3GPP TSG SA WG3 Security — S3#32 **S3-040156**
09 - 13 February 2004
Edinburgh, Scotland, UK

Title: **Liaison on Service Discovery of BSF and PKI portal**
Work Item: **Support for Subscriber's Certificate**
Source: **SA3**
To: **SA2**
Cc: -

Contact Person:
Name: Tao Haukka
Tel. Number: +358 40 5170079
E-mail Address: tao.haukka@nokia.com

Attachments: TS 33.220 (v1.0.0)+CR, TS 33.221(v1.0.0)+CR

1. Overview

SA3 has progressed their work under WI Support for Subscriber's Certificate and identified that service discovery and provisioning function must be specified to locate the service address of BSF (Bootstrapping Service Function) and PKI portal. Two contributions were proposed and also accepted in SA3#32 for this purpose, as shown in revision marks in the attached two specifications. SA3 understands that the judgement falls into expertise of SA2, thus would like to invite their review to the contributions.

2. Action

SA3 kindly invites review of SA2 on the attached draft TSs.

3. Further meetings of 3GPP SA3 working group

S3#33	11-14 May 2004	Beijing, China	Samsung
S3#34	06-09 July 2004 (TBC)	TBC	"NA Friends of 3GPP" (TBC)
S3#35	5-8 October 2004	TBC (Sophia?)	TBC (ETSI/EF3?)
S3#36	23-26 November 2004	Shenzhen, China	HuaWei Technologies
S3#37	February 2005	Australia (TBC)	Qualcomm (TBC)

3GPP TS 33.220 V1.0.0 (2003-12)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (Release 6)

Keywords
Security, GAA

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document describes the security features and a mechanism to bootstrap authentication and key agreement for application security from the 3GPP AKA mechanism. Candidate applications to use this bootstrapping mechanism include but are not restricted to subscriber certificate distribution [5], etc. Subscriber certificates support services whose provision mobile operator assists, as well as services that mobile operator provides.

The scope of this specification includes a generic AKA bootstrapping function, an architecture overview and the detailed procedure how to bootstrap the credential.

Editor's note: The specification objects are scheduled currently in phases. 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. In later phases, other configurations may be considered.

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] 3GPP TS 31.102: "3rd Generation Partnership Project; Technical Specification Group Terminals; Characteristics of the USIM application".

[2] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture".

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

[4] A. Niemi, et al,: "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)", RFC3310, September 2002.

[5] 3GPP TS 33.221: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Support for Subscriber Certificates".

[6] T. Dierks, et al,: "The TLS Protocol Version 1.0", RFC 2246, January 1999.

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

[8] 3GPP TS 23.228: “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 6) ”.

3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AK	Anonymity Key
AKA	Authentication and Key Agreement
BSF	Bootstrapping server functionality BSF is hosted in a network element under the control of an MNO.
BSP	BootStrapping Procedure
CA	Certificate Authority
CMP	Certificate Management Protocols
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
HSS	Home Subscriber System
IK	Integrity Key
MNO	Mobile network operator
NAF	Operator-controlled network application function functionality. NAF is hosted in a network element under the control of an MNO.
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
SCP	Subscriber Certificate Procedure
UE	User Equipment

4 Generic Bootstrapping Architecture

The 3GPP authentication infrastructure, including the 3GPP Authentication Centre (AuC), the USIM, and the 3GPP AKA protocol run between them, is a very valuable asset of 3GPP operators. It has been recognised that this infrastructure could be leveraged to enable application functions in the network and on the user side to communicate in situations where they would not be able to do so without the support of the 3GPP authentication infrastructure. Therefore, 3GPP can provide the "bootstrapping of application security" to authenticate the subscriber by defining a generic bootstrapping function based on AKA protocol.

4.1 Requirements and principles for bootstrapping

Editor's note: The description of AKA bootstrapping shall be added here.

- The bootstrapping function shall not depend on the particular network application function.
- The server implementing the bootstrapping function needs to be trusted by the home operator to handle authentication vectors.
- The server implementing the network application function needs only to be trusted by the home operator to handle derived key material.
- It shall be possible to support network application functions in the operator's home network.
- The architecture shall not preclude the support of network application function in the visited network, or possibly even in a third network.
- To the extent possible, existing protocols and infrastructure should be reused.
- In order to ensure wide applicability, all involved protocols are preferred to run over IP.
- It shall be prevented that a security breach in one application server using the Generic Bootstrapping Architecture can be used by an attacker to mount successful attacks to the other application servers using the Generic Bootstrapping Architecture.

4.1.1 Access Independence

Bootstrapping procedure is access independent. Bootstrapping procedure requires IP connectivity from UE.

4.1.2 Authentication methods

Authentication method that is used to authenticate the bootstrapping function must be dependent on cellular subscription. In other words, authentication to bootstrapping function shall not be possible without valid cellular subscription. Authentication shall be based on AKA protocol.

4.1.3 Roaming

The roaming subscriber shall be able to utilize the bootstrapping function in home network.

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. In later phases, other configurations may be considered.

4.1.4 Requirements on Ub interface

The requirements for Ub interface are:

- The BSF shall be able to identify the UE.
- The BSF and the UE shall be able to authenticate each other based on AKA.
- The BSF shall be able to send a transaction identifier to UE.

4.1.5 Requirements on Zh interface

The requirements for Zh interface are:

- The BSF shall be able to communicate securely with the subscriber's HSS.

Editor's note: this requirement is fulfilled automatically if BSF and HSS are in same operator's network.

- The BSF shall be able to send bootstrapping information request concerning a subscriber.
- The HSS shall be able to send authentication vectors to the BSF in batches.
- The HSS shall be able to send the subscriber's GAA profiles to the BSF.

Editor's note: the intention is not to send all the application-specific profile information, but only the information needed for security purposes.

Editor's note: it's ffs how to proceed in the case where profile is updated in HSS after profile is forwarded. The question is whether this profile change should be propagated to BSF.

- No state information concerning bootstrapping shall be required in the HSS.
- All procedures over Zh interface shall be initiated by the BSF.
- It is preferred to reuse existing specifications if possible.
- The number of different interfaces to HSS should be minimized.

4.1.6 Requirements on Zn interface

The requirements for Zn interface are:

- Mutual authentication, confidentiality and integrity shall be provided.
- The BSF shall verify that the NAF is authorised.
- The NAF shall be able to send a key material request to the BSF.
- The BSF shall be able to send the requested key material to the NAF.
- The NAF shall be able to get the subscriber profile from BSF.

Editor's note: The intention is not to send all the application-specific profile information, but only the information needed for security purposes.

Editor's note: In later phases there is an additional requirement that the NAF and the BSF may be in different operators' networks.

4.2 Bootstrapping architecture

4.2.1 Reference model

Figure 1 shows a simple network model of the entities involved in the bootstrapping approach, and the protocols used among them.

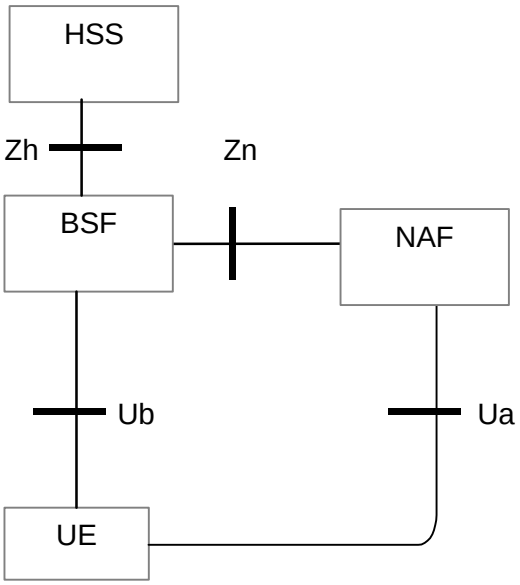

Figure 1: Simple network model for bootstrapping

Figure 2 illustrates a protocol stacks structure in network elements that are involved in bootstrapping of application security from 3G AKA and support for subscriber certificates.

Editor's note: The current protocol stack figure is placed here as a holder. The actual protocols will be defined later.

