3GPP TSG-SA 3 Meeting #28
Berlin, Germany, 6 - 9 May 2003

Tdoc ⌘S3-030240

CR-Form-v7

CHANGE REQUEST

⌘ **SpecNumber** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: **x.y.z** ⌘

*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:	⌘	NDS/AF Lifecycle Management
Source:	⌘	Nokia, Siemens, SSH, T-Mobile, Verisign
Work item code:	⌘	NDS/AF
Date:	⌘	30/04/2003
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 Section 6.2
Summary of change:	⌘	- introduce CMPv2 for use in lifecycle management, as in Feasibility Study - references
Consequences if not approved:	⌘	

Clauses affected:	⌘	6.2, 2			
Other specs affected:	⌘	**Y**	**N**		⌘
		☐	☐	Other core specifications	
		☐	☐	Test specifications	
		☐	☐	O&M Specifications	
Other comments:	⌘				

*** Start of modified section ***

2 References

[4] IETF Draft draft-ietf-pkix-rfc2510bis-08.txt: “Internet X.509 Public Key Infrastructure Certificate Management Protocol”
[5] CMP Interop Project: http://www.ietf.org/proceedings/00dec/slides/PKIX-4/

*** End of modified section ***

*** Start of modified section ***

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 [5]), and expected to move to Draft Standard status in the near future. CMPv2 is preferred to CMPv1(RFC2510), because of the interoperability issues with CMPv1]

*** End of modified section ***