3GPP TS ab.cde V0.1.0 (2003-04)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Bootstrapping of application security using AKA and Support for Subscriber Certificates;
System Description
(Release 6)

Editor's note:

The template of this draft:

[S3-030051]
Nokia and Siemens contribution: Draft TS Table of Contents for "Bootstrapping and Support for Subscriber Certificates"

Source documents are from S3:

[S3-020162]
Work Item Description

[S3-030036]
Alcatel contribution: Alternative proposals for subscriber certificate bootstrapping

[S3-030050]
Nokia and Siemens contribution: Bootstrapping of application security from 3G AKA and support for subscriber certificates

[S3-030072]
Nokia contribution: NAF-BSF (D interface) protocol

[S3-030073]
Nokia contribution: Protocol B: Subscriber Certificate Enrollment based on Bootstrapping

Select keywords from list provided in specs database.

Keywords

<keyword[, keyword]>

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.

Introduction

This clause is optional. If it exists, it is always the second unnumbered clause.

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, etc. Subscriber certificates support services whose provision mobile operator assists, as well as services that mobile operator provides.

The scope of this specification includes two parts. The first part presents a generic AKA bootstrapping function, an architecture overview and the detailed procedure how to bootstrap the credential. The second part is the requirement for applications utilizing the bootstrapping function, as well as the procedure of the utilization. Specifically the present document presents signalling procedures for support of issuing certificates to subscribers and 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 that, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

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

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

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

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

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

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

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

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

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

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

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

3 Definitions, symbols and abbreviations

Delete from the above heading those words which are not applicable.
Subclause numbering depends on applicability and should be renumbered accordingly.

3.1 Definitions

For the purposes of the present document, the [following] terms and definitions [given in ... and the following] apply.

Definition format
***<defined term>**: <definition>.*

example: text used to clarify abstract rules by applying them literally.

3.2 Symbols

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

Symbol format

<symbol> <Explanation>

3.3 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
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 AKA bootstrapping functions

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.

4.1.1 Access Independence

4.1.2 Authentication methods

4.1.3 Roaming

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.

Editor's note: The names for the reference points, A, B, C, and D need to be decided.

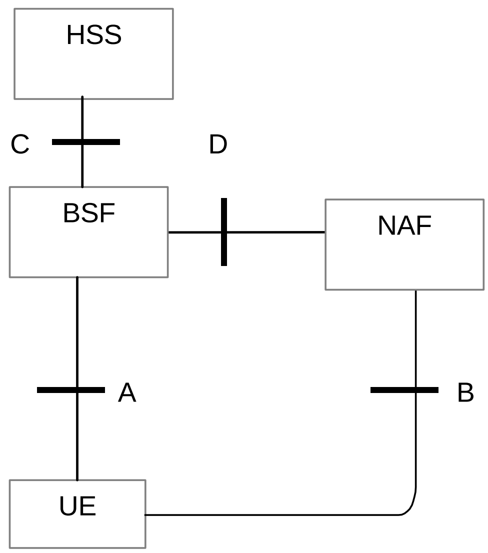

Figure 1: Simple network model for bootstrapping

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.

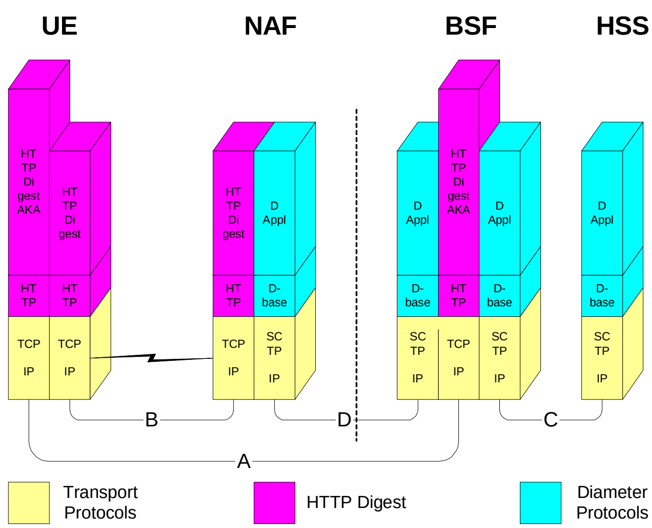

Figure 2: Protocol stack architecture

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).