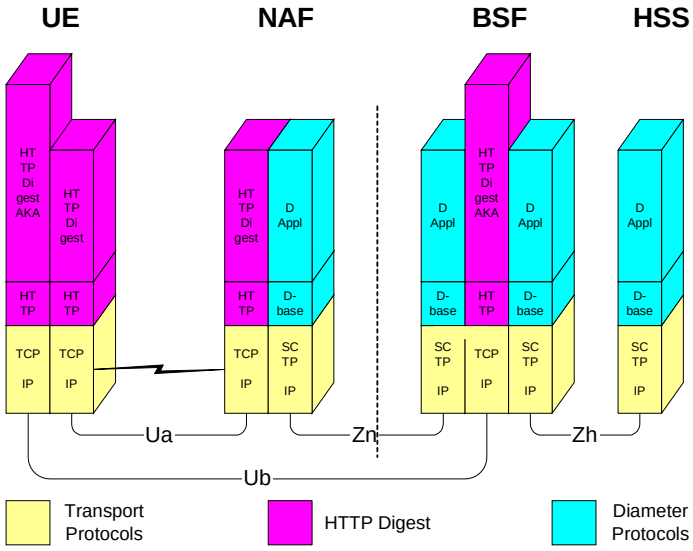

Figure 2: Protocol stack architecture

4.2.2 Network elements

4.2.2.1 Bootstrapping server function (BSF)

A generic bootstrapping server function (BSF) and the UE shall mutually authenticate using the AKA protocol, and agree on session keys that are afterwards applied between UE and an operator-controlled network application function (NAF). The key material must be generated specifically for each NAF independently, that is, for each key uniquely identified by a transaction identifier and that is shared between a UE and a NAF there is a new run of HTTP Digest AKA over the Ub interface. The BSF can restrict the applicability of the key material to a defined set of NAFs by using a suitable key derivation procedure.

Editor's note: Key generation for NAF is ffs. Potential solutions may include:
- Separate run of HTTP Digest AKA over Ub interface for each request of key material from a NAF
- Issues with key lifetime are ffs.

4.2.2.2 Network application function (NAF)

After the bootstrapping has been completed, the UE and an operator-controlled network application function (NAF) can run some application specific protocol where the authentication of messages will be based on those session keys generated during the mutual authentication between UE and BSF.

General assumptions for the functionality of an operator-controlled network application function (NAF):

- there is no previous security association between the UE and the NAF;
- NAF shall able to locate and communicate securely with subscriber's BSF;
- NAF shall be able to acquire a shared key material established between UE and the bootstrapping server function (BSF) during running application-specific protocol.

4.2.2.3 HSS

HSS shall store new parameters in subscriber profile related to the usage of bootstrapping function. Possibly also parameters related to the usage of some network application function are stored in HSS.

Editor's note: Needed new parameters are FFS.

4.2.2.4 UE

The required new functionalities from UE are:

- the support of HTTP Digest AKA protocol;
- the capability to derive new key material to be used with the protocol over Ua interface from CK and IK; and
- support of NAF specific application protocol (see [5]).

4.2.3 Reference points

4.2.3.1 Ub interface

The reference point Ub is between the UE and the BSF. The functionality is radio access independent and can be run in both CS and PS domains.

Editor's note: The solution for CS domain is ffs.

4.2.3.1.1 Functionality

Reference point Ub provides mutual authentication between the UE and the BSF entities. It allows the UE to bootstrap the session keys based on the 3G infrastructure. The session key as result of key agreement functionality, is used to support further applications e.g. certificate issuer.

4.2.3.1.2 Protocol

Ub interface is in format of HTTP Digest AKA, which is specified in [4]. It is based on the 3GPP AKA [2] protocol that requires information from USIM and/or ISIM. The interface to the USIM is as specified for 3G [1].

4.2.3.2 Ua interface

Ua interface is the application protocol which is secured using the keys material agreed between UE and BSF as a result of the run of HTTP Digest AKA over Ub interface. For instance, in the case of support for subscriber certificates [5], it is a protocol, which allows the user to request certificates from the NAF. In this case NAF would be the PKI portal.

4.2.3.3 Zh interface

Zh interface is used between the BSF and the HSS to allow the BSF to fetch the required authentication information and subscriber profile information from the HSS. The interface to the 3G Authentication Centre is HSS-internal, and it need not be standardised as part of this architecture.

4.2.3.4 Zn interface

Zn interface is used by the NAF to fetch the key material agreed during previous HTTP Digest AKA protocol run over Ub interface from the BSF. It may also be used to fetch subscriber profile information from BSF.

4.3 Procedures

This chapter specifies in detail the format of the bootstrapping procedure that is further utilized by various applications. It contains the AKA authentication procedure with BSF, and latter the key material generation procedure.

4.3.1 Initiation of bootstrapping

When a UE wants to interact with an NAF, but it does not know if bootstrapping procedure is required, it shall contact NAF for further instructions (see figure 3).

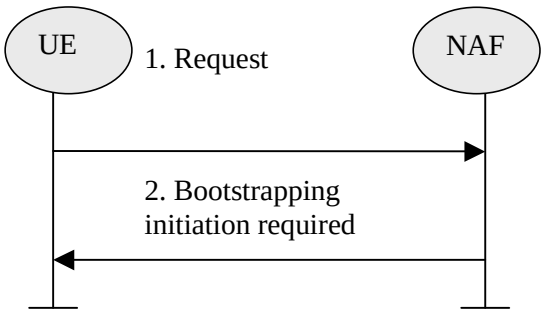

Figure 3: Initiation of bootstrapping

1. UE starts communication over Ua interface with the NAF without any bootstrapping related parameters.
2. If the NAF require bootstrapping but the request from UE does not include bootstrapping related parameters, NAF replies with a bootstrapping initiation message. The form of this indication may depend on the particular Ua interface and is ffs.

Editor's note: If the protocol over Ua interface is based on HTTP, then NAF can initiate the bootstrapping procedure by using HTTP status codes (e.g. 401 Unauthorized).

4.3.2 Bootstrapping procedures

When a UE wants to interact with an NAF, and it knows that bootstrapping procedure is needed, it shall first perform a bootstrapping authentication (see figure 4)

Editor's note: Zh interface related procedure will be added here in future development. It may re-use Cx interface that is specified in TS 29.228.

Otherwise, the UE shall perform a bootstrapping authentication only when it has received bootstrapping initiation required message or a key update indication from the NAF (cf. subclause 4.3.3).

