3GPP TSG–SA3 Meeting #28
Berlin, Germany, 06-09 May 2003

Tdoc ⌘S3-030220

CR-Form-v7

CHANGE REQUEST

⌘ **ab.cde** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: **0.1.0** ⌘

*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⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Further information related to the storage of the public/private key pairs present in the User Equipment.
Source:	⌘	Gemplus
Work item code:	⌘	Support for Subscriber Certificates
Date:	⌘	29/04/2003
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:	⌘	The private keys must be kept secret; it requires that the private keys and the related cryptographic computations shall be managed by the smart cards. So the public/private key pairs present in the User Equipment shall be stored in the UICC. This change is inline with Alcatel contribution S3-030037, which is the based text. The term USIM is replaced by UICC to allow the storage of the key pair in any UICC application.
Summary of change:	⌘	Provides further information related to the storage of the public/private key pairs present in the UE.
Consequences if not approved:	⌘	The privacy of the subscriber private key is not guaranteed. So, there is no assurance that the issued subscriber certificate will be valid and that the digital signatures will be non-repudiable.

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 key pair

Editor's notes: Based on contribution S3-030037, it was agreed to add this part into the present document for ffs.

In this alternative solution, the UE is equipped with a UICC 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. ~~One possible solution is WPKI [WPKI] and one solution for storing long-lasting key pair is WIM [WIM].~~

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.

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~~USIM~~. Or it is also possible for the CA to generate the new key pair and send it (protected) to the UICC~~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.