3GPP TSG-SA3 Meeting #29
San Francisco, USA, 16-19 July 2003

Tdoc ⌘S3-030345

CR-Form-v7

CHANGE REQUEST

⌘	**SpecNumber**	**CR**	**CRNum**	⌘ **rev**	**-**	⌘	Current version:	**0.2.0**	⌘

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:	⌘	Clarification of the authentication mechanism of the TS		
Source:	⌘	Nokia		
Work item code:	⌘	SEC1-SC	***Date:*** ⌘	19/06/2003
Category:	⌘	***A?***	***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 target TS specifies AKA authentication for bootstrapping the credentials to end entity; the mechanim based on long lasting certificate is out of scope and thus should be clarified.
Summary of change:	⌘	The authentication mechanim based on long lasting certificate is out of scope of the target TS.
Consequences if not approved:	⌘	

Clauses affected:	⌘	Annex A.5				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

A.5 Functionality in presence of ~~preloaded, long-lasting~~pre-certified key pair

An alternative to securing certificate enrolment based on AKA and bootstrapping function is to secure certificate enrolment based on signatures made with pre-certified key in the UE. This alternative has been specified by Open Mobile Alliance (see section 7.3.4 of [WPKI]) and is thus out of scope of this specification. The functionality in presence of pre-certified key pair in the UE is explained below only briefly.

In this alternative solution, the UE equipped with a UICC, is previously issued with a pre-loaded, long lasting, public/private key pair from the home network. This phase would occur out of band, and would result in the UE possessing a long lasting key pair stored in the UICC for the purposes of certificate request authentication. Open Mobile Alliance (OMA) group offers standardized solutions by means of WPKI specification [WPKI] and WIM specification [WIM] for the storage and the use of long-lasting key pair. USIM and WIM are examples of applications on the UICC that can deal with the long-lasting keys.

The UE can issue a request for a certificate to the CA, signing the request with the long lasting private key. The certificate request itself could contain a newly generated public key that is to be certified by the CA. This assumes that the new key pair is generated in the UICC. Or it is also possible for the CA to generate the new key pair and send it (protected) to the UICC. Access control security for the pre-loaded long-lasting private key should be at least as good as for access control for USIM.

Two options can be envisaged. Though the public/private key pair is long lasting, the validity of the subscriber certificates issued to the UE could be short-lived. In this case the long lasting public/private key pair is used for PKI applications (e.g. in mobile-commerce) in combination with the short-lived certificates. Alternatively, the long lasting public/private key pair could come with a long-term certificate. The long-term private key would then have a restricted purpose, e.g. only to be used to authenticate subscriber certificate requests. The latter would be used to obtain another, short-lived certificate on a short-lived public/private key pair. It would then be the short-lived keys that could be used for e.g. m-commerce and other 3G PKI applications.