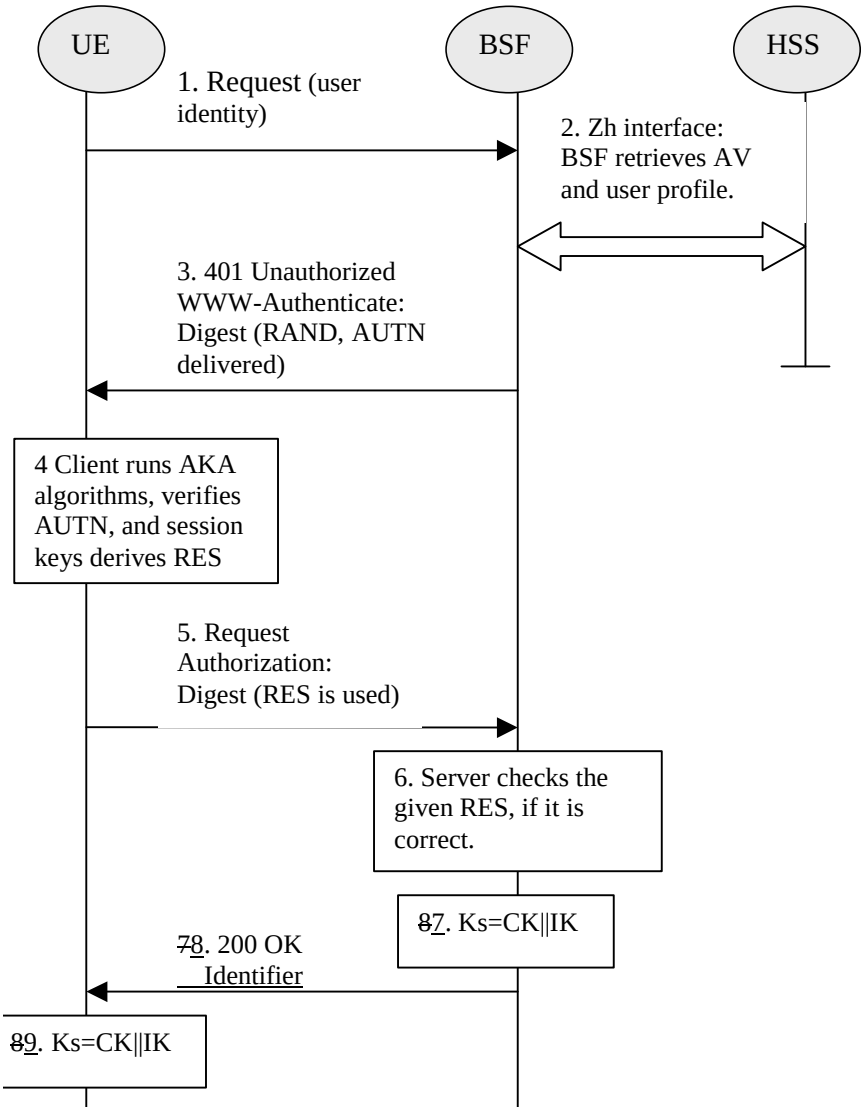

Figure 4: The bootstrapping procedure

1. The UE sends an HTTP request towards the BSF.
2. BSF retrieves the user profile and a challenge, i.e. the Authentication Vector (AV, AV = RAND||AUTN||XRES||CK||IK) over Zh interface from the HSS.
3. Then BSF forwards the RAND and AUTN to the UE in the 401 message (without the CK, IK and XRES). This is to demand the UE to authenticate itself.
4. The UE calculates the message authentication code (MAC) so as to verify the challenge from authenticated network; the UE also calculates CK, IK and RES. This will result in session keys IK and CK in both BSF and UE.
5. The UE sends request again, with the Digest AKA RES as the response to the BSF.
6. If the RES equals to the XRES that is in the AV, the UE is authenticated.
7. BSF generates key material Ks by concatenating CK and IK. Ks is used to derive the key material Ks_NAF. Ks_NAF is used for securing the Ua interface.
8. The BSF shall send 200 OK message and shall supply a transaction identifier to the UE to indicate the success of the authentication. The BSF may also supply the parameter *n* used to determine the NAF_Id_n (cf. previous bullet) to the UE over the Ub interface. If the parameter *n* is not supplied then no key derivation is performed, i.e. Ks = Ks_NAF.

9. The key material Ks is generated in UE by concatenating CK and IK. The Ks is used to derive the key material Ks_NAF. Ks_NAF is used for securing the Ua interface.

Ks_NAF is computed as Ks_NAF = KDF (Ks, key derivation parameters), where KDF is a suitable key derivation function, and the key derivation parameters include the user's IMSI, the NAF_Id_n and RAND. The NAF_Id_n consists of the n rightmost domain labels in the DNS name of the NAF, separated by dots (n= 1, ..., 7). For n = 0, NAF_Id_n equals the full DNS name of the NAF. The next bullet specifies how the UE obtains n.

NOTE: This note gives an example how to obtain the NAF_Id_n: if the DNS name of the NAF is "server1.presence.bootstrap.operator.com", and n = 3, then NAF_Id_n = " bootstrap.operator.com".

Editor's note: The definition of the KDF and the possible inclusion of further key derivation parameters is left to ETSI SAGE.

4.3.3 Procedures using bootstrapped Security Association

After UE is authenticated with the BSF, every time the UE wants to interact with an NAF the following steps are executed as depicted in figure 5.

UE starts communication over Ua interface with the NAF

- In general, UE and NAF will not yet share the key(s) required to protect Ua interface. If they already do, there is no need for NAF to retrieve the key(s) over Zn interface.

- If the NAF shares a key with the UE, but an update of that key it sends a suitable key update request to the UE and terminates the protocol used over Ua interface. The form of this indication may depend on the particular protocol used over Ua interface and is ffs.

- It is assumed that UE supplies sufficient information to NAF, e.g. a transaction identifier, to allow the NAF to retrieve specific key material from BSF.

- The UE derives the keys required to protect the protocol used over Ua interface from the key material, as specified in clause 4.3.2.

NOTE 1: The UE may adapt the key material Ks_NAF to the specific needs of the Ua interface. This adaptation is outside the scope of this specification.

NAF starts communication over Zn interface with BSF

- The NAF requests key material corresponding to the information supplied by the UE to the NAF (e.g. a transaction identifier) in the start of the protocol used over Ua interface.

- The BSF derives the keys required to protect the protocol used over Ua interface from the key material and the key derivation parameters, as specified in clause 4.3.2, and supplies to NAF the requested key material. If the key identified by the transaction identifier supplied by the NAF is not available at the BSF, the BSF shall indicate this in the reply to the NAF. The NAF then indicates a key update request to the UE.

NOTE 2: The NAF may adapt the key material Ks_NAF to the specific needs of the Ua interface in the same way as the UE did. This adaptation is outside the scope of this specification.

NAF continues with the protocol used over Ua interface with UE.

Once the run of the protocol used over Ua interface is completed the purpose of bootstrapping is fulfilled as it enabled UE and NAF to use Ua interface in a secure way.

Editor's note: Message sequence diagram presentation and its details will be finalized later.

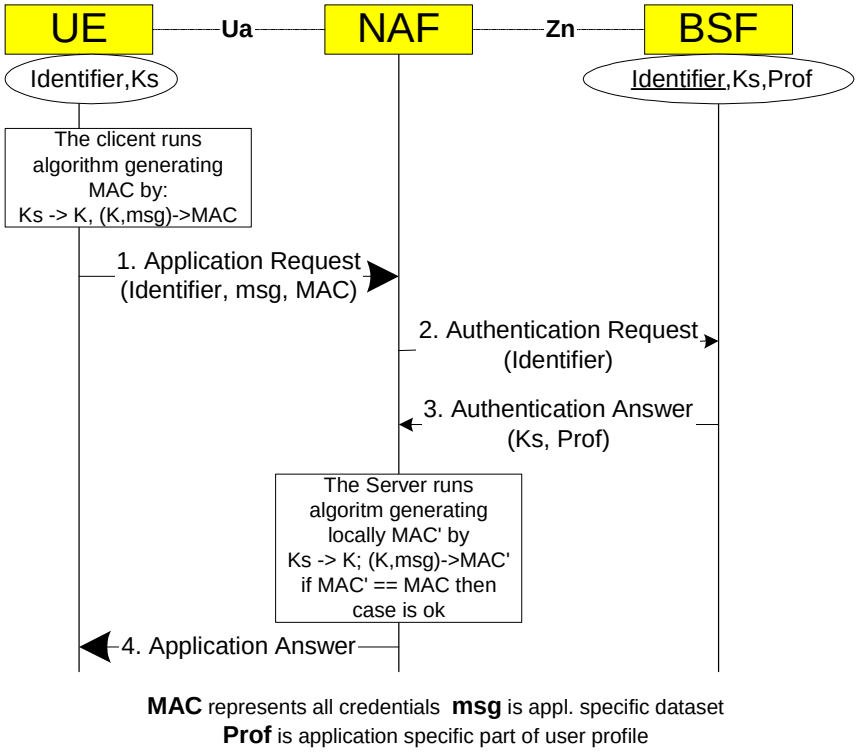

Figure 5: The bootstrapping usage procedure

4.3.4 Procedure related to service discovery

To enable the bootstrapping procedure, a procedure needs to be described on how to discover the location of BSF. 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 initial establishment of IP connectivity. The addresses need to be input only once.

- The address information shall be pushed automatically to the UE over the air interface when the subscription to bootstrapping service is accepted. All the parameters shall be saved in the UE and used the same manner as above. The procedure is specified in [7].

- The location information shall be discovered automatically based on DHCP, after the IP connectivity has been established. The DHCP server shall provide the UE with the domain name of a BSF and the address of a Domain Name Server (DNS) that is capable of resolving the Fully Qualified Domain Name (FQDN) of the BSF. The procedure is specified in [8].

Note: The location of DHCP server may be pushed to UE through the procedure specified in [7].

Note: The case when BSF located in the visited network is ffs in later phase of this work item.

Annex A (informative): Generic secure message exchange using HTTP Digest Authentication

A.1 Introduction

Editor's note: This annex describes how HTTP Digest Authentication can be used between UE and any NAF where the protocol over Ua interface is based on HTTP messaging. The protocol over Ua interface may depend upon the final choice of scheme made by SA WG3 and this will need to be reviewed later by SA WG3.

HTTP Digest Authentication model can also be used as a generic authentication and integrity protection method towards any new NAF. If a new NAF uses BSF-based security association, it could use this generic method to authenticate the UE (and UE authenticate the NAF) and integrity protect any payload being transferred between NAF and UE. As a generic method, it will speed up the specification of new NAFs since the authentication and message integrity protection part of Ua interface are taken care of by HTTP Digest Authentication. It will also ease the implementation of BSF-based authentication in NAFs because there would be one well-defined way to do it.

