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:	⌘	Fetching cross-certificates
Source:	⌘	Nokia, Siemens, SSH, T-Mobile
Work item code:	⌘	NDS/AF
Date:	⌘	08/07/2003
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:	⌘	Implementing the proposal for working assumption (i.e. cross-certificates are stored into CRs, fetched with LDAP and cached in SEGs) in 'Fetching cross-certificates' discussion paper
Summary of change:	⌘	
Consequences if not approved:	⌘	

Clauses affected:	⌘	5.2.1, 6.1, 6.3 (new), 6.4 (new), 6.5 (new), Annex X (new)

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

Other comments: ⌘

---------- FIRST CHANGED SECTION ----------

5.2 Use cases

5.2.1 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 Certificate Repository (CR) which all SEGs that need to communicate with the other domain shall access with LDAP.

---------- NEXT CHANGED SECTION ----------

6.1 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

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.

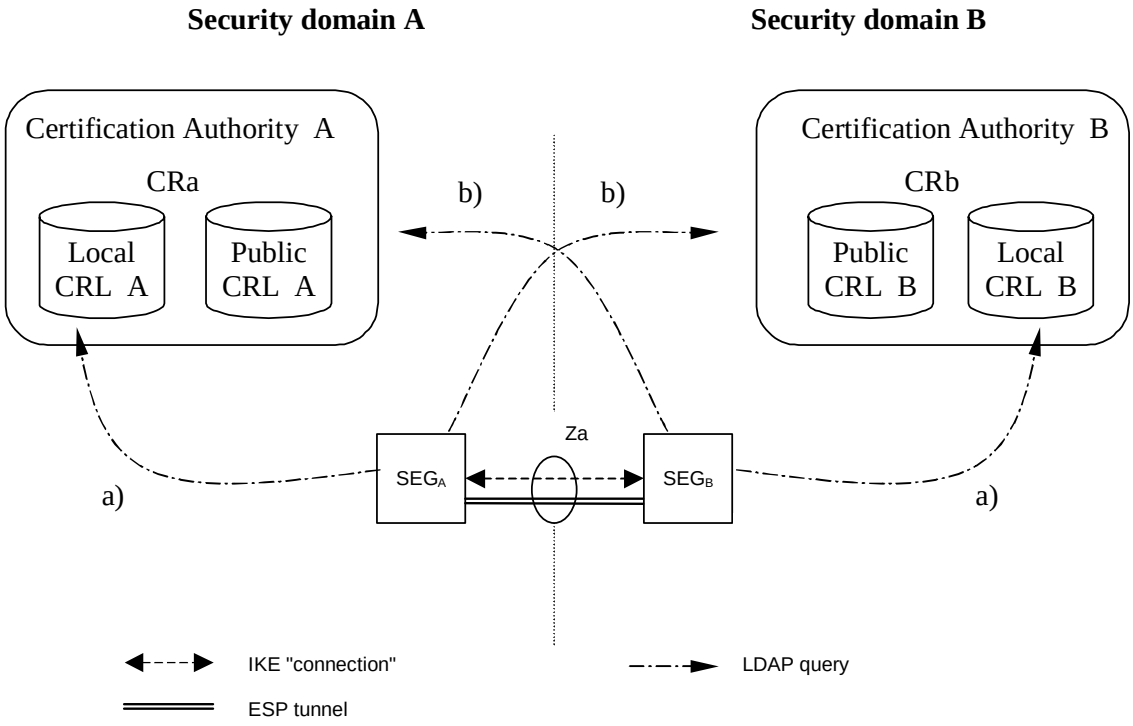

Figure 4: CRL Repositories

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 ADDED SECTIONS ----------

6.3 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 CR and LDAP is used to fetch cross-certificates.

6.4 Revoking a cross-certificate

The following procedure is used to revoke a cross-certificate:

1. The cross-certificate is added into the CRL.
2. The cross-certificate is removed from the CR.

6.5 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) CRb 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) CRa 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)

---------- LAST ADDED SECTION ----------

Annex X <informative>:
Decision for storing the cross-certificates in CR

In order to document the decision for storing the cross-certificates in Certificate Repository, fetching those with LDAP and caching them in SEGs, this section summarises technical advantages and disadvantages of the three alternatives.

The following table summarizes differences between alternatives:

Issue	**A) Cross-certificates are stored into SEGs:**	**B) Cross-certificates are stored into CRs:**	**C) Cross-certificates are stored into CRs and cached in SEGs upon usage:**
1) Initialization issues: storing the cross-certificate during the cross-certification	The cross-certificate is *initially* stored in several places, that is, into *all* SEGs (estimated number is between 2 and 10). Pros: - Cons: Certificate must be initially copied in several places. SEGs from different manufacturers may have other O&M interfaces to handle the certificates.	The cross-certificate is *initially* stored in CR. Pros: The handling is fully standardized. Certificate is initially copied in one place only. The operator should have the repository anyway (due to CRL handling). Cons: -	The cross-certificate is *initially* stored in CR. Pros and cons as in B).
2) Usage issues: latency during the IKE Phase 1	Pros: No extra latency Cons: -	Pros: - Cons: More latency caused by extra LDAP query (the cross-certificate is queried)	Pros & cons: as in B) at the first time, and as in A) at subsequent times
3) Cleanup issues: removing the cross-certificate NOTE: this functionality is needed only to be able to revoke cross-certificates before the next CRL gets published.	Pros: - Cons: The cross-certificate has to be removed from several places, that is, from *all* SEGs	Pros: The cross-certificate has to be removed from one single place only Cons: -	Pros: - Cons: The cross-certificate has to be removed from *both* CR *and* each SEG.
4) Security issues	Pros: No single point of failure exists. Cons: -	Pros: - Cons: CR represents a single point of failure suitable for an attacker,	Pros: Single point of failure partly mitigated Cons: -

		e.g. to submit a denial of service attack by breaking the communication at the CR.	

Analysis:

- Alternative B) requires one additional LDAP query in every IKE Phase 1 negotiation and will introduce new error cases
- Latency of LDAP: information from LDAP to local disk is cached and populating it takes some time, but in practice this time is not significant.
- The benefit of alternative B) and C) compared to alternative A) is easier management, that is, storing and removing the certificate in/from one single place only.

Conclusion: alternative C) is the most feasible choice, because it combines good points of alternatives A) and B).