3GPP TSG SA WG3 Security — S3#32 **S3-040093**
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:	⌘	Certificate issuer name limitations removal
Source:	⌘	Nokia, Siemens, T-Mobile
Work item code:	⌘	NDS/AF
Date:	⌘	02/02/2004
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:	⌘	No need identified for certificate issuer name limitations. Access limitation to operator's certain region or subnet behind SEG can be achieved by operator's IPsec policy management.
Summary of change:	⌘	Removed text on certificate issuer name limitations
Consequences if not approved:	⌘	Need for certificate issuer name limitations would be unclear.

Clauses affected:	⌘	5.2.2 VPN tunnel establishment

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

Other comments:	⌘	-

---------- CHANGED SECTION ----------

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. ~~If access to a certain local subnet is allowed for only certain operators, the VPN connection configuration shall include limitations for certificate issuer name.~~

~~Editor's note: These limitations for certificate issuer name are ff.~~

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. An IKE Phase 1 SA is established and the Phase-2 SA negotiation proceeds as described in NDS/IP [1] with PSK authentication.

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.