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.
- The key material must be generated specifically for each NAF independently.

4.2.2.3 HSS

4.2.2.4 UE

4.2.3 Reference points

4.2.3.1 A

Protocol A is the bootstrapping authentication and key agreement protocol. It is run between the UE and the BSF and provides mutual authentication and key agreement between these entities. Protocol A is based on the 3GPP AKA [4] protocol that requires information from USIM and/or ISIM. The interface to the USIM is as specified for 3G [3].

4.2.3.2 B

Protocol B is the application protocol which is secured using the keys material agreed between UE and BSF as a result of the run of protocol A. For instance, in the case of support for subscriber certificates, 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 C

Protocol C 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 D

Protocol D is used by the NAF to fetch the key material agreed in protocol A from the BSF. It may also be used to fetch subscriber profile information from BSF.

4.3 Procedures

4.3.1 Bootstrapping procedures

When a UE wants to interact with an NAF, the UE must first run a bootstrapping authentication with the BSF with the following steps (see Figure 3):

Editor's note: Detail message sequence diagram will be added later here to present the AKA step in concrete form.

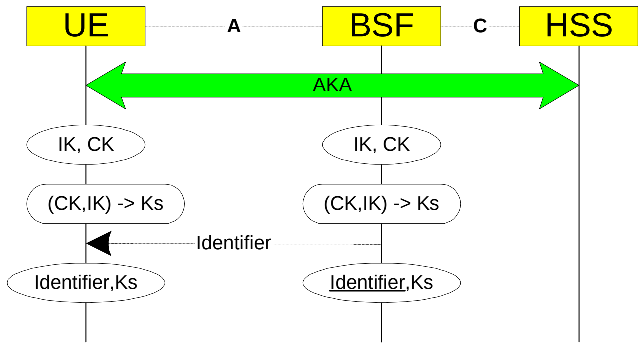

Figure 3: The bootsrapping procedure

UE runs protocol A with the BSF, which in turn runs protocol C with the HSS.

- This will result in session keys IK and CK in both BSF and UE.
- CK and IK are used in both BSF and UE to derive key material for use with protocol B. As the BSF is required to be independent of the particular application protocol B the key material is assumed to be sufficiently so that it can be used with any candidate protocol B. The key material shall not allow any NAF to infer information about CK and IK.
- BSF may supply a transaction identifier to UE in the course of protocol A (ffs, see below).

4.3.2 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 (see part B and D in):

UE starts protocol B with the NAF

- In general, UE and NAF will not yet share the key(s) required to protect protocol B. If they already do, there is no need for NAF to invoke protocol D.
- 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 protocol B from the key material.

NAF starts protocol D 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 protocol B.
- The BSF supplies to NAF the requested key material.
- The NAF derives the keys required to protect protocol B from the key material in the same way as the UE did.

NAF continues protocol B with UE

Once the run of protocol B is completed the purpose of bootstrapping is fulfilled as it enabled UE and NAF to run protocol B in a secure way.

