3GPP TSG SA WG3 Security — S3#29 **S3-030388**
15 - 18 July 2003, San Francisco, USA

CR-Form-v7

PSEUDO CHANGE REQUEST

⌘	**ab.cde**	**CR**	**CRNum**	⌘ **rev**	**-**	⌘	Current version:	0.3.0	⌘

*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:	⌘	Addition of text on usecases		
Source:	⌘	Siemens, Nokia, SSH, T-Mobile		
Work item code:	⌘	NDS/AF	***Date:*** ⌘	07/07/2003
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:	⌘	Inclusion of missing operational usecases for various scenarios
Summary of change:	⌘	
Consequences if not approved:	⌘	

Clauses affected:	⌘	5.2				
		Y	**N**			
Other specs affected:	⌘		**N**	Other core specifications	⌘	
			N	Test specifications		
			N	O&M Specifications		
Other comments:	⌘					

5.2 Use cases

5.2.1 Operator Registration: Creation of r~~R~~oaming agreement

Security gateways (SEG’s) of two different security domains need to establish a secure tunnel, when the operators make a roaming agreement. The first technical step in creating the roaming agreement between domains is the cross-certification of the roaming CAs of the two domains.

Inter-operator cross-certification can be done using different protocols, but the certification authority shall support the PKCS#10 [2] method for certificate requests. Both roaming CAs create a PKCS#10 certificate request, and send it to the other operator. The method for transferring the PKCS#10 request is not specified, but the transfer method shall be secure. The PKCS#10 can be transferred e.g. in a floppy disk, or be send in a signed email. The PKCS#10 request contains the public key of the authority and the name of the authority. When roaming CA accepts the request, a new cross-certificate is created. The authority shall make that new certificate available to SEGs in his own domain, by storing the new cross-certificate into all SEGs that need to communicate with the other domain.

When creating the new cross-certificate, the roaming CA should use basic constraint extension (according to section 4.2.1.10 of [3]) and set the path length to zero. This inhibits the new cross-certificate to be used in signing new CA certificates. The validity of the certificate should be set sufficiently long. The cross-certification process needs to be done again when the validity of the cross-certificate is ending. The validity time could be e.g. 15 years. The start time of the validity should start e.g. a day before the actual roaming is set to start in order to avoid problems with different time zones. Problems in PKI are often due to the time differences.

When the new certificate is available for SEG, all that needs to be configured in SEG is the DNS name of the peering SEG gateway. The authentication can be done based on created cross-certificates.

When the cross-certification is implemented this way, the PKI architecture seems hierarchical to the network elements in the domain: At the very top of the hierarchy sits the roaming CA of the domain. At the second level, there are certificates directly issued by roaming CA for the SEGs together with the cross certificate issued for the peering domains. The certificates of the peer domains are located under the cross-certificates of the peer domains.

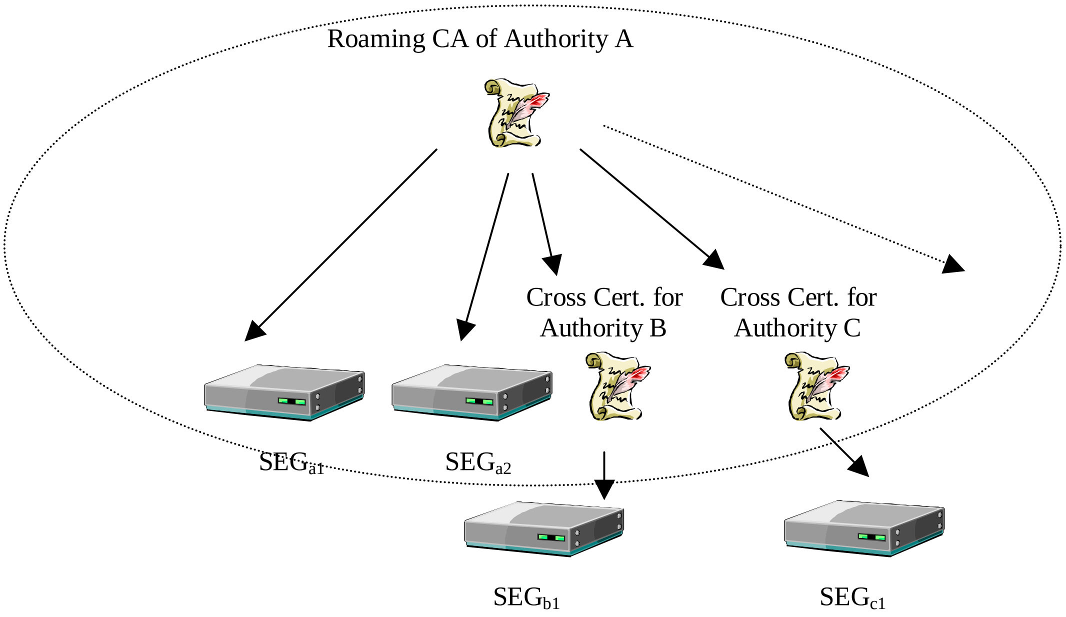
Roaming CA of Authority A
Cross Cert. for Authority B
Cross Cert. for Authority C
SEG$_{a1}$
SEG$_{a2}$
SEG$_{b1}$
SEG$_{c1}$

Figure 3: Security domain A illustrated. The PKI is hierarchical inside the domain.

