3GPP TSG SA WG3 Security — S3#29 **S3-030385**
15 - 18 July 2003, San Francisco, USA

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:	⌘	Addition of a Clause on CRL Management within the SEG		
Source:	⌘	Siemens, Nokia, SSH, T-Mobile		
Work item code:	⌘	NDS/AF	***Date:*** ⌘	07/07/2003
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:	⌘	Addition of a separate clause that collects CRL management issues according to the working assumption that CRLs shall be retrieved out-of-band via LDAP. The alternative way of handling CRLs is exchanging them during IKE Phase 1 (see also according to Section 3.3.9 of draft-ietf-ipsec-pki-profile-02.txt. recommendation). However a product survey revealed that there are still few products supporting this. This statement was confirmed by one of the authors draft-ietf-ipsec-pki-profile-02.txt.
Summary of change:	⌘	
Consequences if not approved:	⌘	

Clauses affected:	⌘	New Clause 6.3				
		Y	**N**			
Other specs affected:	⌘		**N**	Other core specifications	⌘	
			N	Test specifications		
			N	O&M Specifications		
Other comments:	⌘					

6 Security features

[Editor’s note: Subsections may have to be moved to suitable places.]

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 Any certificate could be invalid because it was revoked (and replaced by a new one) or a SEG or operator has been deregistered.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

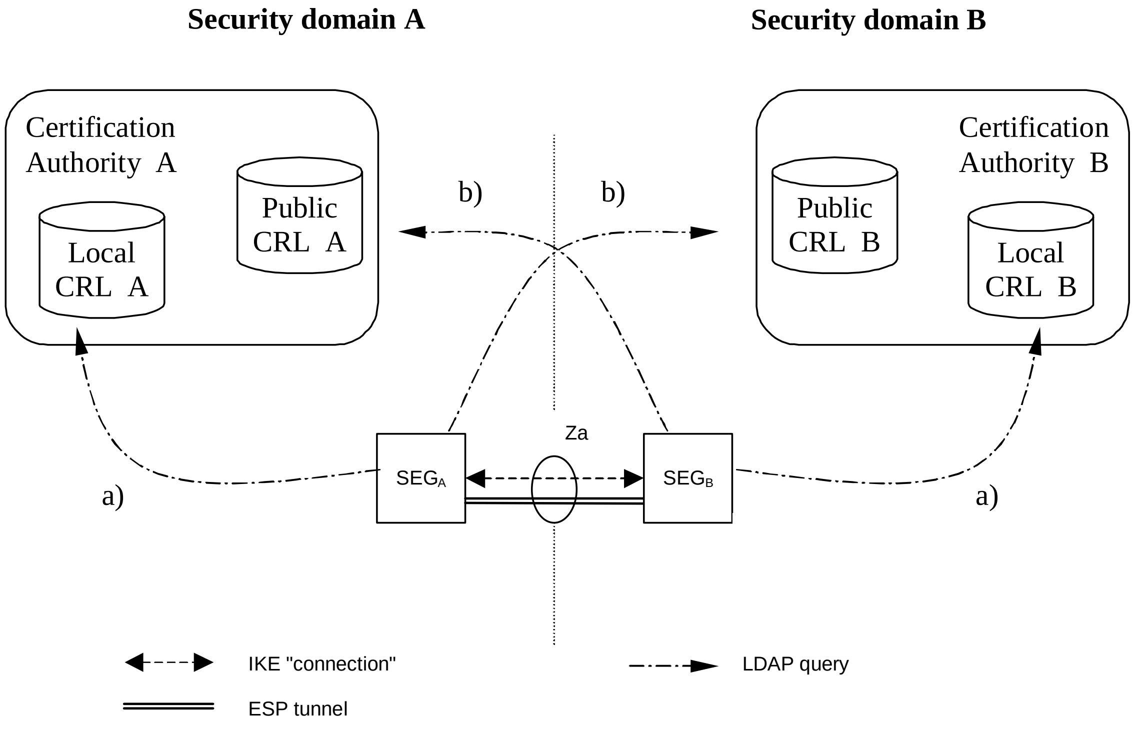

Figure 4: CRL Repositories

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 repositories.

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

6.2 Life cycle management

Certificate management protocol v2 (CMPv2, [4]) shall be the supported protocol to provide certificate lifecycle management capabilities. All SEGs and Roaming CAs shall support initial enrolment by SEG from CA via CMPv2, i.e. receiving a certificate from the Roaming CA, and updating the key of the certificate via CMPv2 before the certificate expires.

[Editor's note: CMPv2 is still at draft status, but is already widely supported (see 'CMP Interop Project': http://www.ietf.org/proceedings/00dec/slides/PKIX-4/), and expected to move to Draft Standard status in the near future. Thus it is expected that CMPv2 receives a RFC status before the NDS/AF specification is completed. Additionally, CMPv2 is preferred to CMPv1(RFC2510), because of the interoperability issues with CMPv1.]

6.3 CRL management

NDS/AF compliant SEGs shall not sent an ISAKMP CERTREQ where the Certificate Type is "Certificate Revocation List (CRL)". Receiving SEGs may ignore this request as section 5.3.1.3 specifies that CRLs shall be retrieved via CRL distribution point.

The CRL issuer (which is in most cases the CA) shall only issue full CRLs. The use of delta CRLs is not forbidden but is not encouraged because of possible interoperability problems. The full CRL shall only contain revoked certificates applicable for use within NDS/AF. The CRL issuer shall issue a CRL also in cases there are no revoked certificates. A SEG is not obliged to query for a CRL via the CRL Distribution Point, if a cached one is still available and valid. If no valid cached CRL is available, the SEG shall fetch a new CRL. If no valid CRL can be fetched, the SEG shall treat this as an error and cancel tunnel establishment.

[Editor's note: It is for ffs whether the ISAKMP SA lifetime shall be restricted to at most the remaining time+ delta defined within the CRLs NextUpdate field. This might result in following guideline
min(Cert. chain lifetime, CRLs lifetimes) >= IKE SA lifetime >= IPsec SA lifetime]