The total Subject serialNumber however is restricted to 64 chars.

For young persons, who are between 15 and 18 years of age the subject DN also includes an **OU** field which is characterized by the following details:

Field	**Value/Description**
Organisational Unit	Ung mellem 15 og 18 - Kan som udgangspunkt ikke lave juridisk bindende aftaler (UTF8String)

6.2 Employee certificates

The contents of the **Subject** field are characterized by the following details:

Field	Value/Description
Country	DK (PrintableString)
Organisation	Organisation name and CVR number (UTF8String) in the form "OrgName // CVR:xxxxxxxx" where the OrgName is the registered name of the organization and xxxxxxxx is the CVR number e.g. "NETS DANID A/S // CVR: 30808460". Note that long organisation names may be truncated
Organisation Unit	Optional Organisation Unit Name fields. Note that more than one field can be present. (UTF8String) e.g. "Marketing"
Common Name	Name of certificate holder which may include the title e.g. "CEO John Doe" (UTF8String)
Subject SerialNumber	The CVR number of the organization followed by the RID of the employee (PrintableString) e.g. CVR:14773908-RID:1234. The total string can be considered unique. The total Subject serial number is restricted to 64 chars. Note that the RID may include other characters than digits.

6.3 Company certificates

The contents of the **Subject** field are characterized by the following details:

Field	Value/Description
Country	DK (PrintableString)
Organisation	Organisation name and CVR number (UTF8String) in the form "OrgName // CVR:xxxxxxxx" where the OrgName is the registered name of the organization

	and xxxxxxxx is the CVR number e.g. “NETS DANID A/S // CVR: 30808460”. Note that long organisation names may be truncated
Organisation Unit	Optional Organisation Unit Name fields. Note that more than one field can be present. (UTF8String) e.g. “Marketing”
Common Name	Common Name consists of organisation, name organisation unit names and optional function description (UTF8String), e.g. “Nets DanID A/S - Marketing - Reciept Broker”
Subject SerialNumber	The CVR number of the organization and followed by the UID of the certificate holder (PrintableString) e.g. CVR:14773908-UID:1234. The total string can be considered unique. The total Subject serial number is restricted to 64 chars. Note that the UID may include other characters than digits.

6.4 Functional certificates

The contents of the **Subject** field are characterized by the following details:

Field	**Value/Description**
Country	DK (PrintableString)
Organisation	Organisation name and CVR number (UTF8String) in the form “OrgName // CVR:xxxxxxxx” where the OrgName is the registered name of the organization and xxxxxxxx is the CVR number e.g. “NETS DANID A/S // CVR: 30808460”. Note that long organisation names may be truncated
Organisation Unit	Optional Organisation Unit Name fields. Note that more than one field can be present (UTF8String), e.g. “Marketing”
Common Name	Common Name consists of organisation, name organisation unit names and optional function description

	(UTF8String), e.g. “Nets DanID A/S - Marketing - Reciept Broker”
Subject SerialNumber	The CVR number of the organization and followed by the FID of the certificate holder (PrintableString) e.g. CVR:14773908-FID:1234. The total string can be considered unique. The total Subject serial number is restricted to 64 chars. Note that the FID may include other characters than digits.

7 Public Key

The content of the **Public Key** field is characterized by the following details:

Field	Value/Description
Public Key	The subscribers public key (BitString)

8 Extensions

The contents of the **Extension** fields are characterized by the following details. Note that extension can be marked as critical. If this is the case, this will be specified under the particular extension.

Field	Value/Description	Critical
Key Usage	The intended key usage for the given certificate. Different for encryption, verification and combined certificates according to the OCES CP. (OctetString).	Yes
Certificate Policies	The Certificate Policy extension holds the following parts: 1. OCES CP OID 2. Reference to www.certifikat.dk/repository where terms can be found 3. A short cook up (200 chars) of the terms	No
CRL Distributio n Points	The CRL Distribution Points extension holds different locations for status information of the given certificate. Two different ways are supported: 1. A full CRL over http 2. A partitioned CRL over LDAP Since most client applications support CRL download over http the full CRL is located at the http link. **Example:** http://crl.oces.certifikat.dk/ocesii.crl The LDAP reference to the partitioned CRL is not full, i.e. the hostname is not included. This prevents clients who are expecting a full CRL to trust a partitioned CRL as full. If a partner wants to implement partitioned CRL support they have to be aware of the following details: 1. A new partitioned CRL is issued for every 750 certificates 2. The most secure way to decide which partitioned CRL to use is to look at the	No

	CRL Distribution Point in the certificate. 3. The hostname of the external LDAP is ldap://dir.certifikat.dk Note further that since the partitioned CRL mechanism is far more complicated it is the responsibility of the partner to ensure that the implementation is correct. **Example:** DirName:/C=DK/O=DanID/CN=DanID OCES CA n/CN=CRL3 Note further that the full CRL can be obtained over LDAP from the node /C=DK/O=DanID/CN=DanID OCES CA n in the attribute certificateRevocationList Note that the CRL files obey the following rule of thumb: A general CRL grows with 38 bytes for each revoked certificate (offset 527 bytes) Hence partitioned CRLs have size 0-30000 bytes The location of the CRL servers is dictated by the DNS names crl.oces.certifikat.dk and dir.certifikat.dk Note that may corresponds to the several IP-addresses since shift between the IP-addresses is done dynamically and without warning however respecting TTL in the DNS system. This means that an implementation of CRL retrieval should comply with the following: 1. The service should not cache DNS/IP information but perform DNS lookups respecting TTL. 2. If the service is behind a firewall make sure that the firewall does not block any of the destination IP-addresses in the list.	
Access Information Authority (AIA)	The OCES certificate holds one AIA extension with two references: A reference (Online Certificate Status Protocol) to the OCSP responder. The OCSP responder can be used as an alternative to CRLs to verify certificates. The responder is compliant with	No

	RFC2560 and is described in further details elsewhere. A HTTP reference (CA Issuers) to a DER-encoded file containing the CA certificate used to sign the certificate. This can be used for building a trusted certificate path. This is useful for relying parties, which only has the end user certificate (or a fraction of a certificate chain).	
Authority Key Identifier	The Authority Key ID holds a fingerprint of the Issuing key. For chain building purposes (OctetString).	No
Subject Key Identifier	The Subject Key ID holds a fingerprint of the Subject key. For chain building and internal client administrative purposes (OctetString)	No
Basic Constraint s	Basic Constraints hold information about whether or not the certificate is an end user or a CA certificate. For OCES End User Certificates this is done by the value CA:FALSE (OctetString)	No
Subject Alternative Name	Certificate holders email address, if subscriber decides to include this in the certificate, e.g.: email:me@mail.dk (OctetString) Note that this extension is optional.	No

9 Signature

The content of the **Signature** field is characterized by the following details:

Field	**Value/Description**
Signature	The CA's signature on the certificate (BitString)