CR-Form-v7

PSEUDO CHANGE REQUEST

⌘ **ab.cde** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: 0.3.0 ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Additions to the clause 5.3 on profiling of certificates
Source:	⌘	Siemens, Nokia, SSH, T-Mobile
Work item code:	⌘	NDS/AF
Date:	⌘	08/07/2003
Category:	⌘	
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)

Reason for change: ⌘ Addition of review remarks and insights delivered from draft-ietf-ipsec-pki-profile-02.txt according to following guidelines:

- Do not refer to draft-ietf-ipsec-pki-profile-02.txt but copy the relevant information to the NDS/AF spec. draft-ietf-ipsec-pki-profile-02.txt will probably not make it to RFC in the short term if it will make it at all!
- Do not include error case descriptions from draft-ietf-ipsec-pki-profile-02.txt if due to interworking with non-compliant NDS/AF SEG.

Details of changes:

- Incorporation of the JNSA lessons from PKI interoperability testing 2001: See attachment or *http://www.jnsa.org/english/e_result.html* (also presented at IETF-55= Nov 2002).
- Adding text on the role of the roaming CA/SEG with respect to the Certificate profiling verification.
- Adding text on relation with RFC3280.
- Correcting inaccurate naming of certificate fields.
- SEG certificates shall be directly signed by the roaming CA.
- Adding an editors note on identities and outstanding profiling work

		- Adding subjectAltName to the SEG certificate profile
Summary of change:	⌘	
Consequences if not approved:	⌘	

Clauses affected:	⌘	5.3			
		Y	**N**		
Other specs affected:	⌘		**N**	Other core specifications	⌘
			N	Test specifications	
			N	O&M Specifications	
Other comments:	⌘				

5.3 Profiling

[Editor's note: "Motivation" statements marked with italic in chapters 5.3.1 and 5.3.2 are included in the drafting stage of the TS, but will be removed before submission for approval to TSG SA.]

5.3.1 Certificate profiles

[Editor's note: A more detailed check on using RFC3280 and draft-ietf-ipsec-pki-profile-02.txt *as the main profiling base is needed. It needs to be assessed why and how we want to deviate from these papers.* draft-ietf-ipsec-pki-profile-02.txt will not be referenced from this specification, but valuable profiling statements will be copied to the NDS/AF specification*]*

This clause profiles the certificates to be used for NDS/AF. An NDS/AF component shall not expect any specific behaviour from other entities, based on certificate fields not specified in this section.

Certificate profiling requirements as contained in this specification have to be applied in addition to those contained within RFC3280. This applies for both the SEG and the roaming CA.

Before fulfilling any certificate signing request, a roaming CA shall make sure that the request suits the profiles defined in this section. Furthermore, the CA shall check the Subject's DirectoryString order for consistency, and that the Subject's DirectoryString belongs to its own administrative domain.

Motivation: This addresses lesson from http://www.jnsa.org/english/e_result.html

SEGs shall check compliance of certificates with the NDS/AF profiles and shall only accept compliant certificates.

Motivation: This addresses lesson from http://www.jnsa.org/english/e_result.html

[Editor's note: the relationship between a) ID's includes within the certificate, B) used at the transport layer and C) IKE ID available within the IKE policy; and their effects on the profiling needs further investigation]

5.3.1.1 Common rules to all certificates

- Version 3 certificate according to RFC3280.

  Motivation: This is the current state of the art [3].

- Hash algorithm for use before signing certificate: Sha-1 mandatory to support, MD-5 shall not be used.

  Motivation: SHA-1, is state of the art, MD-5 shall not be used anymore as it is considered weaker

- Subject and issuer name format. Note that C is optional element. : (C=<country>), O=<Organization Name>, CN=<Some distinguishing name>. Organization and CN shall be in UTF8 format.

  Motivation: RFC3280 states in clause 4.1.2.4 Issuer that The UTF8String encoding in RFC 2279 is the preferred encoding, and all certificates issued after December 31, 2003 MUST use the UTF8String encoding of DirectoryString (except in some migration cases).

- CRLv2 support with LDAPv3 [5] retrieval shall be supported as the primary method of certificate revocation verification.

- Certificate extensions mentioned within RFC3280 but not in NDS/AF are optional for implementation.

SerialNumber shall have a length of exactly 20 octets

Motivation: *This addresses lesson from http://www.jnsa.org/english/e_result.html*

5.3.1.2 CA Certificate profile

In addition to clause 5.3.1.1, following requirements apply:

- The RSA key length shall be at least 2048-bit

  Motivation: "RSA Laboratories currently recommends key sizes of 1024 bits for corporate use and 2048 bits for extremely valuable keys like the root key pair used by a certifying authority "

  see http://www.rsasecurity.com/rsalabs/faq/3-1-5.html

- Extensions:
  - Optionally non critical authority key identifier
  - Optionally non critical subject key identifier
  - Mandatory critical key usage: At least keyCertSign and CRL Sign should be asserted
  - Mandatory critical basic constraints: CA=True, path length unlimited or at least 2.

