3GPP TSG SA WG3 Security — S3#31 **S3-030706**
18 - 21 November 2003
Munich, Germany

CR-Form-v7

PSEUDO CHANGE REQUEST

⌘ **33.310** **CR** **-** ⌘**rev** **-** ⌘ Current version: 0.6.0 ⌘

*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:	⌘	Recommendation to SEG certificate and IKE profiling
Source:	⌘	Nokia, Siemens, Vodafone
Work item code:	⌘	NDS/AF
Date:	⌘	07/11/2003
Category:	⌘	**C**
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:	⌘	Different address types in subjectAltName and ISAKMP would require secure DNS usage. Three alternatives in NDS/AF context: 1) ISAKMP policy and subjectAltName both have IP-address - no additional mapping is needed 2) ISAKMP policy and subjectAltName both have FQDN - initial policy lookup based on IP-address is needed, because CERT- and ID-payloads are obtained in the end of the IKE negotiation -> DNS required 3) ISAKMP policy has IP-address and subjectAltName has FQDN, or vice versa - initial policy lookup based on IP-address is needed, because CERT- and ID-payloads are obtained in the end of the IKE negotiation - additionally secure mapping between IP-address and FQDN is needed -> secure DNS
Summary of change:	⌘	Added clarification that depending on availability of DNS between operators, either IP address-IP address or FQDN-FQDN in both subjectAltName & ISAKMP policy shall be used.
Consequences if not approved:	⌘	Secure DNS usage required in some cases.

Clauses affected:	⌘	6.1, 6.1.3, 6.2.1			
		Y	**N**		
Other specs affected:	⌘		**N**	Other core specifications	⌘
			N	Test specifications	
			N	O&M Specifications	
Other comments:	⌘	-			

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

---------- FIRST CHANGED SECTION ----------

6.1 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]*~~

---------- NEXT CHANGED SECTION ----------

6.1.3 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 6.1.1, 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 certificate.
- 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 extended key usage: If present, at least server authentication and IKE intermediate shall be set
  - Mandatory critical Distribution points: CRL distribution point

NOTE: depending on the availability of DNS between peer SEGs, the following rule is applied:

- subjectAltName should contain IP address (in case DNS is not available)
- subjectAltName should contain FQDN (in case DNS is available)

---------- NEXT CHANGED SECTION ----------

6.2.1 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.

NOTE: depending on the availability of DNS between peer SEGs, the following rule is applied:

- subjectAltName and ISAKMP policy should both contain IP address (in case DNS is not available)
- subjectAltName and ISAKMP policy should both contain FQDN (in case DNS is available)