3GPP TSG–SA3 Meeting #28
Berlin, Germany, 06-09 May 2003

Tdoc ⌘S3-030253

CR-Form-v7

CHANGE REQUEST

⌘ **ab.cde** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: **0.1.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Bootstrapping of application security using AKA.
Source:	⌘	Alcatel
Work item code:	⌘	Support for Subscriber Certificates
Date:	⌘	30/04/2003
Category:	⌘	**D**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The bootstrapping mechanism is generic and application independent such that multiple applications can benefit from it to bootstrap security. Hence the specification of the bootstrapping mechanism does not belong in the subscriber certificate TS.
Summary of change:	⌘	Have this TS describe the bootstrapping principle and the general architecture in depth and the specific applications such as subscriber certificates only in general. Additionally have a separate document with the detailed specification of protocol B for each application, in particular a separate TS describing protocol B for issuing subscriber certificates.
Consequences if not approved:	⌘	Not a logical structure in case other applications (e.g. related to Presence or MBMS or …) would in the future also use the bootstrapping principle. Either the specification of the general mechanism must then be duplicated in the TS of each application or the other applications must refer to the subscriber certificates document for their authentication bootstrapping which has absolutely nothing to do with subscriber certificates.

Clauses affected:	⌘	

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

Other comments:	⌘	

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

Technical Specification

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

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.

Note: The bootstrapping mechanism is generic and application independent such that multiple applications can benefit from it to bootstrap security. Hence the specification of the general bootstrapping mechanism does not belong in the subscriber certificate TS. Suggestion is that this TS describes the bootstrapping principle and the general architecture in depth independent of the application that will use the bootstrapping service and includes the specific applications such as subscriber certificates only as use cases.

Additionally there should then be a separate document describing the detailed specification of protocol B per individual application e.g. one for issuing subscriber certificates.

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.

.

4.2 Procedures

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. Optionally the NAF can request application specific user profile information.
- The BSF supplies to NAF the requested key material and if necessary the profile information.
- 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.

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 is 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 exists:

- 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

5.2 …

Comment: new sections to be added with other applications using the bootstrapping principle (e.g. MBMS, Presence,…) once this has been or would be agreed.

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

Comment: not 100% clear what is meant to stay in this annex and what is meant as 'discussion topic'. If it would be agreed to have a separate document for the general architecture and bootstrapping mechanism and a separate one per application then most of this Annex can probably be incorporated in the main part of the subscriber certificate document rather than in the Annex.

A.1 Introduction

A.2 ~~Additional requirements and principles~~

Comment: 5.1.2 Requirements and principles, then why a section here with Additional requirements and principles?

A.2.1 Usage of Bootstrapping

Comment: seems to be partially included in sections 1, 4 and 5.1.1.

A.2.2 Access independence

Comment: this is also mentioned in section 5.1.2.1

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

Comment: section numbering, either"B"is the only reference point discussed and then it should be "A.3.3 Reference point B" or a section about another reference point should be added, probably then "A.3.3.2 Reference point D".

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

Comment: suggestion to include subsections A.3.3.1.2.1 and A.3.3.1.2.2 in section "A.4.1. Certificate Issuing"

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

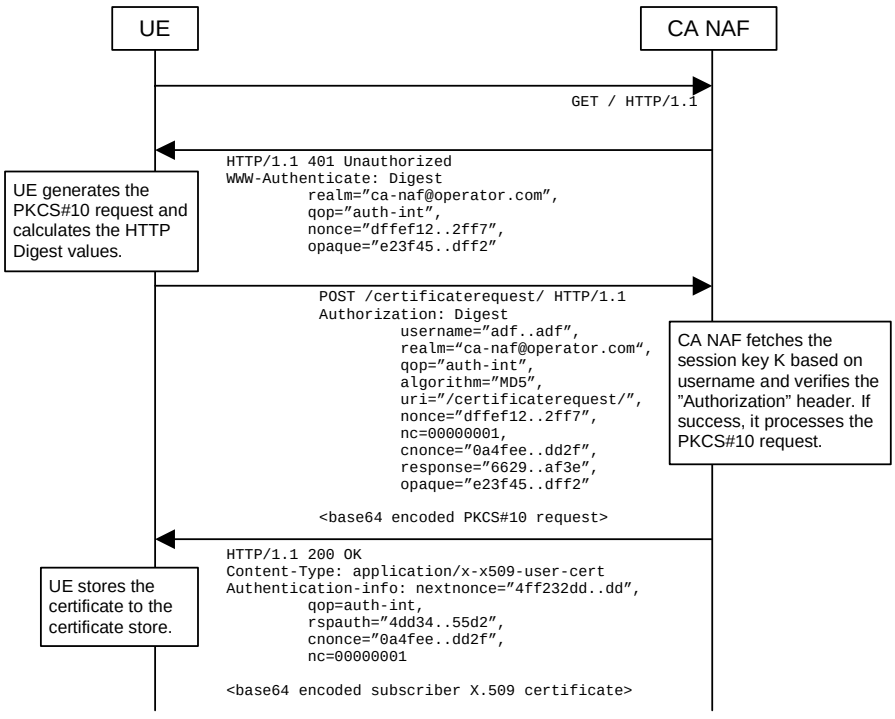

Figure 1: Certificate request using PKCS#10 with HTTP Digest Authentication.

