TSGS#24(04)0393

Source: **SA WG3 (Security)**

Title: **CR to 33.310: Removal of inconsistencies regarding SEG actions during IKE phase 1 (Rel-6)**

Document for: **Approval**

Agenda Item: **7.3.3**

SA Doc number	Spec	CR	Rev	Phase	Subject	Cat	Version-Current	SA WG3 Doc number	Workitem
SP-040393	33.310	001	-	Rel-6	Removal of inconsistencies regarding SEG actions during IKE phase 1	F	6.0.0	S3-040266	SEC1-NDS-AF

3GPP TSG-SA WG 3 Security Meeting #33
Beijing, China, 10-14 May 2004

Tdoc ⌘S3-040266

CR-Form-v7

CHANGE REQUEST

⌘ **33.310** **CR** **001** ⌘**rev** **-** ⌘ Current version: **6.0.0** ⌘

*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:	⌘	Removal of inconsistencies regarding SEG actions during IKE phase 1
Source:	⌘	SA WG3
Work item code:	⌘	SEC-NDS-AF
Date:	⌘	30/04/2004
Category:	⌘	**F**
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:	⌘	a) CRL check for cross certificate and verification of roaming CA certificate steps should be included in section 5.2.2 for alignment/consistency with section 7.5. b) As defined in section 5.2.2, the signature on the IKE message should be verified before the certificate chain is processed. Section 7.5 should be aligned with section 5.2.2 in this respect, i.e. step 9 should be moved so that it happens after step 2.
Summary of change:	⌘	The above changes are implemented.
Consequences if not approved:	⌘	Inconsistencies remain in the specification which could lead to implementation difficulties or interoperability problems.

Clauses affected:	⌘	5.2.2, 7.5

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

Other comments:	⌘	

5.2.2 VPN tunnel establishment

After establishing a roaming agreement and finishing the required preliminary certificate management operations as specified in the previous section, the operators configure their SEGs for SEG-SEG connection, and the SAs are established as specified by NDS/IP [1].

In each connection configuration, the remote SEG DNS name or IP address is specified. Only the local roaming CA is configured as the trusted CA. Because of the cross-certification, any operator whose roaming CA has been cross-certified can get access using this VPN connection configuration

The following is the flow of connection negotiation from the point of view of Operator A's SEG (initiator). Operator B's SEG (responder) shall behave in a similar fashion.

- During connection initiation, the initiating Operator A's SEG A provides its own SEG certificate and the corresponding digital signature in IKE Main Mode message 3;
- SEG A receives the remote SEG B certificate and signature;
- SEG A validates the remote SEG B signature;
- SEG A verifies the validity of the SEG B certificate by a CRL check to both the Operator A and Operator B CRL databases. If a SEG cannot successfully perform both CRL checks, it shall treat this as an error and abort tunnel establishment;
- ~~—~~SEG A validates the SEG B certificate using the cross-certificate for Operator B by executing the following actions:
    - SEG A verifies the validity of the cross-certificate for Operator B by a CRL check to the Operator A CRL database. If a SEG cannot successfully perform the CRL check, it shall treat this as an error and abort tunnel establishment.
    - SEG A validates the cross-certificate for Operator B using its roaming CA's certificate if the roaming CA is not a top-level CA, otherwise the roaming CA's public key is implicitly trusted.
- The~~. An~~ IKE Phase 1 SA is established and the Phase-2 SA negotiation proceeds as described in NDS/IP [1] with PSK authentication.

~~SEG A verifies the validity of the cross-certificate for Operator B by a CRL check to the Operator A CRL database. If a SEG cannot successfully perform the CRL check, it shall treat this as an error and abort tunnel establishment.~~

~~SEG A validates the cross-certificate for Operator B using its roaming CA's certificate if the roaming CA is not a top-level CA, otherwise the roaming CA's public key is implicitly trusted.~~

NOTE: This specification provides authentication of SEGs in an "end-to-end" fashion as regards to roaming traffic (operator to operator). If NDS/AF (IKE) authentication were to be used for both access to the transport network (e.g. GRX) and for the end-to-end roaming traffic, IPsec mechanisms and policies such as iterated tunnels or hop-by-hop security would need to be used. However, it is highlighted that the authentication framework specified is independent of the underlying IP transport network.

7.5 Authentication during the IKE phase 1

Authentication during IKE Phase 1 is shown in Figure 4 above. The SEGa uses the following procedure to authenticate SEGb:

1. SEGa requests SEGb's certificate using the IKE certificate request payload;
2. SEGa receives SEGb's certificate inside the IKE certificate payload;
3. SEGa authenticates SEGb (verifies signatures);
4. SEGa fetches a CRL from the (public) CRLb if the locally cached CRL has not yet expired;

5~~4~~. SEGa uses this CRL to verify the status of SEGb's certificate;

6~~5~~. SEGa uses either the locally cached cross-certificate or fetches the cross-certificate from the (local) CRa;

7~~6~~. SEGa fetches a CRL from the (local) CRLa if the locally cached CRL has not yet expired;

8~~7~~. SEGa uses this CRL to verify the status of the cross-certificate;

9~~8~~. SEGa verifies the status of the roaming CAa certificate if the roaming CAa is not a top-level CA, otherwise roaming CAa is implicitly trusted.~~;~~

~~9. SEGa authenticates SEGb (verifies signatures).~~

NOTE: A cross-certificate only needs to be checked if SEGa and SEGb belong to different CAs.