3GPP TSG SA WG3 Security — S3#32 **S3-040072**
09 - 13 February 2004, Edinburgh, Scotland, UK

CR-Form-v7

CHANGE REQUEST

⌘ **TS 33.221 CR CRNum** ⌘ **rev** ⌘ Current version: 1.0.0 ⌘

*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:	⌘	Service discovery for bootstrapping procedure
Source:	⌘	Nokia
Work item code:	⌘	GBA and Support for subcriber certificates
Date:	⌘	23/1/2004
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:	⌘	The discovery of CA service location
Summary of change:	⌘	Reference to specifications where the procedures that already specified. Several methods are listed in the section 4.2.7.
Consequences if not approved:	⌘	Service will not possible to be deployed to end users.
Clauses affected:	⌘	2, 4.2.7

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

Other comments: ⌘

--- Change starts---

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

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

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

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

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

[7] WAP-211-WAPCert, 22.5.2001: http://www1.wapforum.org/tech/terms.asp?doc=WAP-211-WAPCert-20010522-a.pdf

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

[9] 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] Open Mobile Alliance ECMA Crypto Library http://www.openmobilealliance.org.

[15] OMA: “Provisioning Content Version 1.1”, Version 13-Aug-2003. Open Mobile Alliance.

4 Support for Subscriber Certificates

4.1 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.

Open Mobile Alliance offers an alternative solution for certificate enrolment (c.f. subclause 4.5)

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.

4.2 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;
- the issuing of requested certificate is allowed according to subscriber profile. NAF is responsible for performing this check before issuing the subscriber certificate;
- in the case that the private key is stored in the WIM being capable of providing a proof of key origin (assurance info that the key is securely stored in a tamper-resistant device), it shall be possible to send this information with the certificate request.

NOTE: Procedures for providing proof of key origin are not limited to the WIM application.

4.2.1 Usage of Bootstrapping

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

4.2.2 Access independence

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

4.2.3 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.

4.2.4 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.

Operator control is supported by information in the subscriber profile. For each type of subscriber certificate, i.e. for different keyUsage in WAP Certificate and CRL Profile, subscriber profile shall contain a flag that allows or disallows the issuing of that type of certificate to subscriber.

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

4.2.5 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.

4.2.6 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 [6] and [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.

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

The following certificate extensions shall 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.

4.2.7 Service Discovery

To enable the certificate enrollment procedure, ~~The~~ the addresses of bootstrapping server and PKI portal ~~may be pre-~~ should be configured to the UE ~~or UICC. The possible service discovery or over the air configuration mechanism are FFS.~~ The BSF discovery method is specified in [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 ~~is~~ 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 terminal 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 terminal and used in the same manner as above. The procedure is specified in [15].

--- Change completes---