3GPP TSG-SA 3 Meeting #28
Berlin, Germany, 6 - 9 May 2003

Tdoc ⌘S3-030234

CR-Form-v7

CHANGE REQUEST

⌘	**SpecNumber**	**CR**	**CRNum**	⌘ **rev**	**-**	⌘	Current version:	**x.y.z** ⌘

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:	⌘	NDS/AF Repositories			
Source:	⌘	Nokia, Siemens, SSH, T-Mobile, Verisign			
Work item code:	⌘	NDS/AF	***Date:***	⌘	30/04/2003
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:	⌘	Addition of Section 6.1
Summary of change:	⌘	- introduce CRL repositories - define access protocol
Consequences if not approved:	⌘	

Clauses affected:	⌘	3.1, 6.1, Annex B				
		Y	**N**			
Other specs affected:	⌘	□	□	Other core specifications	⌘	
		□	□	Test specifications		
		□	□	O&M Specifications		
Other comments:	⌘					

*** First modified section ***

3.1 Definitions

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

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

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

Local CRL: Repository that contains cross-certificate revocations

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

*** Next modified 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 Any certificate could be invalid because it was revoked (and replaced by a new one) or a SEG or operator has been deregistered.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.

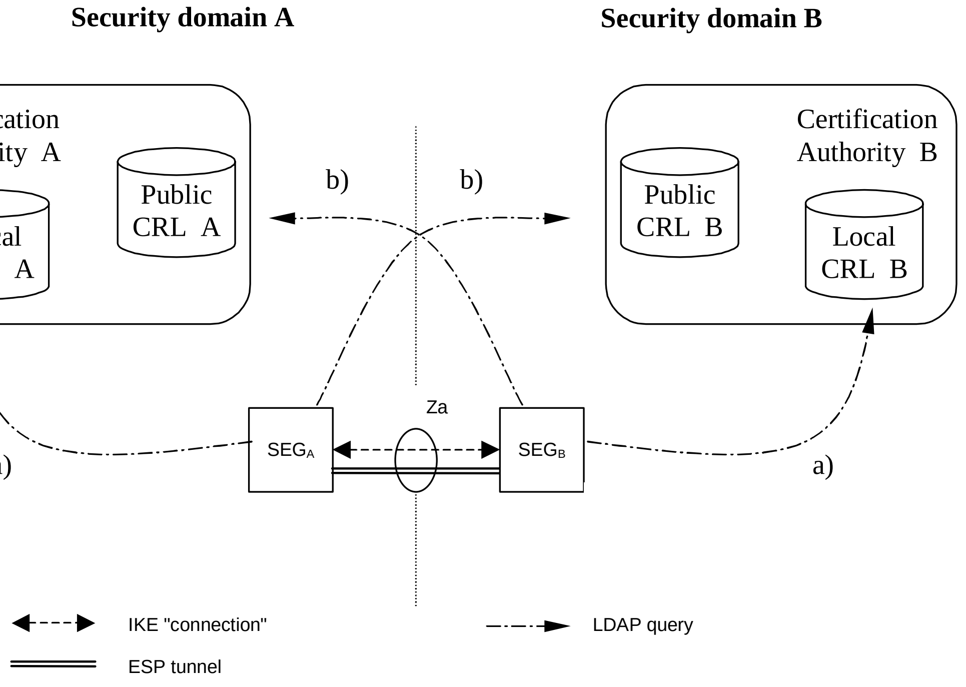

Figure 5: CRL Repositories

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 repositories.

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

*** Next modified section ***

Annex B (informative): Decision for the CRL repository access protocol

In order to document the decision for the protocol to access CRL repositories, this section summarises technical advantages and disadvantages of the two candidates.

LDAP

+ implemented by all PKI products (unless purely manual)

+ scalability

+ flexibility (integration possibility to other systems, automatic public key retrieval possibility)

- complexity

HTTP

+ simple

- not supported by all PKI products (although widely supported)

LDAP was chosen as the more future-proof protocol. Although more complex than HTTP, LDAP is well established amongst PKI vendors and operators.

*** End of modified section ***