A.2 Generic protocol over Ua interface description

The sequence diagram in figure A.1 describes the generic secure message exchange with HTTP Digest Authentication. The conversation may take place inside a server-authenticated TLS [6] tunnel in which case TLS handshake has taken place before step 1.

In step 1, UE sends an empty HTTP request to a NAF. In step 2, NAF responds with HTTP response code 401 "Unauthorized" which contains a WWW-Authenticate header. he header instructs the UE to use HTTP Digest Authentication with a bootstrapped security association. Quality of protection (qop) attribute is set to "auth-int" meaning that the payload of the following HTTP requests and responses should integrity protected. The realm attribute contains two parts. The first part is a constant string "3GPP-bootstrapping" instructing the UE to use a bootstrapped security association. The second part is the DNS name of the NAF.

In step 3, the UE shall verify that the second part of the realm attribute does in fact correspond to the server it is talking to. In particular, if the conversation is taking place inside a server-authenticated TLS tunnel, the UE shall verify that the server name in the server's TLS certificate matches the server name in the realm attribute of the WWW-Authenticate header. The UE generates client-payload containing the message it wants to send to the server. Then it will generate the HTTP request by calculating the Authorization header values using the transaction identifier (base64 encoded) it received from the BSF as username and the session key Ks (base64 encoded) as the password, and send the request to NAF in step 4.

When NAF receives the request in step 5, it will verify the Authorization header by fetching the session key Ks from the bootstrapping server using Zn interface and the transaction identifier. After successful retrieval, NAF calculates the corresponding digest values using K, and compares the calculated values with the received values in the Authorization header. The NAF shall also verify that the DNS name in the realm attribute matches its own. If the conversation is taking place inside a server-authenticated TLS tunnel, the NAF shall also verify that this DNS name is the same as that of the TLS server. If the verification succeeds, the incoming client-payload request is taken in for further processing. Thereafter, the NAF will generate a HTTP response containing the server-payload it wants to send back to the client in step 6. The NAF may use session key Ks to integrity protect and authenticate the response.

In step 7, UE receives the response and verifies the Authentication-Info header. If the verification succeeds, the UE can accept the server-payload for further processing.

Additional messages can be exchanged using steps 3 through 7 as many times as is necessary. The following HTTP request and responses must be constructed according to [3] (e.g., nc parameter must be incremented by one with each new HTTP request made by UE).

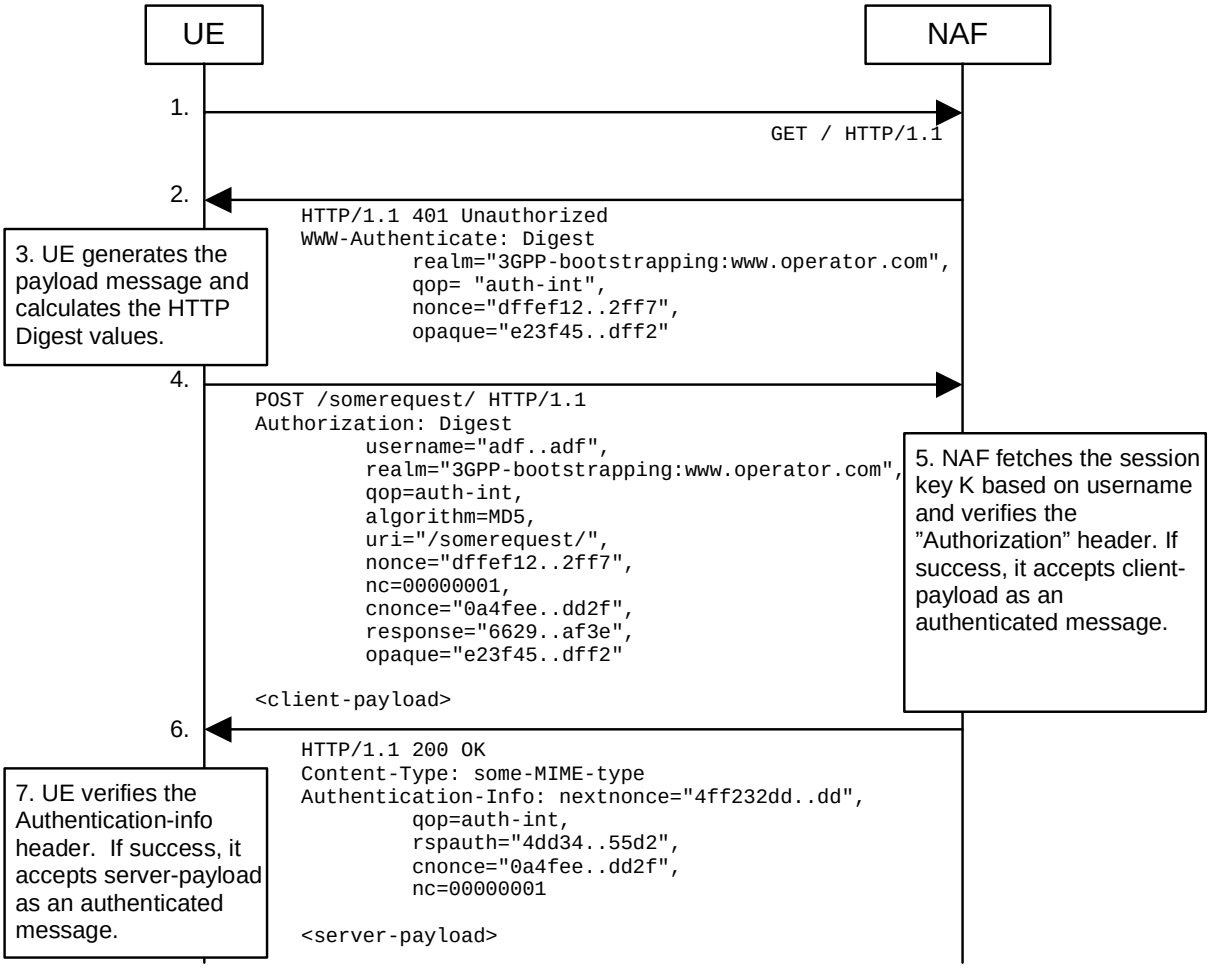

Figure A.1: Generic secure message exchange using HTTP Digest Authentication and bootstrapped security association

Annex B (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2003-10	SA3#30				New draft TS: Generic Bootstrapping Architecture (GBA). Extracted from 33.109 clause 4 and Annex B.		0.1.0
2003-10	SA3#30	S3-030537			New interface names.		0.1.0
2003-10	SA3#30	S3-030538			Requirements for Ub and Zh interfaces added.	0.1.0	0.1.1
2003-10	SA3#30	S3-030545			NAF initiated bootstrapping added	0.1.0	0.1.1
2003-10					Imported Zn interface requirements from SSC TS.	0.1.0	0.1.1
2003-11	SA3#31	S3-030728			Bootstrapping procedure: merging of last two messages	0.1.1	0.2.0
2003-11	SA3#31	S3-030793			Key separation	0.1.1	0.2.0
2003-11	SA3#31	S3-030794			Removal of application specific user profile requirements from GBA	0.1.1	0.2.0
2003-11					Annex A: changed "session key K" to "session key Ks"	0.1.1	0.2.0
2003-12	SP-22	SP-030583	-	-	Presentation to TSG SA#22 for Information	0.2.0	1.0.0

3GPP TS 33.221 V1.0.0 (2003-12)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Support for Subscriber Certificates (Release 6)

Keywords
Security, GAA, Subscriber certificates

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document describes subscriber certificate distribution by means of generic bootstrapping architecture (GBA) [11]. Subscriber certificates support services whose provision mobile operator assists, as well as services that are offered by mobile operator.

The scope of this specification presents signalling procedures for support of issuing certificates to subscribers, the standard format of certificates, and digital signatures. It is not intended to duplicate existing standards being developed by other groups on these topics, and will reference these where appropriate.

Editor's note: The specification objects are scheduled currently in phases. 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. In later phases, other configurations may be considered.

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.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

Subscriber certificate: a certificate issued to a subscriber. It contains subscriber's own public key and possibly other information such as subscriber's identity in some form.

