3GPP TSG SA WG3 Security — S3#32 **S3-040021**
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 ☒

Title:	⌘	Clarification on interface to access public CRL database			
Source:	⌘	Siemens, Nokia, T-mobile, Vodafone			
Work item code:	⌘	NDS/AF	***Date:***	⌘	28/01/2004
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:	⌘	Removal of Editors note, adding clarification how CRL database access relates to the Za-interface.
Summary of change:	⌘	
Consequences if not approved:	⌘	

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

*** Begin of change ***

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 Any certificate could be invalid because it was revoked (and replaced by a new one) or a SEG or operator has been deregistered.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 the same 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 the Za interface.

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.

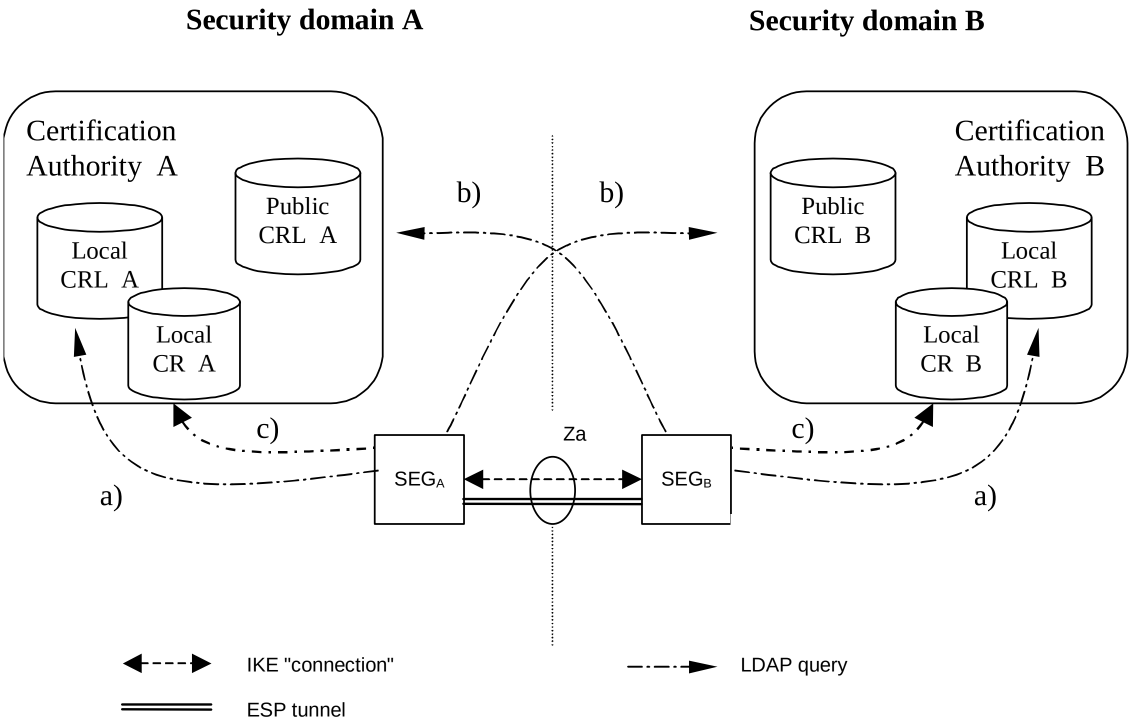

Figure 4: Repositories

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. Access to a public CRL database shall not be done via the ESP tunnel of the Za-interface. First this is not necessary as the retrieved CRL is integrity protected and contains no confidential information. Secondly access via an unprotected interface is anyhow necessary in case no currently valid security association is available to access the public CRL database and would require a dynamic behaviour of the policy database.

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.~~

*** end of change ***