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

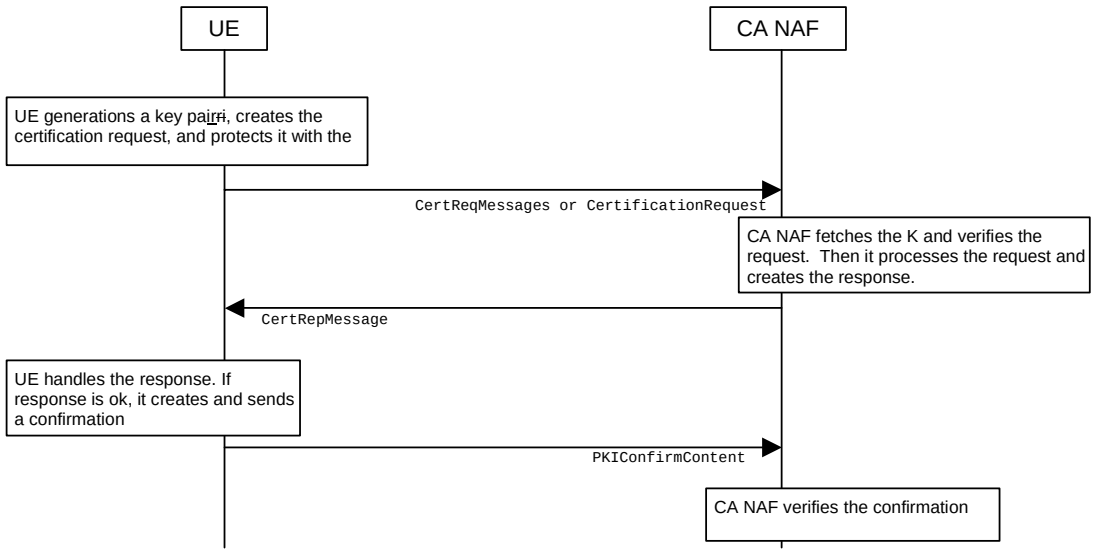

Figure 2: Certificate request using basic authentication scheme of CMP.

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.

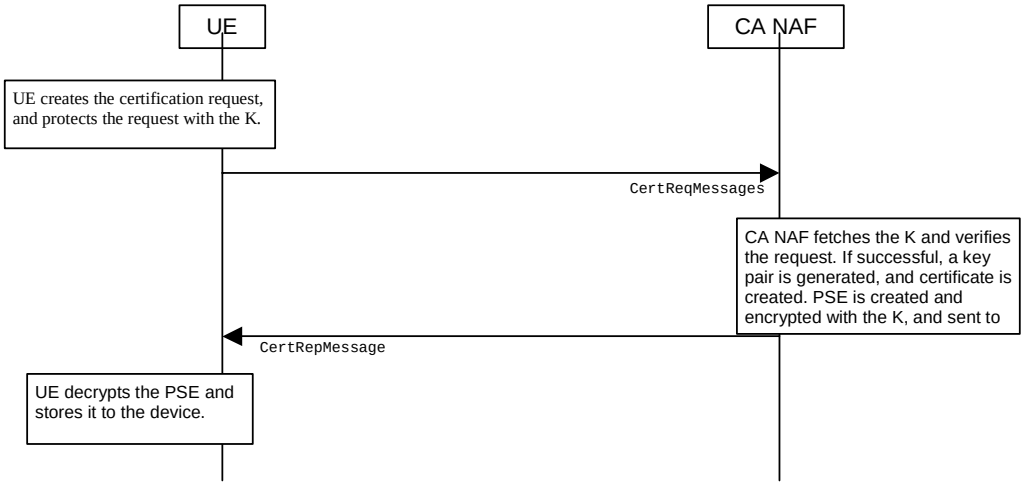

Figure 3: Certificate request using centralized scheme of CMP.

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

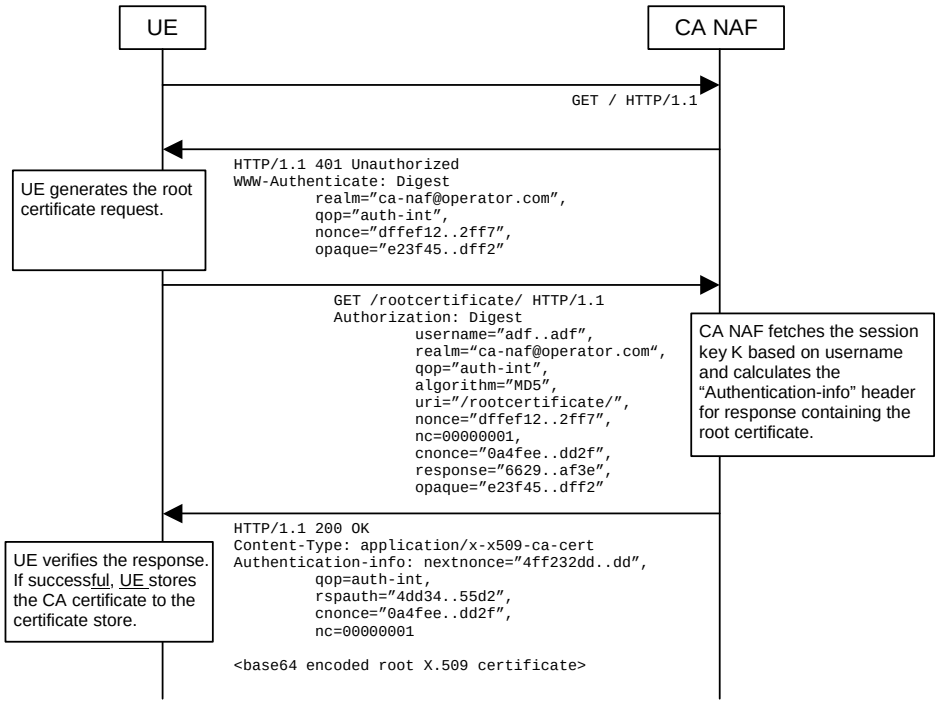

Figure 4: CA certificate delivery using PKCS#10 with HTTP Digest authentication.

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.