CA certificate: A Certificate Authority signs all certificates that it issues with its private key. The corresponding Certificate Authority public key is itself contained within a certificate, called a CA Certificate.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AK	Anonymity Key
AKA	Authentication and Key Agreement
BSF	Bootstrapping server functionality. BSF is hosted in a network element under the control of an MNO.
BSP	BootStrapping Procedure
CA	Certificate Authority
CMP	Certificate Management Protocols
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
HSS	Home Subscriber System
IK	Integrity Key
MNO	Mobile network operator
NAF	Operator-controlled network application function functionality. NAF is hosted in a network element under the control of an MNO.
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
SCP	Subscriber Certificate Procedure
UE	User Equipment

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 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 [15].

4.2.8 Requirements on Ua interface

The requirements for 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 Zn interface [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.

4.3 Certificate issuing architecture

4.3.1 Reference model

Figure 1 shows a simple network model of the entities involved in the certificate issuing, and the protocols used between the network entities.

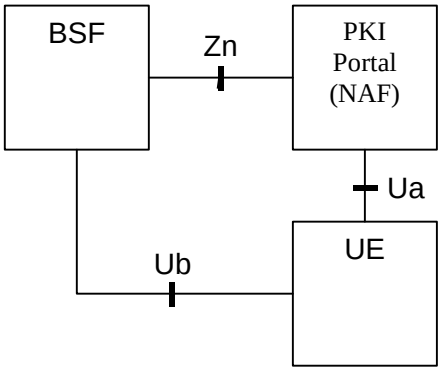

Figure 1: Simple network model for certificate issuing

4.3.2 Network elements

4.3.2.1 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 (over Ub interface). PKI Portal may also function as a Certification Authority (CA) who issues 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.

4.3.2.2 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).

4.3.2.3 UE

The required new functionality from UE is the support of the 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).

4.3.3 Reference points

4.3.3.1 Ua interface

4.3.3.1.1 General description

In the certificate issuing, 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 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 over Ua interface. 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, over 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 Ua interface are based on the BSF generated shared secret.

4.3.3.1.2 Functionality and protocols

4.3.3.1.2.1 PKCS#10 with HTTP Digest Authentication

Editor's note: This section uses HTTP Digest authentication to authenticate and integrity protect the certificate request and response. Shared key TLS is another solution to authenticate and protect the certificate enrolment, and whether it should be used instead of HTTP Digest is ffs.

HTTP Digest Authentication scheme [5] may be done with BSF shared key material the following way:

- UE makes a blank HTTP request to the NAF;
- NAF returns a HTTP response with "WWW-Authenticate" header indicating that HTTP Digest Authentication is needed. Quality of protection (qop) attribute is set to "auth-int" meaning that the content in following HTTP requests and responses are integrity protected;
- UE calculates the correct response to the "WWW-Authenticate" header using the *identifier* (base64 encoded) as the username and the session key Ks (base64 encoded) as the password. The session key Ks is has been previously derived from the key material Ks that resulted from using Ub interface. HTTP Digest Authentication parameters are returned in the "Authorization" header of HTTP Response;
- NAF validates the "Authorization" header and upon successful validation, performs the requested task. In the corresponding HTTP response, NAF calculates the relevant values for "Authentication-Info" header, which is used to authenticate and integrity protect the NAF response;
- UE validates the "Authentication-Info" header and upon successful validation, accepts the payload in the HTTP response.

A PKCS#10 [1] based certification request is sent to the CA NAF using a HTTP POST request, which MUST be authenticated and integrity protected by HTTP Digest Authentication.

Certificate is delivered using the HTTP response, which MAY be authenticated and integrity protected by HTTP Digest Authentication. The content-type of the HTTP response depends on the response format. If a certificate is returned then it is "application/x-x509-user-cert".If a pointer to the certificate is returned then it is "application/vnd.wap.cert-response" as specified in [9]. The content-type and the format of the certificate chain is ffs.

The UE requests a CA certificate delivery by sending a plain HTTP GET request with specific parameters in the request URI. The request MAY be authenticated and integrity protected by HTTP Digest Authentication.

CA certificate is delivered using the HTTP response, which MUST be authenticated and integrity protected by HTTP Digest Authentication. The content-type of the HTTP response would be "application/x-x509-ca-cert". Note that the user should always be notified when a new CA certificate is taken into use.

4.3.3.1.2.2 Key Generation

If the private key is stored in a UICC (e.g.in a WIM) and the UICC demands a special authorization (e.g. from the Operator) to generate the key, the ME may need to perform an HTTP POST request, which MAY be authenticated and integrity protected by HTTP Digest Authentication, to the NAF in order to deliver a nonce that is generated by the UICC. This will allow the NAF to authenticate directly to the UICC application and provide authorization for the key generation.

4.4 Certificate issuing procedure

Editor's note: This section uses HTTP Digest authentication to authenticate and integrity protect the certificate request and response. Shared key TLS is another solution to authenticate and protect the certificate enrolment, and whether it should be used instead of HTTP Digest is ffs.

4.4.1 Certificate issuing

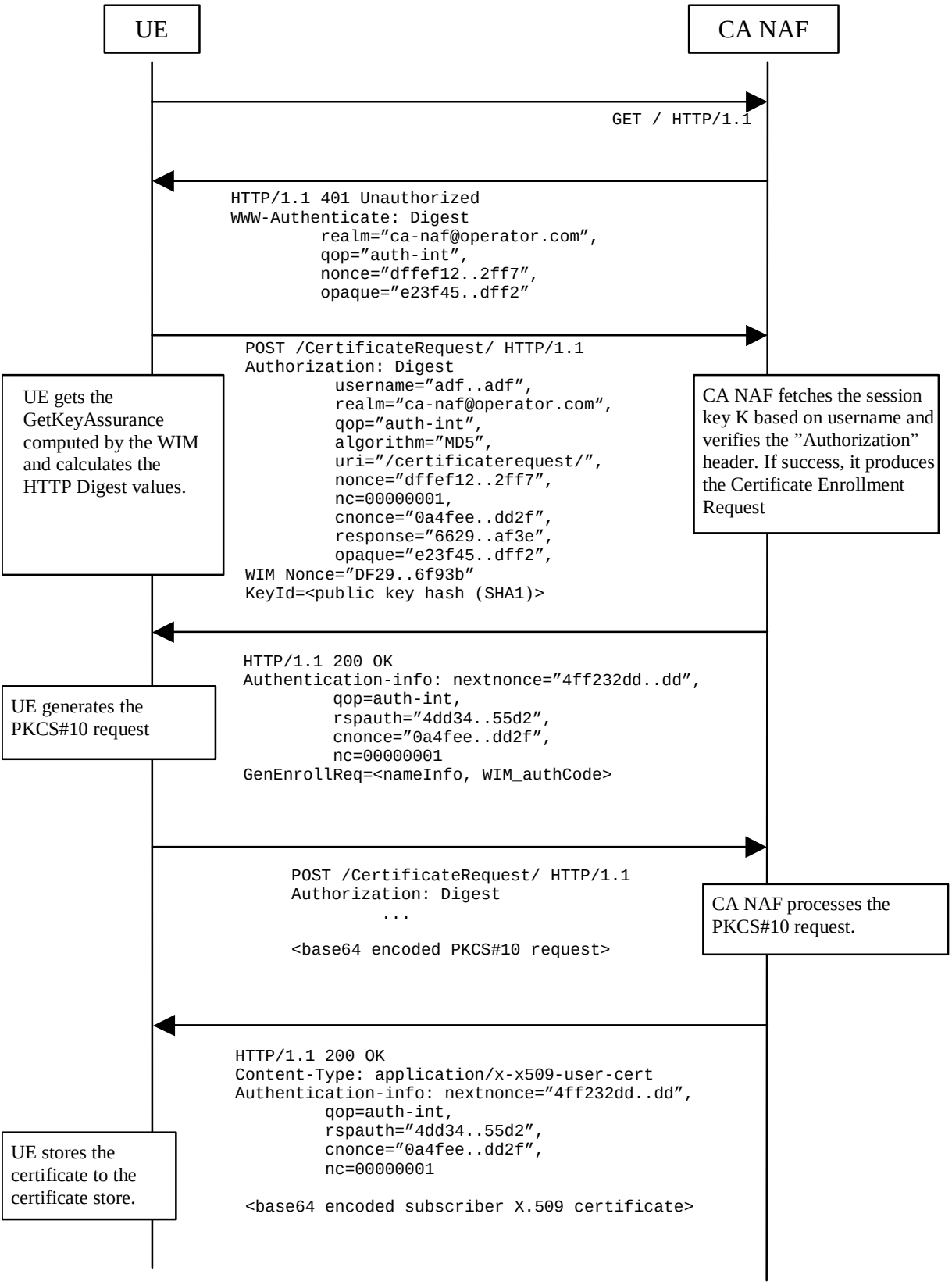

Figure 2: Certificate request using PKCS#10 with HTTP Digest Authentication

The sequence diagram above describes the certificate request when using PKCS#10 with HTTP Digest. The sequence starts with an empty HTTP request to CA NAF. The CA NAF responds with HTTP response code 401 "Unauthorized" which contains a WWW-Authenticate header. The header instructs the UE to use HTTP Digest authentication.