5.2.2 VPN tunnel establishment

After establishing a roaming agreement and finishing 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 is specified. Only 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 ffs.]

Following is the flow of connection negotiation from the point of view of Operator A's SEG (initiator). Operator B 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 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 B CRL databases. If a SEG cannot successfully perform both CRL checks, it shall treat this as an error and abort tunnel establishment. IKE Phase-1 SA is established, and the Phase-2 SA negotiation proceeds as described with 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.

5.2.3 Operator deregistration: Termination of roaming agreement

When a roaming agreement is terminated or due to an urgent service termination need, all concerned peers shall remove the SAs using device-specific management methods. Each concerned operator shall also list the cross-certificate created for the roaming CA of the terminated operator in his own local CRL.

5.2.4 Roaming CA registration

In principle only one roaming CA shall be used within the operator's network, but using more than one roaming CA is possible. The involved actions are those as described in cross-certification part of clause 5.2.1: ‘Operator Registration: creation of roaming agreement’. Such a situation may exist if the roaming CA functions are to be moved from one responsible organisation to another (e.g. outsourcing of CA services).

5.2.5 Roaming CA deregistration

If a roaming CA is removed from the network, it shall be assured that all cross-certificates and certificates that have been issued by that roaming CA, and have not expired yet, shall be listed in the CRLs.

5.2.6 Roaming CA certificate creation

The roaming CA certificate may not be the top-level CA of the operator, which means that the Roaming CA certificate is not self-signed. If the roaming CA certificate is self-signed then it needs to be securely transferred to each SEG and stored within secure memory otherwise it can be managed in the same way as a SEG-certificate.

The roaming CA certificate shall have a ‘longer’ lifetime in order to avoid the cross-certification actions that are needed each time a roaming CA certificate has to be renewed.

5.2.7 Roaming CA certificate revocation

If a roaming CA key pair gets compromised then a hacker could use the keys to issue himself cross-certificates. Since however the trusted cross-certificates are stored locally on the device or in a dedicated repository (So received cross-certificates within the IKE payload shall not accepted), the hacker also needs to compromise the SEG or the local repository to be able to set up an IPsec tunnel.

Existing IPsec tunnels need not to be torn down. The operator has to create a new roaming CA certificate, initiate new cross-certification and SEG certificates as if he would create new roaming agreements with all his partner networks. The old cross-certificates and certificates can be taken out of service by listing them in the CRL.

5.2.8 Roaming CA certificate renewal

The Roaming CA certificate has to be renewed before the old roaming CA certificate expires. The renewing of a roaming CA certificate results in the need to renew the cross-certificates. This should be done before the old expire.

5.2.9 SEG registration

If not already done, a SEG certificate has to be created (See clause 5.2.11 for a description on certificate creation)

If a SEG is added to the network, the policy database of this SEG has to be configured using device-specific management methods.

Other operators have to be informed of the new SEG: The SEG policy databases of SEGs in other networks may have to adapted

~~5.2.4~~5.2.10 SEG deregistration

If a SEG is removed from the network, the SAs shall be removed using device-specific management methods.~~as above~~. The operator of the SEG shall have the certificate of the SEG listed in his CRL. The SPD of partner network may have to be adapted.

5.2.11 SEG certificate creation

Using device specific management methods, the certificate creation is initiated. The CMPv2 protocol is used between the roaming CA and the SEG for automatic certificate enrolment.

5.2.12 SEG certificate revocation

If a SEG key pair gets compromised then the existing SAs shall be removed using device-specific management methods. The operator of the SEG shall have the certificate of the SEG listed in his CRL.

5.2.13 SEG certificate renewal

A new SEG certificate needs to be in place before the old SEG certificate expires. The procedure is similar to the SEG certificate creation and if fully automated by CMPv2.

~~*[Editor's note:*~~

~~*Two new paragraphs needed to describe the involved actions for revocation and check our model !?*~~

~~*Roaming CA certificate revocation ?*~~

~~*A)of the own roaming CA*~~

~~*B)of a partner roaming CA*~~

~~*SEG revocation*~~

~~*A)own SEG*~~

~~*B)*~~*A)* ~~*SEG of a roaming partner]*~~