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

S3-030386

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:	⌘	Handling critical and non critical certificate extensions		
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 explanation on how the specification text on mandatory and optional implementation (within the profiling clause 6.2) of critical and non-critical extensions has to be interpreted i.e. how to handle a mandatory critical extension, a optional critical extension, …
Summary of change:	⌘	
Consequences if not approved:	⌘	Implementers have to interpret this from RFC3280. <draft-ietf-ipsec-pki-profile-02.txt> contains similar explanations see 4.1.3. X.509 Certificate Extensions

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

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.

Annex C (normative): Critical and non critical Certificate Extensions.

According to RFC3280 section 4.2 a certificate extension can be designated as either critical or non-critical.

> *"A certificate using system MUST reject the certificate if it encounters a critical extension it does not recognize; however, a non-critical extension MAY be ignored if it is not recognized."*

Optional and mandatory support statements (e.g. Clause 5.3 profiling) are being made with respect to implementation requirements. A receiving SEG shall be able to process an extension marked as critical that is mandatory to support in NDS/AF. When optional to support, a received extension marked as critical shall lead to an error according to RFC3280.

Annex <D~~C~~> (normative): <Normative annex title>