The UE will generate the HTTP request by calculating the Authorization header values using the identifier it received from the BSF as username and the session key Ks. If the certificate request needs extra assurance by a WIM application for key Proof of Origin, the UE should include a WIM Nonce and the key id (i.e. SHA-1 public key hash) in this request

When CA NAF receives the request, it will verify the Authorization header by fetching the session key Ks from the bootstrapping server using the identifier, then calculating the corresponding digest values using K, and finally comparing the calculated values with the received values in the Authorization header. If the verification succeeds, the CA NAF may use the subscriber profile to compute and send back a GenEnrollReq attribute containing additional parameters that are needed for the following PKCS#10 request generation (e.g. nameInfo, WIM_authCode, ...). The CA NAF may use session key Ks to integrity protect and authenticate this response.

The UE will then generate the PKCS#10 request and send it to the CA NAF by using an HTTP Digest request. In the case that the private key is stored in a WIM application the ME should request the AssuranceInfo from the WIM application and include it in the PKCS#10 request, if provided (see annex B for all details). The AssuranceInfo provides a proof of origin for the key processing.(e.g. identifies the WIM application and provides a proof that the key is stored in it). UE may indicate the desired format of the certification response: a certificate, a pointer to the certificate (e.g., URL), or a full certificate chain (i.e., from the issued certificate to the corresponding root certificate). The enrolment request shall be as follows:

POST <base URL>?response=<indication>[other URL parameters] HTTP/1.1
Content-Type: application/x-pkcs10

<base64 encoded PKCS#10 blob>

where:
<base URL> identifies a server/program.
<indication> used to indicate to the CA NAF what is desired response type for the UE. The possible values are: "single" for subscriber certificate only, "pointer" for pointer to the subscriber certificate, or "chain" for full certificate chain.
[other URL parameters] are additional, optional, URL parameters.

The incoming PKCS#10 request is taken in for further processing. If the CA NAF is actually a registration authority (RA NAF), the PKCS#10 request is forwarded to CA using any protocol available (e.g., CMC or CMP). After the PKCS#10 request has been processed and a certificate has been created, the new certificate is returned to the CA NAF. It will generate a HTTP response containing the certificate, or the pointer to the certificate as defined subclause 7.4 of [9], or a full certificate chain from issued certificate to the root certificate.

If the HTTP response contains the subscriber certificate itself, it shall be base64 encoded, and it may be demarcated as follows:

HTTP/1.1 200 OK
Content-Type: application/x-x509-user-cert

-----BEGIN CERTIFICATE-----
<base64 encoded X.509 certificate blob>
-----END CERTIFICATE-----

If the HTTP response contains the pointer to the certificate itself, the CertResponse structure defined in subclause 7.3.5 of [9] shall be used, and it may be demarcated as follows:

HTTP/1.1 200 OK
Content-Type: application/vnd.wap.cert-response

-----BEGIN CERTIFICATE RESPONSE-----
<base64 encoded CertResponse structure blob>
-----END CERTIFICATE RESPONSE-----

If the HTTP response contains a full certificate chain, each certificate shall be base64 encoded and shall be demarcated as follows:

HTTP/1.1 200 OK
Content-Type: ffs

-----BEGIN CERTIFICATE-----
<base64 encoded X.509 certificate blob>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<base64 encoded X.509 certificate blob>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<base64 encoded X.509 certificate blob>
-----END CERTIFICATE-----

The certificates in the response are not needed to be in any particular order. The content-type header value for the certificate chain is ffs.

The CA NAF may use session key Ks to integrity protect and authenticate the response, if a certificate or a pointer to the certificate is sent to the UE. The CA NAF shall use integrity protection and authenticate the response if full certificate chain is sent to the UE.

When UE receives the subscriber certificate, it is stored to local certificate management system.

NOTE: On board key generation is already defined in the WIM specification [8] issued by Open Mobile Alliance (OMA) group.

4.4.2 CA Certificate delivery

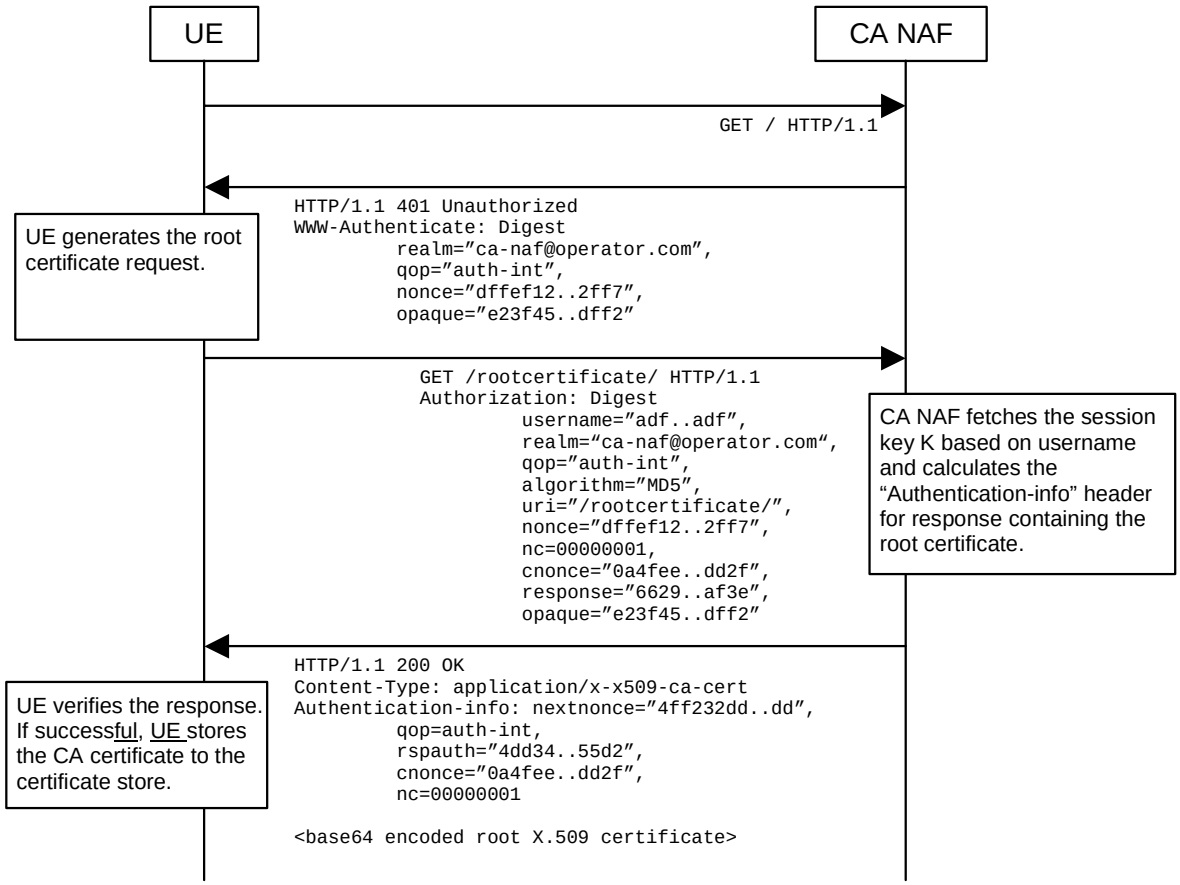

Figure 3: CA certificate delivery with HTTP Digest authentication

The sequence diagram above describes the CA certificate delivery when using HTTP Digest authentication. The sequence starts with an empty HTTP request to CA NAF. The CA NAF responds with HTTP response code 401 "Unauthorized" which contains a WWW-Authenticate header. The header instructs the UE to use HTTP Digest for authentication.

