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

Tdoc ⌘S3-040505

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:	⌘	Editorial cleanup
Source:	⌘	Nokia
Work item code:	⌘	GBA-SSC
Date:	⌘	29/06/2004
Category:	⌘	**D**
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: ⌘ Cleanup is done to improve readability, and synchronize the notation style compared to other specifications (such as TS 33.220).

Summary of change: ⌘ The following changes are done:
- the name of the specification is added to reference number in the text to improve readability
- renamed "interfaces" to "reference points"
- the format of references unified (removed version numbering, and publication dates)

Consequences if not approved: ⌘ Clarifications on the text is not done.

Clauses affected: ⌘ 2, 4.2, 4.3.2, 4.3.3, 4.4.3, 4.4.6, 4.4.7, 4.4.8, 4.5.1, 4.5.1.1, 4.7.1, 4.7.2

Other specs affected: ⌘

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

Other comments: ⌘

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

2 References

The following documents contain provisions which, 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*.

[1] PKCS#10~~ v1.7~~: "Certification Request Syntax Standard"~~, RSA Laboratories, May 2000~~.

[2] IETF RFC 2510~~Adams C., Farrell S.~~: "Internet X.509 Public Key Infrastructure Certificate Management Protocols"~~, RFC 2510, March 1999~~.

[3] IETF RFC 2511~~Myers M., et al.~~: "Internet X.509 Certificate Request Message Format"~~, RFC 2511, March 1999~~.

[4] IETF RFC 2527~~Chokhani S., et al.~~: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"~~, RFC 2527, March 1999~~.

[5] IETF RFC 2617~~Franks J., et al.~~: "HTTP Authentication: Basic and Digest Access Authentication"~~, RFC 2617, June 1999~~.

[6] IETF RFC 3280~~Housley R., et al.~~: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"~~, RFC 3280, April 2002~~.

[7] OMA: "WAP Certificate and CRL Profiles".~~WAP-211-WAPCert, 22.5.2001: http://www1.wapforum.org/tech/terms.asp?doc=WAP-211-WAPCert-20010522-a.pdf~~

[8] OMA: "Wireless Identity Module; Part: Security".~~WAP-260-WIM-20010712, 12.7.2001: http://www1.wapforum.org/tech/documents/WAP-260-WIM-20010712-a.pdf~~

[9] OMA: "Wireless Application Profile; Public Key Infrastructure Definition".~~WAP-217-WPKI, 24.4.2001: http://www1.wapforum.org/tech/documents/WAP-217-WPKI-20010424-a.pdf~~

[10] ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8:1997: "Information Technology - Open Systems Interconnection - The Directory: Authentication Framework"~~, 1997~~.

[11] 3GPP TS 33.220: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[12] 3GPP TS 33.222: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Access to Network Application Function using HTTPS".

[13] 3GPP TR 33.919: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); System description".

[14] OMA: "Crypto Object for the ECMAScript Mobile Profile".~~Open Mobile Alliance ECMA Crypto Library http://www.openmobilealliance.org.~~

[15] IETF RFC 3546~~Blake-Wilson, S., et al,~~: "Transport Layer Security (TLS) Extensions"~~, RFC 3546, June 2003~~.

[16] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[17] IETF RFC 3039~~Santesson, S., Polk, W., Barzin, P., and M. Nystrom,~~: "Internet X.509 Public Key Infrastructure Qualified Certificates Profile"~~, RFC 3039, January 2001~~.

[18] ETSI TS 101 862: "Qualified certificate profile".

[19] OMA: "Provisioning Content Version 1.1"~~, Version 13-Aug-2003. Open Mobile Alliance~~.

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

4.2 Reference model

Figure 1 shows a simple network model of the entities involved in the certificate issuing, and the ~~interfaces~~reference points used between the network entities.

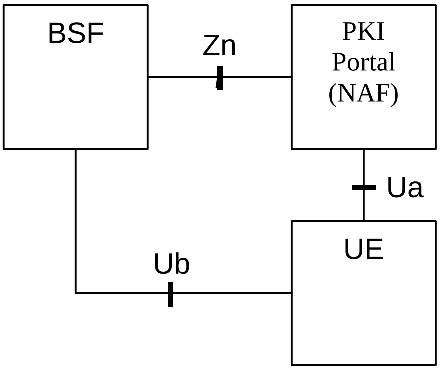

Figure 1: Simple network model for certificate issuing

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

4.3.2 Bootstrapping Server Function

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

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

4.3.3 User Equipment

The required new functionality from UE is the support of the reference point Ua ~~interface~~ (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).

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

4.4.6 Subscriber Certificate Profile

Subscriber certificate profile shall be based on WAP Certificate and CRL Profile [7], which in turn is based on profiles defined in IETF RFC 3280 [6] and ITU-T X.509 [10]. A certificate profile defines the format and semantics of certificates in a specific context. WAP Certificate and CRL profiles specification defines four certificate profiles: two user certificate profiles – one for authentication and the other for non-repudiation purposes, server certificate profile for authentication, and authorization certificate profile (i.e., CA certificate). Since subscriber certificates are issued to users, and since services need CA certificate to validate subscriber certificates, the relevant WAP certificate profiles to be used with subscriber certificate profiles are the user certificate profiles, and CA certificate profile.

~~IETF's and ETSI's~~ Qualified certificate profiles by IETF [17]~~,~~ and ETSI [18] may also be used as the subscriber certificate profile if the certification practices followed by the certificate issuing operator fulfil all of the requirements stated in [16,17,18].

The following certificate extensions may be filled with the information given by the UE in the certification request:

- Intended certificate usage (i.e. using keyUsage and/or extKeyUsage extensions [7]).
- Subscriber identities (i.e., subject name field, and possible additional identities defined in the subjectAltName extension [7]). 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) [4], where it describes the general requirements and steps taken during the certificate issuing.

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 OMA's "Provisioning Content Version 1.1" [19].

4.4.8 Requirements on reference point Ua ~~interface~~

The requirements for reference point Ua ~~interface~~ are:

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

- UE shall be able to authenticate the NAF response (i.e., operator CA certificate delivery);
- the procedure shall be independent of the access network used;
- the NAF shall have access to the subscriber profile to check the certification policies. This means that the reference point Zn ~~interface~~ TS 33.220 [11] shall support for retrieving a subset of the subscriber profile;
- the response and delivery of certificate to UE shall be within a few seconds after the initial certification request;
- certification request format shall be PKCS#10;
- certification response format shall be one of the following: a certificate, a pointer to the certificate, or a full certificate chain.

4.5 Certificate issuing architecture

4.5.1 Reference point Ua ~~interface~~

4.5.1.1 General description

In the certificate issuing, reference point Ua ~~interface~~ 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 format shall be 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 over reference point Ua ~~interface~~. Upon receiving the certification request, the 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, over reference point Ua ~~interface~~.

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 messages sent over reference point Ua ~~interface~~ are based on the BSF generated shared secret according to the GBA in TS 33.220 [11], where the PKI portal acts as a Network Application Function (NAF).

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

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 WPKI [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 OMA's WIM [8], WPKI [9], and ECMA script [14] specifications).

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 OMA's WIM [8], WPKI [9], and ECMA script [14] specifications).

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

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