3GPP TSG-SA WG3 Meeting #30
Povoa de Varzim, Portugal, 6-10 October 2003

Tdoc ⌘S3-030574

CR-Form-v7

CHANGE REQUEST

⌘	**33.310**	**CR**		⌘**rev**	**-**	⌘	Current version:	**0.5.0**	⌘

*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:	⌘	Clarifications to usage of certificate repositories			
Source:	⌘	Nokia, Siemens, SSH, T-Mobile, Vodafone			
Work item code:	⌘	NDS/AF	***Date:***	⌘	29/09/2003
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:	⌘	To clarify usage of certificate repositories and certificate revocation lists.
Summary of change:	⌘	
Consequences if not approved:	⌘	

Clauses affected:	⌘	Modified: 3.1, 3.2, 5.2.1, 5.2.2, 5.2.6, 7.1, 7.3 and 7.5				
		Y	**N**			
Other specs affected:	⌘		**N**	Other core specifications	⌘	
			N	Test specifications		
			N	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

Local CR: Repository that contains cross-certificates

Local CRL: Repository that contains cross-certificate revocations

PSK: Pre-Shared Key. Method of authentication used by IKE between SEG in NDS/IP [1].

Public CRL: Repository that contains revocations of SEG and CA certificates and can be accessed by other operators

Roaming CA: The CA that is responsible for issuing certificates for SEG that have interconnection with another operator

Next modified section

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AF	Authentication Framework
CA	Certification Authority
CR	Certificate Repository
CRL	Certificate Revocation List
NDS	Network Domain Security
SEG	Security Gateway
Za	Interface between SEGs belonging to different networks/security domains (a Za interface may be an intra or an inter operator interface).
Zb	Interface between SEGs and NEs and interface between NEs within the same network/security domain

Next modified section

5.2.1 Operator Registration: Creation of roaming 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 local CR (Certificate Repository) ~~(CR)~~ which all SEGs that need to communicate with the other domain shall access with LDAP. The cross-certification is a manual operation, and thus PKCS#10 is a suitable solution for the roaming agreement.

[Editor's note: CMPv2 as a protocol has cross-certification capabilities as well, but that functionality is not considered to be implemented widely enough or interoperable.]

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.

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.

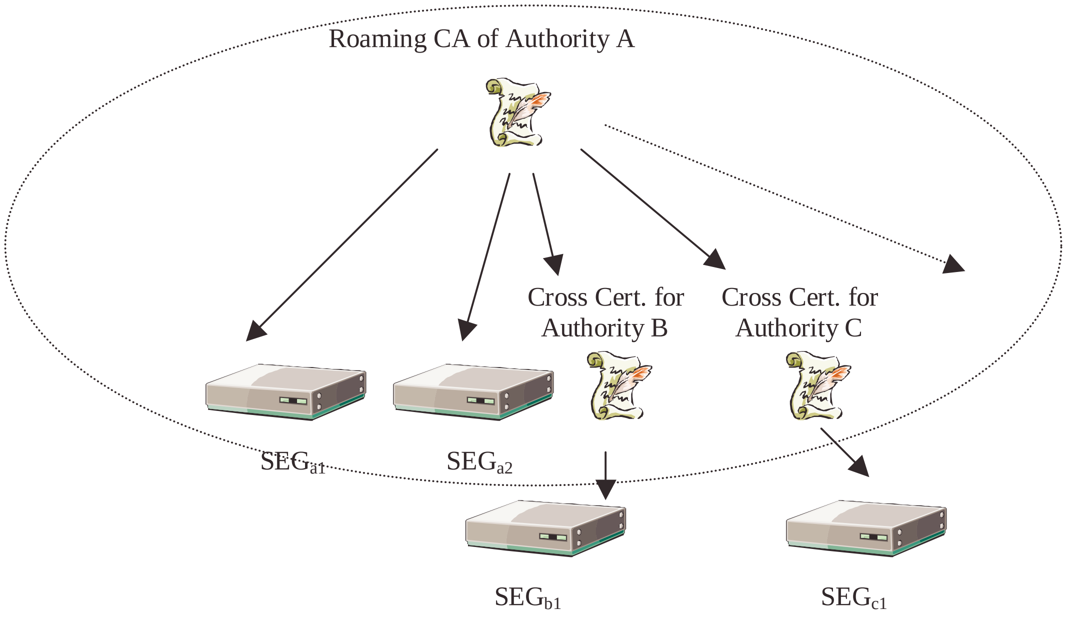
Roaming CA of Authority A
Cross Cert. for Authority B
Cross Cert. for Authority C
SEG$_{a1}$
SEG$_{a2}$
SEG$_{b1}$
SEG$_{c1}$

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

Next modified section

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.

- SEG A validates the SEG B certificate using the cross certificate for Operator B.

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.

Next modified section

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 than cross-certificates and SEG certificates in order to avoid the cross-certification actions that are needed each time a roaming CA certificate has to be renewed.