The UE generates another HTTP request for requesting the CA certificate. UE shall indicate the CA issuer name in the request URL as specified in subclause 7.4.1 of [9]. The serial number field shall be omitted. The Authorization header values are calculated using the identifier and the session key Ks. The authentication of this HTTP request is not necessary, but it is done in order to follow HTTP Digest authentication specification. Also, the identifier needs to be transported to the CA, i.e. the NAF. A request of subscriber's certificate is specified in subclause 4.4.1.1. The CA certificate delivery request shall be as follows:

GET <base URL>?in=<issuer name>[other URL parameters] HTTP/1.1

where
<base URL> identifies a server/program.
<issuer name> identifies the certificate issuer. It is a base64 encoding of the DER encoded Issuer field in the X.509 certificate.
[other URL parameters] are additional, optional, URL parameters.

When CA NAF receives the request, it may verify the Authorization header by fetching the session key Ks from the bootstrapping server using the identifier. CA NAF will generate a HTTP response containing the CA certificate and use the session key Ks to authenticate and integrity protect the HTTP response using the Authentication-info header. Essentially, the response could also be other delivery protocol in HTTP format, e.g. PKCS#7 cryptographic message with content type signedData.

HTTP response contains the CA certificate. The CA certificate shall be base64 encoded, and it may be demarcated as follows:

HTTP/1.1 200 OK
Content-Type: application/x-x509-ca-cert

-----BEGIN CERTIFICATE-----
<base64 encoded X.509 certificate blob>
-----END CERTIFICATE-----

When UE receives the new CA certificate, it must validate the Authentication-info header. If validation succeeds, the user is notified that a new CA certificate is taken into use. If user accepts the new CA certificate, it is stored to the local certificate management system and marked as "trusted" CA certificate.

4.5 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.

4.5.1 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]).

4.5.2 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.

Annex A (informative): Key pair storage

A.1 Introduction

The storage of the public/private key pair associated to the requested subscriber certificate is relevant to the procedure of issuing subscriber certificates.

The key pair storage can be performed in different ways. The nature of this storage may have impacts on the trust level associated to the subscriber certificates.

This annex provides a key pair storage security risk analysis in different scenarios.

A.2 Key pair storage use-cases

There are different scenarios to store the public/private key pair associated to the requested subscriber certificate.

A.2.1 Key pair storage on the ME

A possible place for the storage of the key pair is the Mobile Equipment.

The extension of the scope of the subscriber certificates outside the cellular domain to SIMless terminal introduces two alternatives for the key pair storage on the ME: key pair storage on the MT or on the TE.

A.2.2 Key pair storage on the UICC

Another solution for the storage of the key pair is the UICC.

For the following study we will consider only two key pair storage use-cases: on the ME or on the UICC.

A.3 Threats associated with the key pair

A.3.1 Key pair generation

The key pair generation is a very sensitive operation for the secrecy of the private key. The key pair generation has to be of good quality and the exchange, between the device where the key pair generation took place and the device where the key pair will be stored, has to be protected to avoid private key cloning/disclosure. UICC provides a greater level of protection, compared to ME, against unauthorized access to the private key itself.

A.3.2 Unauthorized usage of the private key

There are two kinds of threats associated with unauthorized usage of the private key:

1. An attacker getting hold of the private key; and
2. An attacker using the private key of the victim without getting hold of that key.

With respect to threat 1, having the key in UICC offers better protection than having it in the ME. However, an attacker who can compromise the ME can possibly *use* the private key for unauthorized purposes even if it is in the UICC because the UICC does not have direct trusted path to the user.

Attacks due to threat 2 always require an interaction with the UE to gain access to the UICC. While with the threat 1, as soon as the key is retrieved, the associated attacks do not requires any interaction with the UE to use the retrieved private key.

A.3.3 Portability

If the key pair is stored on the Mobile Equipment there is a threat in case of a new UICC inserted in this ME. There will be on the ME personal and sensitive data that do not belong to the new user. Since access to private keys is protected by PINs or passwords, the new user cannot access the private key of the old user unless he knows the PIN or the password.

Also, an important aspect of enrolling subscriber certificates based on AKA is the use of short-lived certificates. With short-lived certificates, even if the new user can access the old user's private key, it could happen that he cannot masquerade as the old user in authorization transactions because he can no longer get subscriber certificates for the key pair on behalf of the old user if the subscriber certificate expired. Moreover, if the key pair in ME is short-lived, owner of the new UICC will not be able to use that key pair after the pair expires. But there is no assumption that the subscriber certificate/key pair expired when the new user gets access to the old user's private key. In general, short-lived keys – on UICC or on ME – are useful for identity and privacy protection. Frequent change of key pair prevents outsiders from linking together transactions made by same user.

A.3.4 Environment

The threats to the key pair depend on the environment, the place of the key pair storage.

All implementations on mobile terminal, PC, MAC or PDA leave potential risks such as the possibility to load Trojan horses, worms or virus. Software applications lack the protective mechanisms existing in smart card (tamper resistance, physical encapsulation of critical circuitry). Reverse engineering techniques, such as extracting program code and disassembly/debugging methods, are simplified greatly in a software environment, allowing a token's secret components such as cryptographic algorithms, private keys, and other assumed secure information to be recovered.

Currently, the Mobile Equipments do not have all the hardware and software countermeasures that are built into UICC to protect them against invasive and non-invasive attacks performed to retrieve secrets. But mechanisms like code signing are already being taken into use.

A.3.5 Threat to the required properties for digital signatures

To be valid, digital signatures require the following properties:

- Authenticity: a valid signature implies that the signer deliberately signed the associated message;
- Unforgeability: only the signer can give a valid signature for the associated message;
- Non-re-usability: the signature of a document can not be used on another document;
- Non-repudiation: the signer can not deny having signed a document that has valid signature;
- Integrity: ensure the contents have not been modified.

Those properties involve the secrecy of the keying material, having a trusted input/output path to the user, and the use of strong and secure cryptographic mechanisms.

So, the trust in the digital signatures depends on the storage of the key pair and the related cryptographic computations and the security of communication between the user and the module performing private key operations. The impacts of the key pair storage are studied in the following clause A.4.

A.4 Security risk analysis related to key pair storage

There are many different subscriber use-cases describing the range of applications or services utilizing subscriber certificates. But, the level of trust associated to the proposed services depends on the key pair storage. This will be presented in the following security risk analysis.

A.4.1 Subscriber certificate use-cases

The use-cases for subscriber certificates can be divided into 2 main categories:

A.4.1.1 Secure services

Those services provide convenient way of authenticating cellular subscribers to services. These services can be provided by cellular operators, corporations, or 3rd party content providers. Secure services may also support billing.

The different subscriber use-cases could be:

- person-to-person authentication: per-to-per authentication;
- corporate services: authentication to corporate intranet applications;
- person-to-content:
  - access to Presence services;
  - self-service management;
  - access to operator's Web services;
  - access to 3rd party content services;
  - enhanced LCS privacy;
  - notifications through cellular network;
  - MBMS security;
  - support of Liberty Alliance use cases;
- small to medium payment through cellular operator.

A.4.1.2 Secure connectivity

This service utilizes cellular infrastructure and existing operators customer relationships to authenticate users:

- alternative access authentication:
  - corporate WLAN access authentication;
  - broadband access, e.g. DSL or cable access;
- service authentication: e.g. VPN authentication.

A.4.2 Security risk analysis in some scenarios

All subscriber use-cases do not require the same level of security for the key pair storage since they propose services that have different features in terms of:

- added value: high or low valued services;
- involved partners and trust relationships: there is agreement between different cellular network operators or between cellular network operator and service provider or 3rd party content provider;

- type of required certificates (short-lived or long-term certificates).

This section presents some scenarios where the nature of the key pair storage has security impacts on the service.

A.4.2.1 Scenarios involving subscriber's personal data

An example of scenario involving subscriber's data could be the self-service management.

A.4.2.1.1 Self-service management

This scenario allows user to authenticate to a Web portal, run by operator, to achieve secure access for self-provisioning. Secure end-to-end (TLS) tunnel from the terminal to the Web portal can be established (subscriber's private key and the certificate are used in standard fashion, i.e. no changes needed in TLS components). The user can have either mobile or fixed network access (e.g. GPRS, WLAN, or xDSL). The main use cases are billing information queries and modifying one's subscription profile.

User experience:

The authorization may be based directly on subscriber certificates, or on a combination of authentication with subscriber certificate and access control list in the Web portal. In the first case the self-management server:

- receives an assertion signed by the data owner, which contains a public key and set of access rights;
- verifies that the sender of the assertion holds the matching private key; and
- allows the secure access (e.g. TLS connection) only if the verification succeeds.

