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

Tdoc ⌘S3-030222

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:	⌘	Requirements on UE's public/private key pair associated to requested subscriber certificate.
Source:	⌘	Gemplus
Work item code:	⌘	Support for Subscriber Certificates
Date:	⌘	29/04/2003
Category:	⌘	**B**
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 issuance of a valid certificate that will allow the subscriber to perform digital signature mandates some security requirements on the public/private key pair associated to the requested certificate, since the private key pair has to be kept secret. It requires that the subscriber private key and the related cryptographic computations shall be managed by the smart cards. Those principles were already discussed in 3GPP S3-020625 contribution (Gemplus, November 2002) and agreed at Oxford SA3#26 meeting. The UICC on board key generation guaranties that nobody can access the private key.
Summary of change:	⌘	Add security requirements on the UE's public/private key pair associated to the requested subscriber certificate.
Consequences if not approved:	⌘	The privacy of the subscriber private key is not guaranted. So, there is no assurance that the issued subscriber certificate will be valid and that the digital signatures will be non-repudiable.

Clauses affected:	⌘	5.1.2

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

Other comments:	⌘	

5 Application specific functions using bootstrapping

5.1 Support for subscriber certificates

5.1.1 Introduction

Digital signatures can be used, for instance, to secure mobile commerce, service authorization and accounting. But digital signature by itself is not enough; there is need of a global support for authorization and charging. Thus 3GPP shall use global and secure authorization and charging infrastructure of mobile networks to support local architecture for digital signatures.

Subscriber certificates provide a migration path towards global Public Key Infrastructure (PKI). Local architecture for digital signatures can be deployed incrementally; an operator can choose to deploy independently of the others. On the other hand, the existence of subscribers and service providers that use digital signatures makes it easier to build global PKI.

3GPP systems shall issue subscriber certificates in order to authorize and account for service usage both in home and in visited network. This requires specification of:

1. Procedures to issue temporary or long-term certificates to subscribers.
2. Standard format of certificates and digital signatures, e.g. re-using wireless PKI.

The mechanism shall allow a cost efficient implementation of the security support of the UE. It will also enable a user's anonymity towards the service provider, whilst the user who invoking the service, can be identified by the network.

Subscriber certificates support services whose provision mobile operator assists, as well as services that mobile operator provides. There is no need to standardize those services. Also, the communication between service provider and the operator (in the role of certificate issuer) need not be standardized.

5.1.2 Requirements and principles for issuing subscriber certificates

The following prerequisites for issuing of subscriber certificates exits:

- The shared key material is available for the UE application, which does the certificate request and operator CA certificate retrieval.

5.1.2.1 Requirements on UE's public/private key pair associated to the requested subscriber certificate

- The public/private key pair shall be stored in the UICC
- The private key shall never leave the UICC
- In case of public/private key pair generation in the UE: the UICC shall perform the on-board key generation

~~5.1.2.1 Requirements on protocol B~~

5.1.2.2 Requirements on protocol B

The requirements for protocol B are:

- UE is able to request for subscriber's certification from the PKI portal that plays the role of the NAF over a network connection.
- NAF is able to authenticate UE's certificate request.
- UE is able to acquire an operator's CA certificate over the network connection.

- UE is able to authenticate the NAF response (i.e., operator CA certificate delivery).
- The procedure is independent of the access network used.
- The NAF should have access to the subscriber profile to check the certification policies. This means that the protocol D (cf. clause 5.1.2.2) should have support for retrieving a subset of the subscriber profile.
- The response and delivery of certificate to UE must be within a few seconds after the initial certification request.

~~5.1.2.2Requirements on protocol D~~

5.1.2.3 Requirements on protocol D

5.1.3 Certificate issuing