CR-Form-v7

PSEUDO CHANGE REQUEST

⌘ **33.310 CR** ⌘ **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:	⌘	Adding domain component support to NDS/AF certificate profiles
Source:	⌘	Nokia, Siemens, SSH, T-Mobile
Work item code:	⌘	NDS/AF
Date:	⌘	30/09/2003
Category:	⌘	**B**
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:	⌘	Domain component support missing from NDS/AF certificate profiles.
Summary of change:	⌘	Domain component support added.
Consequences if not approved:	⌘	Misalignment between NDS/AF certificate profiles and RFC 3280 *PKI Certificate and CRL Profile* requirement to support domain components.
Clauses affected:	⌘	6.1.1

Other specs affected: ⌘	Y	N		⌘
		N	Other core specifications	
		N	Test specifications	
		N	O&M Specifications	

Other comments: ⌘

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

---------- 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*