5.3.1.3 SEG Certificate profile

SEG certificates shall be directly signed by the roaming CA, i.e. without employing any intermediate CAs. This limits NDS/AF complexity and makes retrieval and validation of intermediate CA certificates by SEGs unnecessary.

In addition to clause 5.3.1.1, following requirements apply:

- The RSA key length shall be at least 1024-bit

  Motivation: "RSA Laboratories currently recommends key sizes of 1024 bits for corporate use and 2048 bits for extremely valuable keys like the root key pair used by a certifying authority ~~-~~"

  see http://www.rsasecurity.com/rsalabs/faq/3-1-5.html

- Issuer name is the same as the subject name in the roaming CA~~Domain authority~~ cert.
- Extensions:
  - Optionally non critical authority key identifier
  - Optionally non critical subject key identifier
  - Mandatory non-critical subjectAltName
  - Mandatory critical key usage: At least digitalSignature and keyEncipherment shall be set.
  - Optional critical ~~enhanced~~ extended key usage: If present, at least server authentication and IKE intermediate shall be set
  - Mandatory ~~non~~ critical Distribution points: CRL distribution point

5.3.1.4 Cross Certificate profile

In addition to clause 5.3.1.1, following requirements apply:

- Subject name is the same, which the authority of the other domain uses in it’s certificates
- Issuer Name is the same as used for signing our entities
- Extensions:
  - Optionally non critical authority key identifier
  - Optionally non critical subject key identifier
  - Mandatory critical key usage: At least keyCertSign and CRL Sign, should be asserted

- Mandatory critical basic constraints: CA=True, path length 0.

5.3.2 IKE negotiation and profiling

[Editor's note: A more detailed check on using draft-ietf-ipsec-pki-profile-02.txt *as the main profiling base is needed. It needs to be assessed why and how we want to deviate from these papers]*

5.3.2.1 IKE Phase-1 profiling

The Internet Key Exchange protocol shall be used for negotiation of IPsec SAs. The following requirements on IKE in addition to those specified in NDS/IP [1] are made mandatory for inter-security domain SA negotiations over the Za-interface.

For IKE phase-1 (ISAKMP SA):

- The use of RSA signatures for authentication shall be supported.
- The identity of the CERT payload (including the SEG certificate) shall be used for policy checks.

  Motivation: ISAKMP contains two different payloads that allow the specification of the endpoint identity, the ID payload and the CERT payload. Within the NDS/AF framework only the SEG certificate is sent within IKE Phase 1 so there will be no ambiguity is selecting the peer ID from the received certificates. See also section 3.1.2 of draft-ietf-ipsec-pki-profile-02.txt on Endpoint identification.
- Initiating/responding SEG are required to send certificate requests in the IKE messages

  Motivation: suggested by draft-ietf-ipsec-pki-profile-02.txt to avoid interoperability problems
- Cross-certificates shall not be send by the peer SEG as they are pre-configured in the SEG.

  Motivation: avoiding known problems (see clause 5.3.5.2)
- The SEG shall always send its own certificate in the certificate payload of the last (third) Main Mode message

  Motivation: avoids the need to cache Peer SEG certificates.
- The certificates in the certificate payload shall be encoded as type 4 (X.509 Certificate – Signature).
- The lifetime of the Phase-1 IKE SA shall be limited to at most the remaining validity time of the peer SEG certificate.

5.3.2.2 Potential interoperability issues

Some PKI-capable VPN gateways do not support fragmentation of IKE packets, which becomes an issue when more than one certificate is sent in the certificate payloads, forcing IKE packet fragmentation. This means that direct cross-certification or manually importing the peer CA certificate to the local SEG and trusting it is preferable to bridge CA systems. When IKE is run over pure IPv6 the typical MTU sizes do not increase and long packets still have to be fragmented (allowed for end UDP hosts even for IPv6, see Path MTU Discovery for IPv6 – [6]), so this is a potential interoperability issue.

Certificate encoding with PKCS#7 is supported by some PKI-capable VPN gateways, but it shall not be used.

5.3.3 Path validation

5.3.3.1 Path validation profiling

- Validity of certificates received from the peer SEG shall be verified by CRLs retrieved with LDAP, based on the CRL Distribution Point in the certificates.
- A SEG shall not validate received certificates from the peer SEG whose validity time has expired, but end the path validation with a negative result.

- A SEG shall not validate received certificates from the peer SEG whose CRL distribution point field is empty, but end the path validation with a negative result.
- Certificate validity calculation results shall not be cached for longer than the resulting IKE phase-1 lifetime.