3GPP TSG SA WG3 Security — S3#31 **S3-030677**
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:	⌘	Clarification of SEG certificate profiling
Source:	⌘	Nokia, Siemens, T-Mobile, Vodafone
Work item code:	⌘	NDS/AF
Date:	⌘	06/11/2003
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: ⌘ If a SEG may use more than one certificate for itself within NDS/AF (e.g. signed by different CAs), it is not defined which one should be sent during the IKE exchange.

A peer SEG A learns the remote roaming CA's identity only after it received the certificate of the remote SEG B. Therefore, it can not insert the CA identity in advance into its certification request.
If SEG B is allowed to have multiple certificates for itself, it also does not generally know in advance, which one to use during IKE exchange with SEG A.

Summary of change: ⌘ Added clarification that each SEG shall use only one certificate for itself within NDS/AF.

Consequences if not approved: ⌘ Potential for interoperability problems.

Clauses affected: ⌘ 6.1.3

Other specs affected: ⌘

Y	N	
	N	Other core specifications ⌘
	N	Test specifications
	N	O&M Specifications

Other comments: ⌘ -

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. Any SEG shall use exactly one certificate to identify itself within the NDS/AF.

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