OFTP2 Certificate Policy
Version 1.1

Table of Contents

Copyright (C) 2009 Odette International Limited. All rights reserved

1. Certificate Usage:

OFTP2 application usage for encryption, authentication and integrity.

2. Certificate Requirements:

2.1. Types of certificates

TLS:
- One for session authentication and encryption ,

OFTP protocol:
- One for OFTP authentication (challenge encryption),
- One for EERP signing,

File security service (CMS):
- One for file signature,
- One for file encryption.

Considering the OFTP authentication challenge as a temporary key, it is allowed to use a single TLS standard certificate for all the OFTP2 security features in accordance with the X509 standard; the decision is at the user's discretion.

2.2. Basic fields

- Version : 3 (coded : 2),
- Serial Number : assigned by the signer,
- Signature algorithm : "Sha1WithRSAEncryption",
- Issuer : Identity of the signer,
- Validity : Not before, Not after,
- Subject: Contains some recommended items. Other items must be accepted even if not used.

  Recommended items:
  - Company name (Organisation),
  - Organisation Unit,
  - Location,
  - Country
  - Common Name.
    Note: if an item is used in the subject, the content must not be empty.

- Subject public key info,
- Signature algorithm and signature data.

If the certificate is used for TLS it is recommended that the subject contains the fully qualified domain host name (FQDHN). If the fully qualified domain name is stored in the subject, the CN attribute should be used.
Alternatively the Subject Alt Name can be used to store the FQDHN or the IP address (see section 2.3).

Copyright (C) 2009 Odette International Limited. All rights reserved

2.3. Extensions fields User certificate

If the certificate is used for TLS the following fields are mandatory and MUST be present:

- Authority Key Identifier = hash (1)
- CRL Distribution Point = "http URL" (2)

Further optional fields:

- a second CRLDP with an LDAP address.
- Key Usage = Digital Signature, Key Encipherment(3).
- Extended Key Usage = TLS Web Server Authentication and/or TLS Web Client Authentication or SSL server and/or SSL client (4).
- Subject Alt Name can carry the Odette ID using the keyword URI. Example: URI: "Odette ID"

If the certificate is used for TLS it is recommended that the subject (see section 2.2) or the subject alternative name contains the FQDHN. The subject alternative name may also contain the IP address. If the FQDN is stored in the Subject Alt Name, the dNSName attribute should be used. If the IP address is stored in the Subject Alt Name, the iiPAddress attribute should be used.

2.4. Extensions fields CA's certificate

Root CA's certificate MUST include:

- CRL Distribution Point = "http URL" (for automatic CRL fetching)
- Optional: a second CRLDP with an LDAP address.
- The basic constraint "CA" MUST be present and its value MUST be "TRUE".

In addition to these fields, intermediate CA's certificate MUST include also the "Authority Key Identifier" in order to facilitate the trust chain verification.

---

(1) Makes the "Trust chain" verification easier
(2) To enable the automatic CRL fetching.
(3) Mandatory items for TLS. C.f. RFC 2246 page 38.
Note: As this extension must be flagged "Critical", using such a certificate for OFTP2 authentication should normally not be allowed according to [RFC 2459]. It is explicitly allowed in OFTP2 in order to make possible OFTP2 running with only one certificate, while using widely spread out certificates (SSL server certificates).
(4) If present, these items shouldn't cause a certificate rejection, neither by the file security service layer, nor by the OFTP authentication and EERP signing service. In order to achieve that point while still conform to [RFC 2459], this extension MUST NOT be flagged "Critical".

Copyright (C) 2009 Odette International Limited. All rights reserved

2.5. Usage flags to crypto functions mapping

		Key Usage and Extended Key Usage			
		Digital Signature	Key Encipher-ment	TSL Server Authent.	TSL Client Authent.
File security service (CMS)	File Signing	YES			
	File Encryption		YES		
OFTP	Authentication		YES**		
	EERP Signing	YES			
TLS	Authentication & Key Exchange	YES	YES	YES	YES

Figure 1 Crypto functions mapping table

** This is normally not allowed according to [RFC 2459]. But It is explicitly allowed in OFTP2 in order to make OFTP2 able to run with only one certificate, while using widely spread out certificates (SSL server certificates).

