3GPP TSG-SA3 Meeting #28
Berlin, Germany, 6-9 May 2003

Tdoc ⌘S3-030232

CR-Form-v7

CHANGE REQUEST

⌘ **SpecNumber CR CRNum** ⌘**rev** **-** ⌘ Current version: **x.y.z** ⌘

*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:	⌘	Development to the annex of the draft TS		
Source:	⌘	Nokia		
Work item code:	⌘	SEC1-SC	***Date:*** ⌘	25/04/2003
Category:	⌘	C	***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:	⌘	Current specification TS is just in initial form; stage 2 work should be added.
Summary of change:	⌘	This pseudo-CR provides further development to the draft TS in the subscriber's certificates delivery as well as CA certificate delivery. New references added.
Consequences if not approved:	⌘	Stage 2 work is missing.

Clauses affected:	⌘	2, Annex A.1, A.2, A.3				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

2 References

The following documents contain provisions that, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[<seq>] <doctype> <#>[([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".

[1] 3GPP TR 41.001: "GSM Release specifications".

[2] 3GPP TR 21.912 (V3.1.0): "Example 2, using fixed text".

[3] 3GPP TS 31.102: "Characteristics of the USIM Application".

[4] 3GPP TS 33.102: "Security Architecture".

[PKCS10] “PKCS#10 v1.7: Certification Request Syntax Standard”, RSA Laboratories, May 2000.

[RFC2510] Adams C., Farrell S., “Internet X.509 Public Key Infrastructure Certificate Management Protocols”, RFC 2510, March 1999.

[RFC2511] Myers M., et al., ”Internet X.509 Certificate Request Message Format”, RFC 2511, March 1999.

[RFC2527]

[RFC2617] Franks J., et al, “HTTP Authentication: Basic and Digest Access Authentication”, RFC 2617, June 1999.

[RFC3280]

[WAPCert]

[WIM] WAP-260-WIM-20010712, 12.7.2001: http://www1.wapforum.org/tech/documents/WAP-260-WIM-20010712-a.pdf

[WPKI] WAP-217-WPKI, 24.4.2001: http://www1.wapforum.org/tech/documents/WAP-217-WPKI-20010424-a.pdf

[X.509]

********* NEXT CHANGE**********

Annex <A> (informative): Support for subscriber certificates based on bootstrapping

A.1 Introduction

This annex describes how operators issue the subscriber certificates and deliver operator CA certificates to subscribers.

A.2 Additional requirements and principles

A.2.1 Usage of Bootstrapping

Issuing procedures of the subscriber certificate and operator CA certificate shall be secured by using shared keys obtained from bootstrapping function.

A.2.2 Access independence

Subscriber certificate and operator CA certificate issuing procedures are access independent. Certificate issuing procedures require IP connectivity from UE.

A.2.3 Roaming and service network support

The roaming subscriber shall be able to request subscriber certificates and operator CA certificates from home network.

Editor's note: Certificate requests to any than home network may be supported in later phase of the present specification.

A.2.4 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.

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, when also visited network may issue certificates, standardized way of transferring the control information from home network to visited network is needed.

A.2.5 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.

A.2.6 Subscriber Certificate Profile

Subscriber certificate profile shall be based on WAP Certificate and CRL Profile [WAPCert], which in turn is based on profiles defined in [RFC3280] and [X.509]. A certificate profile defines the format and semantics of certificates in a specific context.

Editor's note: Applicability of other certificate profile specifications, e.g. RFC 3281, ETSI QC profile is FFS.

During certificate issuing, UE may include the following certificate extensions to the certification request:

- Intended certificate usage (i.e., using keyUsage and/or extKeyUsage extensions [WAPCert]).
- Subscriber identities (i.e., subject name field, and possible additional identities defined in the subjectAltName extension [WAPCert]). Operator CA shall authorize each suggested subscriber identity.
- Proof of key origin (i.e., keyGenAssertion). Operator CA shall verify the proof of key origin if it is presented.

Note: It is not mandatory for Operator CA to insert these suggested extensions by UE to the certificate. Rather, Operator CA shall issue certificates based on its certification policies. It may write a certification practice statement (CPS) [RFC2527], where it describes the general requirements and steps taken during the certificate issuing.

A.2.7 Service Discovery

The addresses of bootstrapping server and PKI portal may be pre-configured to the UE or UICC. The possible service discovery or over-the-air configuration mechanism are FFS.

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 is 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.3 Certificate issuing architecture

A.3.1 Reference model

Figure 5 below shows a simple network model of the entities involved in the certificate issuing, and the protocols used between the network entities.

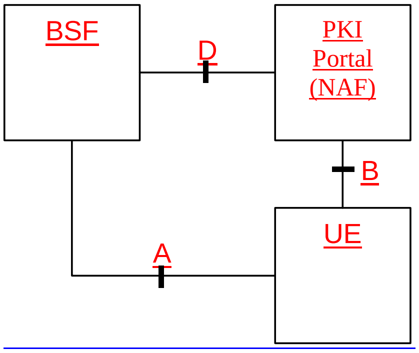

Figure 5: Simple network model for certifiate issuing.

A.3.2 Network elements

A.3.2.1 PKI Portal

A PKI Portal shall issue a certificate for UE and deliver an operator CA certificate. In both cases, requests and responses are protected by shared key material that has been previously established between UE and a BSF

In PKI terms, the PKI portal is a Registration Authority (RA) who authenticates the certification request based on cellular subscription (using protocol A). PKI Portal may also function as a Certification Authority (CA) who will issue certificates.

However, this task may also be done in an existing PKI infrastructure towards which the PKI Portal would function as a RA only, and the CA would be in the PKI infrastructure.

A.3.2.2 Bootstrapping Server Function

The bootstrapping server function (BSF) shall support the PKI portal by providing the authentication (c.f. section 4.2.2.1) and subscriber profile information (i.e., whether subscriber is able to enrol a certain types of subscriber certificate).

A.3.2.3 UE

The required new functionality from UE is the support of the protocol B (i.e. certification enrolment protocol) that is protected using the shared keys established during bootstrapping function.

In addition UE may have the capability to generate public and private key pairs, store the private key part to a non-volatile memory (e.g., in UICC), and protect the usage of the private key part (e.g., with a PIN).

A.3.3 Reference points

A.3.3.1 B

A.3.3.1.1 General description

In the certificate issuing, protocol B is used to for:

- The operator CA certifying subscriber's public keys in format of certificates, and

- The delivery of the Operator CA certificate to the UE.

During subscriber certificate issuing, UE may request a certification of a public key. The supported request formats shall include PKCS#10. It is used to encapsulate the public key and other attributes (i.e., subject name, intended key usage, etc.). The request is transported from the UE to the PKI Portal using protocol B. Upon receiving the certification request, PKI portal will certify the public key according to its own certification practice policies and subscriber profile which is fetched through BSF from HSS. If PKI Portal decides to certify the public key, it will digitally sign it, and generate the corresponding certificate, which is returned from PKI Portal to the UE, using protocol B.

During operator CA certificate delivery, the UE may request the PKI Portal to deliver operator CA's certificate. In the corresponding response, the PKI Portal will deliver the CA's certificate to the UE. Since the operator's CA certificate is typically a self-signed certificate and the validation of certificates signed by this CA is based on this particular CA certificate, it needs to be delivered over authenticated and secured channel.

Authentication, integrity protection, and possibly encryption of the protocol B messages are based on the BSF generated shared secret.