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

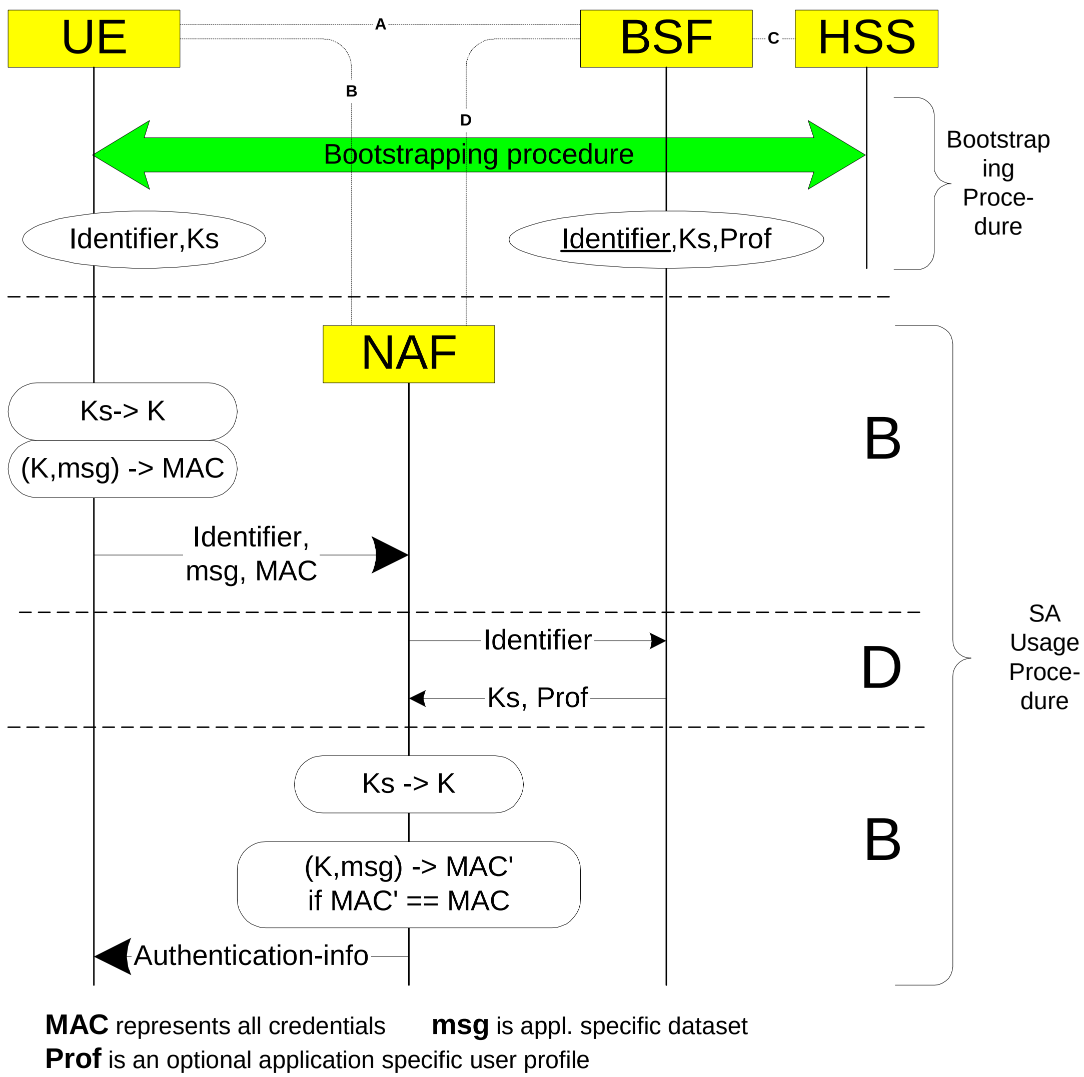

Figure 4: The bootstrapping usage procedure

5 Application specific functions using bootstrapping

5.1 Support for subscriber certificates

5.1.1 Introduction

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

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

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

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

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

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

5.1.2 Requirements and principles for issuing subscriber certificates

The following prerequisites for issuing of subscriber certificates exits:

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

5.1.2.1 Requirements on protocol B

The requirements for protocol B are:

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

5.1.2.2 Requirements on protocol D

5.1.3 Certificate issuing

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

A.1 Introduction

A.2 Additional requirements and principles

A.2.1 Usage of Bootstrapping

A.2.2 Access independence

A.2.3 Roaming and service network support

A.2.4 Home operator control

A.2.5 Charging principles

A.3 Certificate issuing architecture

A.3.1 Reference model

A.3.2 Network elements

A.3.2.1 PKI Portal

A.3.2.2 Bootstrapping Server Function

A.3.2.3 UE

A.3.3 Reference points

A.3.3.1 B

A.3.3.1.1 General description

A.3.3.1.2 Functionality and protocols

Editor's note: From five alternatives investigated in S3-030073 and S3-030036, only the following two have been agreed to add to the present document as potential solutions.

