

CR-Form-v7
PSEUDO CHANGE REQUEST
⌘ 33.310 CR - ⌘ rev - ⌘ Current version: 0.6.0 ⌘

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:	⌘ Local repository access clarification		
Source:	⌘ Nokia, Siemens, T-Mobile, Vodafone		
Work item code:	⌘ NDS/AF	Date:	⌘ 10/11/2003
Category:	⌘ D	Release:	⌘ Rel-6
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	F (correction)		2 (GSM Phase 2)
	A (corresponds to a correction in an earlier release)		R96 (Release 1996)
	B (addition of feature),		R97 (Release 1997)
	C (functional modification of feature)		R98 (Release 1998)
	D (editorial modification)		R99 (Release 1999)
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Rel-4 (Release 4)
			Rel-5 (Release 5)
			Rel-6 (Release 6)

Reason for change:	⌘ Local interfaces needed for locating the data used for functions in Za interface.
Summary of change:	⌘ Added clarification on local repository relationship to the Za interface.
Consequences if not approved:	⌘ Not interoperable SEG and repository implementations.

Clauses affected:	⌘ 7.1									
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="width: 20px; text-align: center;"><input type="checkbox"/></td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="width: 20px; text-align: center;"><input type="checkbox"/></td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="width: 20px; text-align: center;"><input type="checkbox"/></td> <td style="width: 20px; text-align: center;">N</td> </tr> </table> Other core specifications	Y	N	<input type="checkbox"/>	N	<input type="checkbox"/>	N	<input type="checkbox"/>	N	⌘
	Y	N								
	<input type="checkbox"/>	N								
<input type="checkbox"/>	N									
<input type="checkbox"/>	N									
	Test specifications									
	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.

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

7.1 Repositories

During VPN tunnel establishment, each SEG has to verify the validity of its 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.

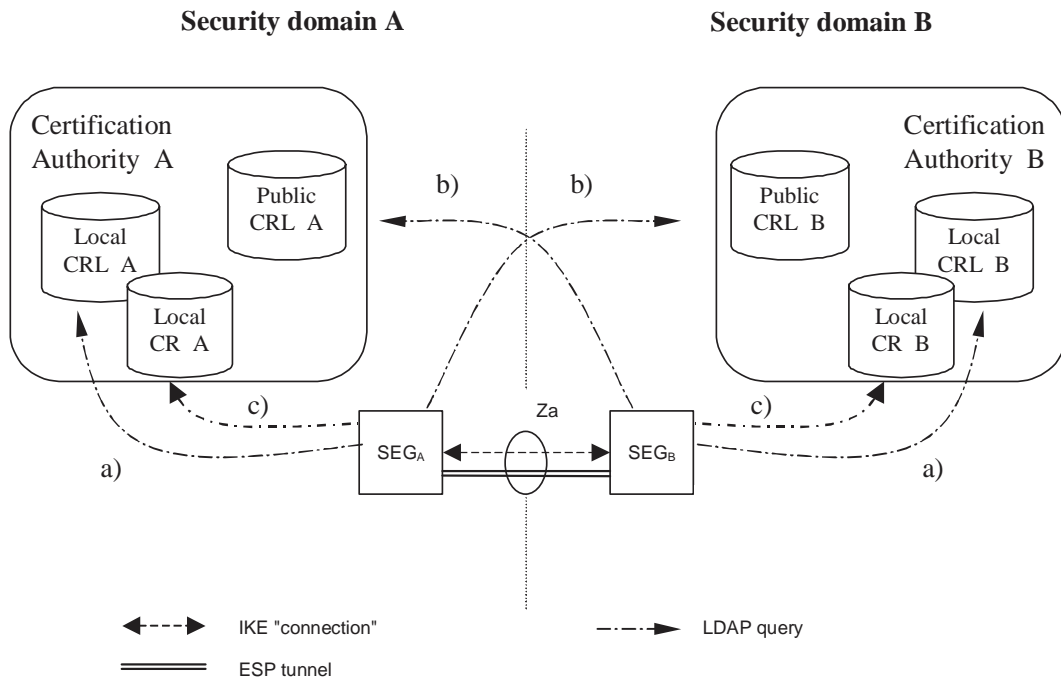


Figure 4: Repositories

The public and local repositories of a CA may be implemented as 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.

NOTE: Interfaces a) and c) for locating the data used for functions in Za interface belong to the scope of NDS/AF (in addition to public b) interface) as the purpose is to guarantee the interoperability between different SEG and repository implementations. The possible migration to the cross-certification with a Bridge CA would also require these interfaces to be specified.

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