A.4.2.1.2 Security Risk Analysis in this scenario

The security risk analysis is performed according to the unauthorized usage threats identified in clause A.3.2.

Unauthorized usage by using the private key of the victim without retrieving the private key:

Potential attack:

so, an attacker could get usage of the subscriber private key to authenticate to the Web portal and access for self-provisioning. The attacker could for example modify the subscription profile of the subscriber.

Feasibility:

the attacker requires an interaction with the UE to gain access to the UICC.

the attack applies in case of:

- key pair storage on the ME;
- key pair storage on the UICC.

Unauthorized usage by getting hold of the private key:

Potential attack:

so, an attacker could retrieve the subscriber private key to authenticate to the Web portal and access for self-provisioning. The attacker could for example modify the subscription profile of the subscriber.

Feasibility:

once the key retrieved, the attacker does not require any interaction with the UE equipment to gain access to the UICC.

the attack applies in case of:

- key pair storage on the ME

  This attack is based on the key retrieval. So, as the UICC is tamper resistant device so the attack does not apply to UICC.

Consequences of these attacks:

the self-service management is low added value and the consequences of the key pair storage on the UE are limited.

A.4.2.2 Scenarios involving payment and agreement between operator and service provider

Some scenarios deal with payment and agreement between cellular network operator and service provider, 3rd party.

A.4.2.2.1 Notifications through cellular network scenario

The subscriber authorizes the operation of sending notifications by service provider through the cellular network. The service provider does not need to know subscriber's identity. If there is no identity information in the certificate, then the subscriber may remain anonymous towards the service provider. However, subscriber may pay for the notification through his phone bill. Subscriber authorizes such payment and the charging is triggered when the service provider sends a notification.

User experience:

During a transaction UE sends to the service provider an assertion, i.e. signed authorization, to send a notification message to that UE through the cellular network, and subscriber certificate or subscriber certificate URL. The service provider verifies the authorization text and UE's signature with the aid of subscriber certificate. If the signature and the authorization text are correct, then the service provider will send a positive acknowledgement to the UE.

At a later time, for example when a certain sport's event takes place, the service provider creates a notification and submits it to the operator together with the signed UE's authorization and subscriber's certificate. The operator verifies the signed authorization. If the verification succeeds the operator will forward the notification text to the subscriber in an SMS or MMS message.

A.4.2.2.2 Small to medium payment through cellular operator scenario

The subscriber authorizes payment for a service through his phone bill (or with separate bill). Note that the provider of the service does not need to know subscriber's identity. If there is no information in the certificate, then the subscriber may remain anonymous towards the service provider. The service may be e.g. non-cellular access in a environment where the operator's traditional billing mechanisms are not directly applicable, e.g. non-cellular access is provided by 3rd party.

During a payment transaction the UE sends to the service provider a signed invoice and subscriber certificate (or subscriber certificate URL). The service provider verifies the UE's signature with the aid of subscriber certificate. If the signature and the invoice are correct, then the service provider will grant UE access to, or deliver the requested service.

In the settlement phase the service provider forwards the signed invoice to the operator for verification. If the verification is successful then the operator will reimburse service provider and charge the subscriber the price of the service through his phone bill (or with separate bill).

Prerequisite:

the service provider has a business relationship with operator that issued subscriber's certificate and it knows operator's signature verification key.

if the service provider (e.g. visited access network provider abroad) does not have a direct relationship with the subscriber's home network, the certificate should come from the visited network. The independent access network provider trusts the visited operator as well as the subscriber authentication and certificate from that operator.

User experience:

the subscriber trusts the billing from the home operator and payment is convenient. During the service usage he will have to type in the payment PIN for configured amounts. The terminal may automatically sign very small amounts. In this case only larger amounts and cumulative sum above a threshold trigger the PIN query.

A.4.2.2.3 Security Risk Analysis in these scenarios

These secure services deal with payment and an agreement between a cellular network operator and a service provider. The nature of the key pair storage has consequences. The security risk analysis is performed according to the unauthorized usage threats identified in clause A.3.2.

Unauthorized usage by using the private key of the victim without retrieving the private key:

Potential attacks:

if the ME is not sufficiently secure, the attacker may have a program that shows the user a certain message ("payment of €1") but ask the UICC to sign a different message ("payment of €100). Also if the attacker's program discovers the PIN, it can command the UICC to generate signatures even without the user being aware of it.

Feasibility:

the attacker requires an interaction with the UE to gain access to the UICC.

these attacks apply in case of:

- key pair storage on the ME;
- key pair storage on the UICC.

Unauthorized usage by getting hold of the private key:

Potential attacks:

if an attacker manages to discover the subscriber's private key then an attack could consists in sending signed authorizations to the service provider, then the subscriber would have to pay for services he did not ask for.

Feasibility:

once the key retrieved, the attacker does not require any interaction with the UE equipment to gain access to the UICC.

The attack applies in case of:

- key pair storage on the ME.

This attack is based on the key retrieval. So, as the UICC is tamper resistant device so the attack does not apply to UICC.

Consequences of these attacks:

- forgeability: the subscriber could pay for services he did not ask for;
- repudiation: The cellular network operator and the service provider are not paid for the service they provided.

  If there is any way to attack the system a signer can repudiate the performed signatures arguing that the system is not secure. So, if it is possible to use the subscriber's private key without his deliberate consent, then the subscriber can repudiate the signatures sent for authorization, and not pay the associated phone bill. So,:

  - the operator and the service provider could not be paid for the proposed service;
  - the trust relationship between the operator and the service provider can be destroyed. The service provider has no guaranty of security; he would no longer trust the subscriber certificates issued by the cellular network operator and the associated signatures;

- if there is any problem due to some unauthorized usages of the subscriber private key then the trust in 3G PKI may be lost;
- high valued services involving payment and relationship with service provider or 3rd party content provider often require the use of long-term certificates. The issuance of long-term certificates requires more security constraints than the issuance of short-lived certificates. So, according to the unauthorized usage threats present on the UE, the security level may not satisfy the security requirements for long-term certificates issuance and usage.

A.4.3 Summary of risk analysis

To prevent the identified unauthorized usages of the private key the following recommendations need to be addressed:

- the storage of the private key and the related cryptographic computations to be done in a secure manner;
- the solution should provide a secure path to the private key usage.

The UICC provides the most secure location for storage and usage of the private key in terms of security (in the form of, e.g. the WIM application). This does not preclude the use of other locations for certain services. On the other hand, the ME can provide a secure path to using the private key (e.g. with mechanisms such as code signing). The combination of solutions will provide a complete secure solution and enable the deployment of secure services.

Annex B (informative): Enrolment request that includes AssuranceInfo from the Secure Element

The enrolment request will follow the PKCS #10 certificate enrollment format as defined in [1]. Adding AssuranceInfo in this request is defined in the OMA ECMA Script GenEnrollReq specification [14].

Annex C (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2003-10	SA3#30				First draft TS: Support for Subscriber Certificates (SSC). Extracted from 33.109 clause 5 and Annex A.		0.1.0
2003-10	SA3#30	S3-020536			Further clarification on WAP Certificate and CRL profile.		0.1.0
2003-10	SA3#30	S3-030537			New interface names		0.1.0
2003-10	SA3#30	S3-030645			Annex A material moved to the main body.	0.1.0	0.1.1
2003-10					Requirements on Zn interface moved to GBA TS.	0.1.0	0.1.1
2003-11	SA3#31	S3-030730			Subscriber Certificate Enrollment Protocol	0.1.1	0.2.0
2003-11	SA3#31	S3-030667			Updated Annex C to 33.109: Key pair storage	0.1.1	0.2.0
2003-11	SA3#31	S3-030795			Results of risk analysis in the "Key Pair Storage" informative annex	0.1.1	0.2.0
2003-11	SA3#31	S3-030796			PSEUDO CR on clarifications on Certificate enrollement using pre-certified keys	0.1.1	0.2.0
2003-11	SA3#31	S3-030797			PSEUDO CR on enrollment of keys in a WIM application	0.1.1	0.2.0
2003-11	SA3#31	S3-030685			PSEUDO CR on on-board key generation in a UICC	0.1.1	0.2.0
2003-11					Changed "session key K" to "session key Ks"	0.1.1	0.2.0
2003-12	SP-22	SP-030584	-	-	Presentation to TSG SA#22 for Information	0.2.0	1.0.0