3GPP TSG SA WG3 Security — S3#32 **S3-040092**
09 - 13 February 2004, Edinburgh, Scotland, UK

CR-Form-v7

PSEUDO CHANGE REQUEST

⌘ **33.310** **CR** **-** ⌘ **rev** **-** ⌘ Current version: 1.0.0 ⌘

*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 **X**

Title:	⌘	Certificate enrolment
Source:	⌘	Nokia, Siemens, T-Mobile, Vodafone
Work item code:	⌘	NDS/AF
Date:	⌘	30/01/2004
Category:	⌘	**F**
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:	⌘	Also manual certificate enrolment should be allowed.
Summary of change:	⌘	Manual certificate enrolment added.
Consequences if not approved:	⌘	Automated certificate enrolment by CMPv2 would be mandatory to use although there might be only few SEG elements.

Clauses affected:	⌘	5.2.11 SEG certificate creation 5.2.13 SEG certificate renewal 7.2 Life cycle management

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

Other comments:	⌘	-

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

5.2.11 SEG certificate creation

Using device-specific management methods, the certificate creation shall be initiated. As specified in section 7.2, either t~~T~~he CMPv2 protocol ~~shall be used~~ between the roaming CA and the SEG for automatic certificate enrolment or manual SEG certificate installation using PKCS#10 formats can be used. This is an operator decision depending for example on the number of SEG elements.

---------- NEXT CHANGED SECTION ----------

5.2.13 SEG certificate renewal

A new SEG certificate needs to be in place before the old SEG certificate expires. The procedure is similar to the SEG certificate creation and can~~shall~~ be either fully automated by using CMPv2 as specified in section 7.2 or done manually using PKCS#10 formats. This is an operator decision depending for example on the number of SEG elements.

---------- NEXT CHANGED SECTION ----------

7.2 Life cycle management

Certificate Management Protocol v2 (CMPv2) [4] shall be the supported protocol to provide certificate life cycle 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.

Enrolling a certificate to a SEG is an operation done more often than inter-operator cross-certifications, thus more automation ~~is~~could be required by the operator than is possible with a PKCS#10 approach. However, also manual SEG certificate installation using PKCS#10 formats shall be supported. It should be also noted that the lifetime of a cross-certificate is considerably longer than the lifetime of a SEG certificate. The basic CMPv2 functionalities such as enrolment and key update are widely implemented and interoperable.

Editor's note: CMPv2 is still at draft status, but is already widely supported (see 'CMP Interop Project': http://www.ietf.org/proceedings/00dec/slides/PKIX-4/), and expected to move to Draft Standard status in the near future. Thus it is expected that CMPv2 receives a RFC status before the NDS/AF specification is completed. Additionally, CMPv2 is preferred to CMPv1(RFC2510), because of the interoperability issues with CMPv1.