Copyright (C) 2009 Odette International Limited. All rights reserved

3. CA Requirements:

The chapter 5.4 of ETSI TS 102042 is applicable in its entirety.

The LCP profile of the ETSI TS 102042 chapter 6 is applicable with these modifications:

- o 6.2-b: the key pair can be used for OFTP authentication even if the Key usage doesn't mention "Data Encipherment". This amendment is not conformant to X509 [RFC 2459], but it allows usage of a single "standard" SSL certificate to cover all the OFTP2 security features.

- o 6.2-d: Key length: 1024 bits minimum.

- o 6.3-b: same as 6.2-b.

The LCP profile of the ETSI TS 102042 chapter 7 is applicable with these modifications:

- o 7.1-c: adding "At least, the CA shall publish its CPS on the Web in standard html format via http protocol".

- o 7.2.3-a: replace " NOTE: For example, certification authority public keys may be distributed in certificates" by "Certification authority public key MUST be distributed by means of X509 certificates.
  These certificates MUST contain: (c.f. 2.5.1 of this document: Basic fields and 2.5.3: Extension fields CAs certificates)."

- o 7.2.8-b: Key length: 1024 bits minimum.

- o 7.2.8-e: Any copies of the subject's private key held by the CA MUST be destroyed.

- o 7.3.1-c: adding "At least, the CA MUST publish this information on the Web in standard html format via http protocol".

- o 7.3.1-i: identifier of the device by which it may be referenced (e.g. Internet domain name, Odette Id as described in 5.4 of [RFC 5024] based on [ISO 6523].)

- o 7.3.3-a: replaced by 2.5.1 and 2.5.2 of the present document.

- o 7.3.4-b: adding "At least, the CA MUST publish this information on the Web in standard html format via http protocol".

- o 7.3.5-b: replaced by "Certificates are available for retrieval unless the subject has expressly made known his opposition.

- o 7.3.6-a: remove it. Rely on modified 7.3.6-g.

- o 7.3.6-g: replaced by "The status of revoked certificates MUST be published using CRL. After the revocation status of a certificate

Copyright (C) 2009 Odette International Limited. All rights reserved

has changed, the CRL MUST be updated in a very short time period; typically less than 5 minutes."

o 7.3.6.h: replaced by: CRLs MUST include :
- The time for next scheduled CRL issue
- The signature of the certification authority or an authority designated by the CA.
- The list of the serial numbers of the revoked certificate. This list can be partial: "delta CRL" mechanism is allowed.

o 7.3.6-i: replace "[LCP]" by "The CRL MUST be available at least on the Web in a standard html format via http protocol".

Copyright (C) 2009 Odette International Limited. All rights reserved

4. Legal binding statement of TSL:

no legal binding

5. Subscribing process

5.1. Policy compliance:

5.1.1.

SCXA requires a signed statement of compliance of an authorised person of the CA.

5.1.2.

SCXA is entitled to add CAs on own discretion to the list, provided the CAs fulfill the requirements according to number 3 of this policy and issue the certificates under a extended validation policy according to chapter 4.5 of ETSI TS 102042.

5.2. Authentication:

Precondition for addition of a CA on their own request is the subscription to the BASIC list.

5.3. Authorisation:

SCXA requests signed self-commitment of subscriber to be authorised to register the CA in case of registration according to 5.1.1.

6. Security Trust Level Description:

For all CAs on TSL OFTP2 an identity check for the CA owner has been performed. No checks of CA infrastructure are performed. A statement of policy compliance has been obtained of those CAs, which were registered on their own request. In these cases, authorisation checking for CA owner was done by self-commitment.

Copyright (C) 2009 Odette International Limited. All rights reserved