A.3.3.1.2.1 PKCS#10 with HTTP Digest Authentication

HTTP Digest Authentication scheme [RFC2617] 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 K (base64 encoded) as the password. The session key K is has been previously derived from the key material Ks that resulted from running protocol A. 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 [PKCS10] or a CRMF [RFC 2511] 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 is either "application/x-x509-user-cert" or "application/vnd.wap.cert-response" as specified in [WPKI].

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.

A.3.3.1.2.2 Certificate Management Protocols (CMP)

Certificate Management Protocols (CMP) [RFC2510] describes a set of messages that can be used between different PKI components, e.g., between the CA and the end entity as well as between two CAs. The messages used in the specification have the following general message structure called PKIMessage. PKIMessage contains four fields: PKIHeader, PKIBody, optional PKIProtection, and optional certificate list. The PKIHeader contains information, which is common to many PKI messages. The PKIBody contains the message-specific information. The PKIProtection, when used, contains bits that protect the PKI message. The certificate list can contain certificates that may be useful to the recipient. [RFC2510]

In CMP, authentication is achieved by the PKI issuing the end entity with a secret value (initial authentication key) and reference value (used to identify the transaction) via some out-of-band means. The initial authentication key can then be used to protect relevant PKI messages (see chapters 2.2.1.2. and 3.1.3 of [RFC2510] for details). Also a replay prevention mechanism is specified.

The supported certificate request formats are PKCS#10 [PKCS10] and CRMF [CRMF]. However, PKCS#10 format is not recommended by CMP. The certificate request is inserted in the PKIBody field of the PKIMessage. The response to the certificate request is a CertRespMessage that is inserted in the PKIBody field of the PKIMessage. The CertRespMessage contains the status of the response, and if certificate request was approved the certificate itself. CMP supports also a certification procedure where the key generation happens in the CA rather the in the UE. However, CMP states that this procedure is only optionally implemented by CAs. See more details in [RFC2510].

CMP defines data structures, which can support mechanism where the CA is able to publish its current public key using self-signed certificates that are distributed via some “out-of-band” means. Alternatively the self-signed CA certificate can be published on a directory server and a hash of the certificate can be distributed via some out-of-band means. The idea is that anyone who has securely received a hash value can verify the authenticity of the CA certificate. The structure of such a self-signed out-of-band certificate or hash is specified in the RFC. However, the way how the CA publishes the self-signed certificate and/or securely delivers the hash value is considered out-of-scope for CMP (see chapter 3.2.5 of [RFC2510]).

A.4 Certificate issuing procedures

A.4.1 Certificate issuing

Editor’s note: From five alternatives investigated in S3-030073 and S3-030036, only the following two have been agreed to add to the present document as potential solutions.

