CR-Form-v7

PSEUDO CHANGE REQUEST

⌘ **33.310** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: 0.6.0 ⌘

*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 unnecessary restriction on serial number
Source:	⌘	Siemens, Nokia, SSH, T-mobile
Work item code:	⌘	NDS/AF
Date:	⌘	10/11/2003
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 requirement that NDS/AF compliant devices shall only generate serial numbers of 20 octets long is too heavy. The NDS/AF specification profile RFC3280. Clause 4.1.2.2 of RFC3280 is thought to be enough to ensure interoperability between NDS/AF compliant devices.

- RFC3280 states in clause 4.1.2.2 Serial number

"The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA (i.e., the issuer name and serial number identify a unique certificate). CAs MUST force the serialNumber to be a non-negative integer.

Given the uniqueness requirements above, serial numbers can be expected to contain long integers. Certificate users MUST be able to handle serialNumber values up to 20 octets. Conformant CAs MUST NOT use serialNumber values longer than 20 octets.

Note: Non-conforming CAs may issue certificates with serial numbers that are negative, or zero. Certificate users SHOULD be prepared to gracefully handle such certificates"

- History of NDS/AF specification: The requirement in section 6.1.1 had been incorporated due to a lesson learned by the JNSA paper. This paper however covered interoperability issues in 2001 in testing RFC2459 'compliant' devices. RFC3280 was approved in April 2002 and obsoletes RFC2459.

- The latest version of the PKI-Profile draft does not mention any interoperability issues with the serial number: http://www.ietf.org/proceedings/03jul/I-D/draft-ietf-ipsec-pki-profile-03.txt

Summary of change:	⌘	
Consequences if not approved:	⌘	

Clauses affected:	⌘	6.1.1				
		Y	**N**			
Other specs affected:	⌘		**N**	Other core specifications	⌘	
			N	Test specifications		
			N	O&M Specifications		
Other comments:	⌘					

---------- CHANGED SECTION ----------

6.1.1 Common rules to all certificates

- Version 3 certificate according to RFC3280.

  Motivation: This is the current state of the art [3].

- Hash algorithm for use before signing certificate: Sha-1 mandatory to support, MD-5 shall not be used.

  Motivation: SHA-1, is state of the art, MD-5 shall not be used anymore as it is considered weaker

- Subject and issuer name format. Note that C is optional element. : (C=<country>), O=<Organization Name>, CN=<Some distinguishing name>. Organization and CN shall be in UTF8 format.

  Motivation: RFC3280 states in clause 4.1.2.4 Issuer that The UTF8String encoding in RFC 2279 is the preferred encoding, and all certificates issued after December 31, 2003 MUST use the UTF8String encoding of DirectoryString (except in some migration cases).

  or

- Subject and issuer name format. Note that ou is optional element. : cn=<hostname>, (ou=<servers>), dc=<domain>, dc=<domain>.

  Motivation: RFC 3280 states in clause 4.1.2.4 Issuer that implementations of this specification MUST be prepared to receive the domainComponent attribute, as defined in RFC 2247.

- CRLv2 support with LDAPv3 [5] retrieval shall be supported as the primary method of certificate revocation verification.

- Certificate extensions mentioned within RFC3280 but not in NDS/AF are optional for implementation.

~~- SerialNumber shall have a length of exactly 20 octets~~

~~Motivation: *This addresses lesson from http://www.jnsa.org/english/e_result.html*~~