CR-Form-v7

PSEUDO CHANGE REQUEST

⌘ 33.310 CR CRNum ⌘rev - ⌘ Current version: 0.5.0 ⌘

*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:	⌘	Removal of support for delta CRLs
Source:	⌘	Nokia, Siemens, SSH, T-Mobile, Vodafone
Work item code:	⌘	NDS/AF
Date:	⌘	28/09/2003
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: ⌘ * The use of Delta CRLs may cause interoperability problems

See Delta CRL statements from http://www.ietf.org/internet-drafts/draft-ietf-ipsec-pki-profile-03.txt
in section 4.1.3 and section 4.2.3.4 and Appendix B.

* CRLs will not grow too large in NDS/AF so delta CRLs should be prohibited for the sake of interoperability

Summary of change: ⌘

Consequences if not approved: ⌘

Clauses affected: ⌘ 5.2

Other specs affected: ⌘

Y	N	
	N	Other core specifications
	N	Test specifications
	N	O&M Specifications

⌘

Other comments: ⌘

5.2 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 6.1.3 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 allowed~~forbidden but is not encouraged~~ because of possible interoperability problems and because in NDS/AF environment the full CRL is not expected to grow too large. 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]