A.4.1.1 Certificate issuing using PKCS#10 with HTTP Digest Authentication

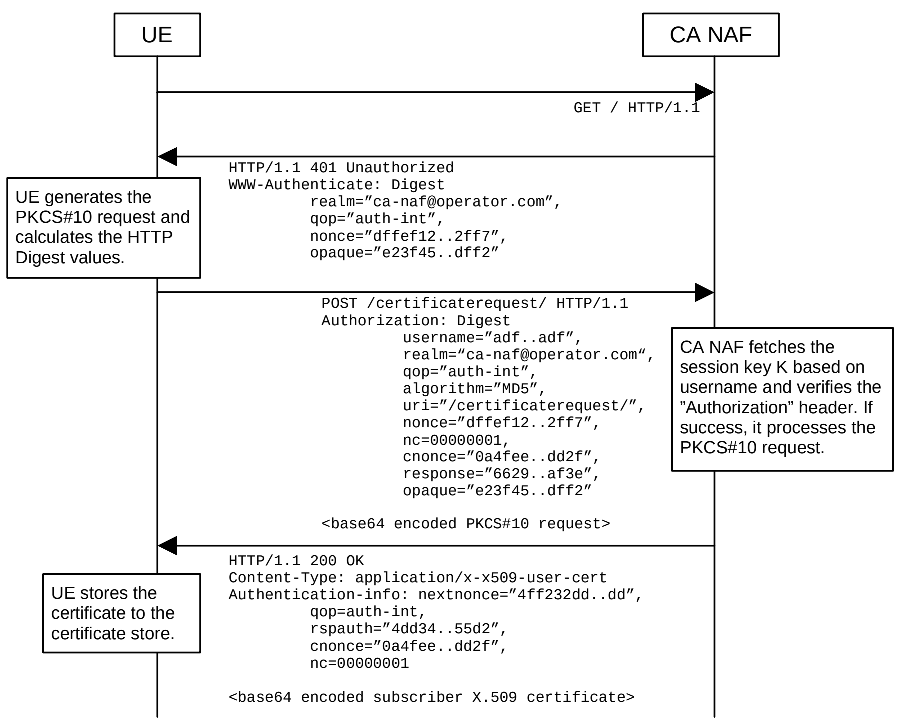

Figure 5: Certificate request using PKCS#10 with HTTP Digest Authentication.

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 generates a PKCS#10 request with the subject name, public key, additional attributes and extensions. Then it 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 K.

When CA NAF receives the request, it will verify the Authorization header by fetching the session key K 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 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. The CA NAF may use session key K to integrity protect and authenticate the response.

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

A.4.1.2 Certificate issuing with CMP

CMP defines two methods to do the certificate issuing: basic authenticated scheme and centralized scheme. In the basic authenticated scheme the key generation happens in the UE while in the centralized scheme the key generation is done in the CA (or RA). CMP states that the support for the basic authenticated scheme for certificate issuing is mandatory for CAs while the support for the centralized scheme is optional. See more details in chapters 2.2 and B8 of [RFC2510].

The messages can be transported using various methods such as file based protocol, (such files can be used to transport PKI messages e.g. using FTP, HTTP, email etc.), direct TCP-based management protocol, management protocol via e-mail, and management protocol via HTTP mentioned in section 5 of [RFC2510].

A.4.1.2.1 Basic authenticated scheme

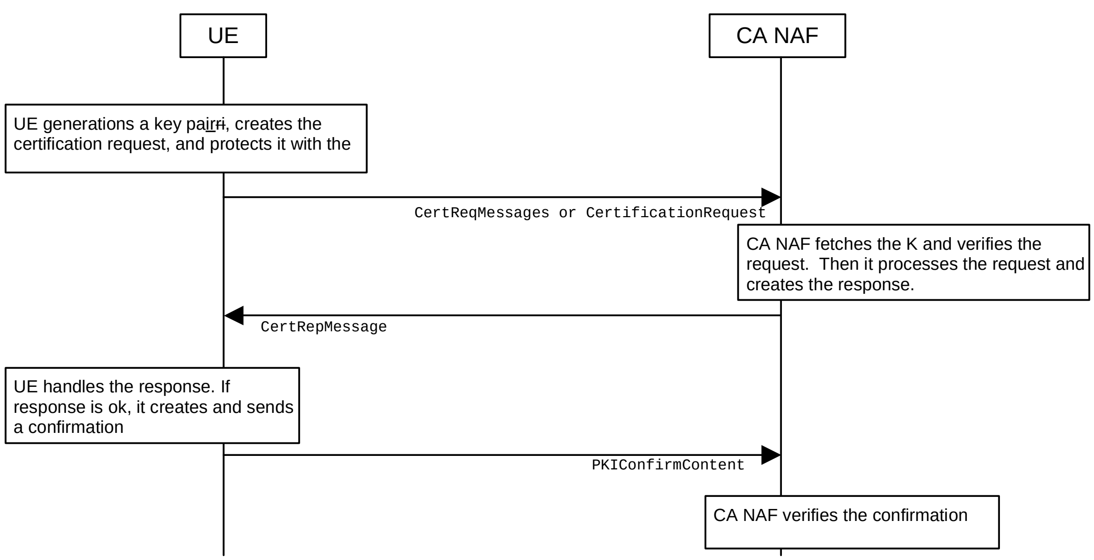

Figure 6: Certificate request using basic authentication scheme of CMP.

