3GPP TSG SA WG3 Security — S3#32 **S3-040022**
09 - 13 February 2004, Edinburgh, Scotland, UK

CR-Form-v7

PSEUDO CHANGE REQUEST

⌘ **33.310** **CR** ⌘ **rev** **-** ⌘ Current version: **1.0.0** ⌘

*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 **X**

Title:	⌘	Clarification on the SA lifetimes
Source:	⌘	Siemens, Nokia, T-mobile, Vodafone
Work item code:	⌘	NDS/AF
Date:	⌘	28/01/2004
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: ⌘ * Removal of Editors note in section 7.6

1) as clause 6.2.1 already contains an ISAKMP lifetime restriction statement.

'- *The lifetime of the Phase 1 IKE SA shall be limited to at most the remaining validity time of the peer SEG certificate.'*

2) If the operator removes compromised ISAKMP SA (see Clause 5.2.12) when the SEG certificate has to be revoked, then setting rules on ISAKMP SA lifetimes, that take into account CRL update cycles, has no merit from a security point of view. Compromised ISAKMP SA's will be removed anyhow.

"If a SEG key pair gets compromised then the existing SAs shall be removed using device-specific management methods."

** Correction of certificate lifetime for ISAKMP SA in clause 6.2.1*

Summary of change: ⌘

Consequences if not approved: ⌘

Clauses affected: ⌘ 6.2.1 IKE phase-1 Profiling
7.6 CRL management

Other specs affected: ⌘	Y	N		⌘
	☐	☐	Other core specifications	
	☐	☐	Test specifications	
	☐	☐	O&M Specifications	

Other comments: ⌘

*** begin of change ***

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 sent 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) IKE 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 (ISAKMP SA) shall be limited to at most the remaining validity time of both ~~the~~ peer SEG certificates.

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).

*** End of change ***

*** begin of change ***

7.6 CRL management

NDS/AF compliant SEGs shall not sent an ISAKMP CERTREQ where the Certificate Type is "Certificate Revocation List (CRL)". Receiving SEGs may ignore this request as section 6.1.3 specifies that CRLs shall be retrieved via a CRL distribution point.

The CRL issuer (which is in most cases the CA) shall only issue full CRLs. The use of delta CRLs is not allowed because of possible interoperability problems and because in the NDS/AF environment the full CRL is not expected to grow too large. The full CRL shall only contain revoked certificates applicable for use within NDS/AF. The CRL issuer

shall issue a CRL also in cases that there are no revoked certificates. A SEG is not obliged to query for a CRL via the CRL Distribution Point if a cached one is still available and valid. If no valid cached CRL is available, the SEG shall fetch a new CRL. If no valid CRL can be fetched, the SEG shall treat this as an error and cancel tunnel establishment.

~~Editor's note: It is for ffs whether the ISAKMP SA lifetime shall be restricted to at most the remaining time+ delta defined within the CRLs NextUpdate *field. This might result in following guideline min(Cert. chain lifetime, CRLs lifetimes) >= IKE SA lifetime >= IPsec SA lifetime*~~

*** End of change ***