Next modified section

7.1 Repositories

During VPN tunnel establishment, each SEG has to verify the validity of it's peer SEG's certificate according to section 5.2.2. Any certificate could be invalid because it was revoked (and replaced by a new one) or a SEG or operator has been deregistered.

SEG$_B$ has to verify that

a) the cross-certificate of CA$_A$ is still valid

b) the certificate of SEG$_A$ is still valid

and be able to

c) fetch the cross-certificate of CA$_A$ (if not found in SEG$_B$‘s cache)

SEG$_A$ performs according checks from its own perspective.

Check a) can be performed by querying the local CRL. For check b), a CRL of the peering CA shall be queried. At this point of time, the VPN tunnel is not yet available, therefore the public CRL of the peering CA shall be accessible for a SEG without utilising Za interface.

The Figure 4 illustrates the repositories and the above mentioned steps a) – c). The local CR contains cross-certificates, the local CRL contains cross-certificate revocations, and the public CRL contains revocations of SEG and CA certificates and can be accessed by other operators.

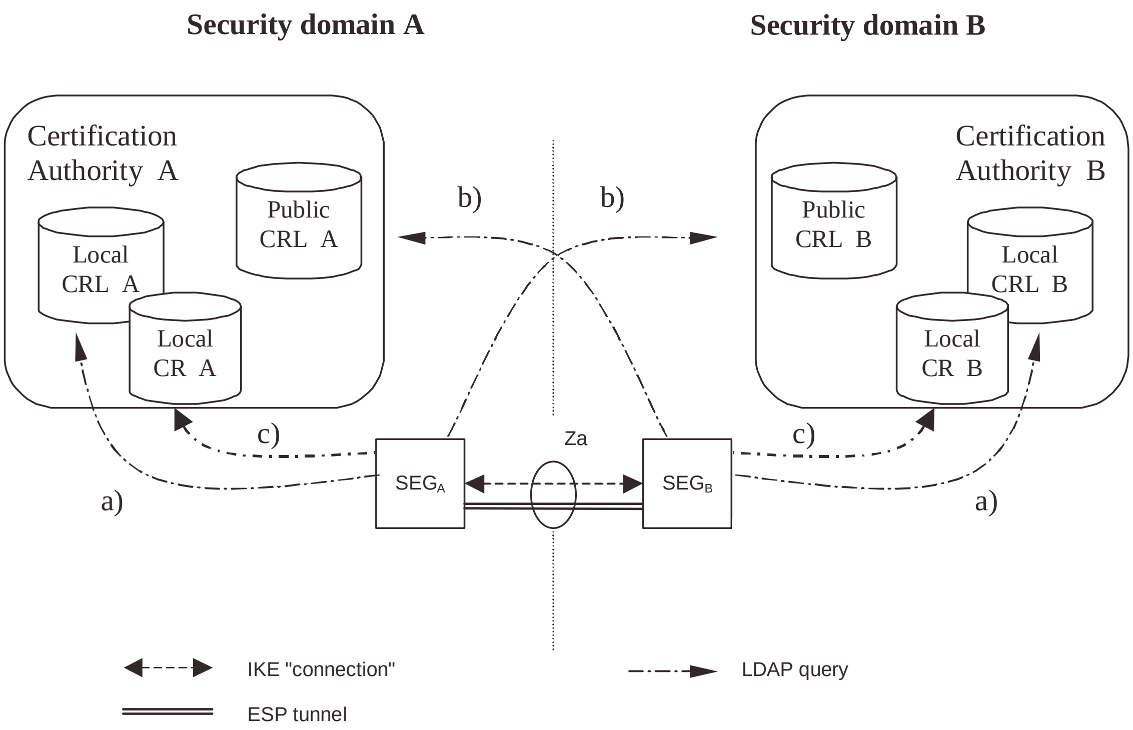

Figure 4: ~~CRL~~ Repositories

The public and local ~~CRL~~ repositories of a CA may be implemented as ~~two~~ separate databases or as a single database which is accessible via two different interfaces. Access to the "public" CRL is public with respect to the interconnecting transport network (e.g. GRX). The public CRL should be adequately protected (e.g by a firewall) and the owner of the public CRL may limit access to it according to his roaming agreements.

SEGs shall use LDAP to access the CRL and cross-certificate repositories.

[Editor's note: Further specification of public CRL interface and its relation to Za is ffs.]

Next modified section

7.3 Cross-certification

Both operators use the following procedure to create cross-certificates:

1. The roaming CA creates a PKCS#10 certificate request, and sends it to the other operator.
2. The roaming CA receives a similar request from the other operator.
3. The roaming CA accepts the request and creates a new cross-certificate.
4. The cross-certificate is stored once into the local CR and LDAP is used to fetch cross-certificates.

Next modified section

7.5 Authentication during the IKE phase 1

Authentication during the IKE Phase 1 is shown in the Figure 4 above. The SEGa uses the following procedure to authenticate the 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 fetches a CRL from the (public) CRLb if the locally cached CRL has not yet expired.

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

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

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

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

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

9. SEGa authenticates the SEGb (verifies signatures)

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