The sequence diagram above describes the certificate request and delivery procedure when using CMP and basic authenticated scheme [RFC2510]. The sequence starts with UE generating a key pair, creating the certificate request message format (CRMF) message, inserting it to CertReqMessages message, and integrity protecting this message with the initial authentication key (IAK). The session key K, which has been derived earlier using protocol A, can be used as IAK.

The certificate request message is sent to CA NAF who fetches the corresponding K based on the identifier received in the request. CA NAF verifies the request with the K. If the verification succeeds, the CA NAF processes the request, i.e. generates and signs the certificate and sends the certification response to the UE.

UE verifies the certificate response message with the K. If the message verification is successful, the issued certificate is stored to the device, and UE sends a confirmation message to the CA NAF.

CA NAF verifies the confirmation message. If the verification fails or CA NAF never receives the confirmation message, CA NAF must revoke the newly issued certificate if it has been already published.

A.4.1.2.2 Centralized scheme initiated by the UE

The centralized scheme provides a mechanism where the public/private key pair is generated outside the UE, e.g. by the CA.

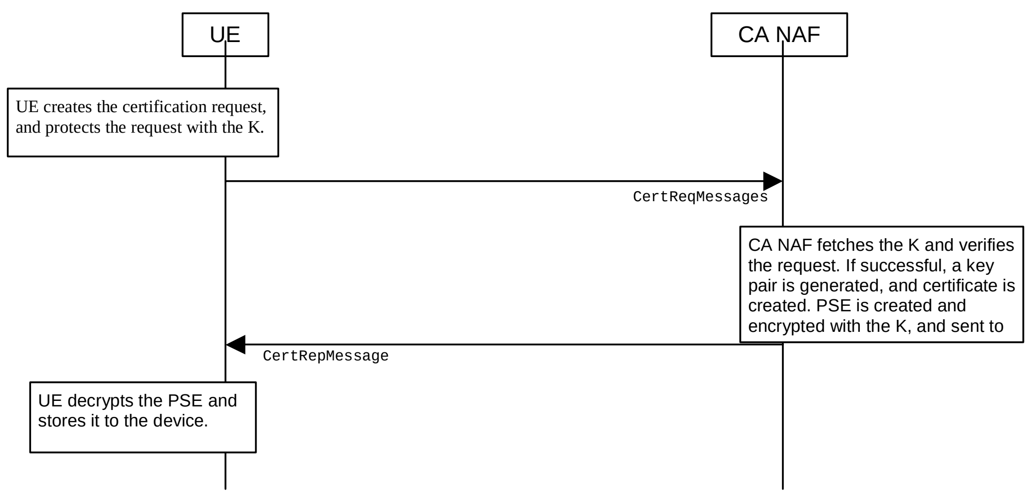

Figure 7: Certificate request using centralized scheme of CMP.

The sequence diagram above describes the delivery mechanism initiated by the UE using CMP in centralized scheme. This scheme is optional in CMP [RFC2510]. The sequence starts with the UE by creating CertReqMessages message with certain parameters, and protecting this message with initial authentication key (IAK). The session key K, which has been derived earlier using protocol A, can be used as IAK.

The certificate request message is sent to CA NAF who fetches the corresponding K based on the identifier received in the request. CA NAF verifies the request with the K. If the verification succeeds, CA NAF processes the request, i.e. generates a key pair, generates and signs the certificate, and sends the certification response containing the Personal Security Environment (PSE) encrypted to the UE. PSE typically contains the generated private key and newly issued certificate with corresponding public key.

UE verifies the certificate response message with the K. If the message verification is successful, the issued PSE is decrypted and stored to the device. A confirmation message is not sent in the centralized scheme.

