3GPP TSG-SA WG3 Meeting S3#34
Acapulco, Mexico, July 6-9, 2004

Tdoc ⌘S3-040507

CR-Form-v7

CHANGE REQUEST

⌘ **33.221** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

*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 ☒

Title:	⌘	Removal of unnecessary editor's notes
Source:	⌘	Nokia
Work item code:	⌘	GBA-SSC
Date:	⌘	29/06/2004
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:	⌘	Editor's notes that are not needed or are unnecessary are removed or changed.
Summary of change:	⌘	Reason for removal: 4.4.4 - 1st editor's note: text is added to the proceeding paragraph reflecting the content of the editor's note (editor's note deleted) 4.4.4 - 2nd editor's note: there are no phases any more because NAF can be in visited network in release 6 (cf. TS 33.220) (editor's note modified) 4.4.5 - The charging mechanism does not have to addressed in this specification (editor's note deleted) 4.4.7 - The more flexible solutions are already specified below the editor's note (editor's note deleted) 4.7 - The material has been added thus this editor's note is obsolete (editor's note deleted)
Consequences if not approved:	⌘	Unnecessary editor's note are deleted.

Clauses affected:	⌘	4.4.4, 4.4.5, 4.4.7, 4.7

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

Other comments:	⌘	

===== BEGIN CHANGE =====

4.4.4 Home operator control

Home operator shall be able to control the issuing of subscriber certificates. The control includes to whom the certificates are allowed to issue and the types of issued certificates.

Operator control is supported by information in the subscriber profile. For each type of subscriber certificate, i.e. for different key ~~U~~usage in WAP Certificate and CRL Profile [7], subscriber profile shall contain a flag that allows or disallows the issuing of that type of certificate to subscriber. According to WAP Certificate and CRL Profile [7], there are two types of certificates for users (i.e., subscribers): user certificates for authentication and user certificates for digital signatures (i.e., non-repudiation).

~~Editor's note: Currently two keyUsage values are envisioned: authentication and signing.~~

Delivery of operator CA certificates is always allowed.

Editor's note: ~~For the first phase of standardisation, only the case is considered where bootstrapping server functionality and network application function are located in the same network as the HSS. Thus is the first phase the home network control does not require any communication between home and visited networks. In later phases, w~~When ~~also~~ visited network may issue certificates, standardized way of transferring the control information from home network to visited network is needed.

4.4.5 Charging principles

The operator shall be capable to charge issuing of subscriber certificates or delivery of operator CA certificates.

~~Editor's note: The charging mechanism and whether it needs to be standardized in 3GPP is FFS.~~

===== BEGIN NEXT CHANGE =====

4.4.7 Service Discovery

To enable the certificate enrollment procedure, the addresses of bootstrapping server and PKI portal should be configured to the UE. The BSF discovery method is specified in TS 33.220 [11].

~~Editor's note: For the first phase of standardisation, when bootstrapping server functionality and network application function are always located in home network, therefore pre-configuration of addresses may be sufficient. In later phases, however, when UE needs to address of PKI Portal in the visited network, more flexible is needed in the solution.~~

A procedure needs to be described on how to discover the location of PKI portal. It shall be possible to enable the UE to be configured either manually or automatically via one of the following approaches:

- The address information shall be published via reliable channel. Subscribers shall store all the parameters as part of the establishment of IP connectivity. The address information needs to be input only once.
- The address information shall be pushed automatically to the UE over the air when the subscription to bootstrapping service is accepted. All the parameters shall be saved into the UE and used in the same manner as above. The procedure is specified in [19].

===== BEGIN NEXT CHANGE =====

4.7 Functionality in presence of pre-certified key pair or pre-shared keys

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

4.7.1 Presence of 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 [9]) 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 [9] and WIM specification [8] 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, including a proof of origin (e.g. private key is stored in WIM) by using an administrative 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. Access control security for the pre-loaded long-lasting private key should be at least as good as for access control for USIM.

The certificate for the administrative long lasting private key, that provides the proof of generated key origin, is always long lasting certificate. On the other hand the generated user keys in the WIM may have short or long-lived certificate depending on CA policies (see [8], [9], [14]).

4.7.2 Presence of symmetric pre-shared key

Same as above but the administrate key that provides the proof of generated key origin is a shared symmetric key, in which case it does not have a certificate (see [8], [9], [14]).

NOTE: The pre-shared symmetric key discussed in this chapter is not the same as the shared key associated with GBA.

===== END CHANGE =====