A.4.2 CA Certificate delivery

A.4.2.1 CA Certificate delivery with HTTP Digest Authentication

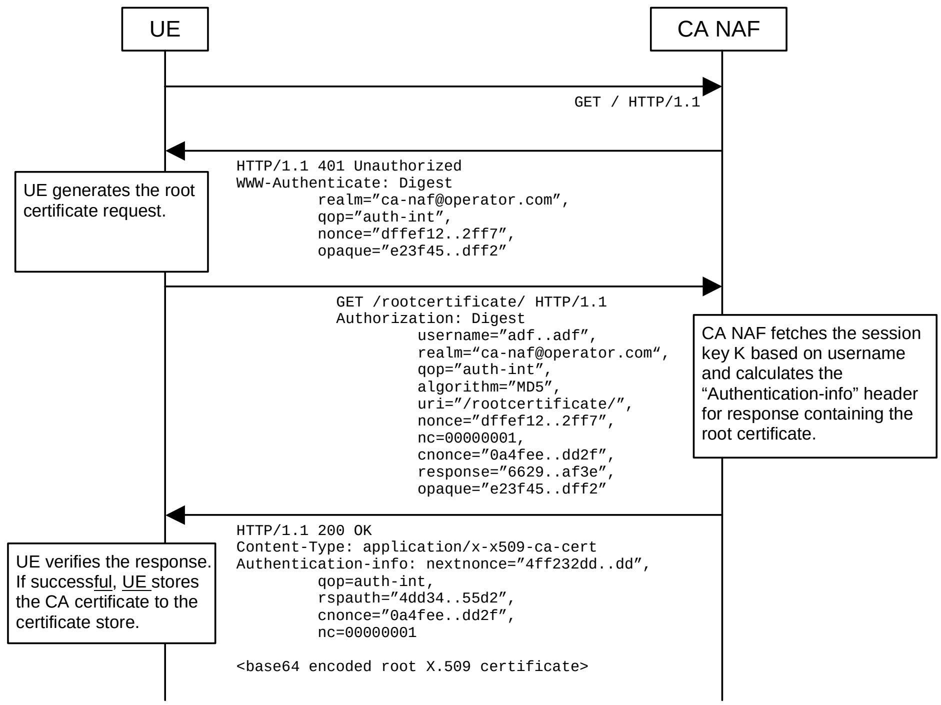

Figure 8: CA certificate delivery using PKCS#10 with HTTP Digest authentication.

The sequence diagram above describes the CA certificate delivery when using PKCS#10 with 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 empty HTTP request for requesting the CA certificate. The Authorization header values are calculated using the identifier and the session key K. 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 section A.4.1.1.

When CA NAF receives the request, it may verify the Authorization header by fetching the session key K from the bootstrapping server using the identifier. CA NAF will generate a HTTP response containing the CA certificate and use the session key K 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.

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.

A.4.2.2 CA Certificate delivery with CMP

CMP defines only out-of-band method for delivering CA certificates. CA certificate may be delivered as part of the certificate request, where the response could contain certificates that may be useful to the recipient. It can contain the whole certificate chain (including the CA certificate). The root CA produces a "self-certificate" and also produces a fingerprint of its public key. End entities that acquire this fingerprint securely via some out-of-band means can then verify the CA's self-certificate and hence the other attributes contained therein.

A.5 Functionality in presence of preloaded, long-lasting key pair

Editor's notes: Based on contribution S3-030037, it was agreed to add this part into the present document for ffs.

In this alternative solution, the UE 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 for the purposes of certificate request authentication. One possible solution is WPKI [WPKI] and one solution for storing long-lasting key pair is WIM [WIM].

The UE can issue a request for a certificate to the CA, signing the request with the 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 USIM. Or it is also possible for the CA to generate the new key pair and send it (protected) to the USIM.

Two options can be envisaged. Though the public/private key pair is long lasting, the validity of the subscriber certificates issued to the UE could be short-lived. In this case the long lasting public/private key pair is used for PKI applications (e.g. in mobile-commerce) in combination with the short-lived certificates. Alternatively, the long lasting public/private key pair could come with a long-term certificate. The long-term private key would then have a restricted purpose, e.g. only to be used to authenticate subscriber certificate requests. The latter would be used to obtain another, short-lived certificate on a short-lived public/private key pair. It would then be the short-lived keys that could be used for e.g. m-commerce and other 3G PKI applications.

Annex <X> (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New