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

Tdoc ⌘S3-040506

CR-Form-v7

CHANGE REQUEST

⌘ **33.221** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

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

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Cleanup of procedure descriptions
Source:	⌘	Nokia
Work item code:	⌘	GBA-SSC
Date:	⌘	29/06/2004
Category:	⌘	**F**
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:	⌘	Extra stage 3 level material is removed, and some editorial clarifications are done to the procedure descriptions.
Summary of change:	⌘	The following changes are done: - HTTP Digest usage with GBA description is removed in subclause 4.5.1.2.1, and it refers now to TS 24.109. - procedure descriptions in subclause 4.6 are clarified. - changed “CA NAF” to “PKI portal” - missing abbreviations are added - some of the references in the text contain the name of the spec as well - references to stage 3 level details (TS 24.109) are added - references to RFC 2797, RFC 2510, and RFC 2511 are added - the format of references unified (removed version numbering, and publication dates) - error fix: “application/pkix-path” should be “application/pkix-pkipath”
Consequences if not approved:	⌘	The specification contains stage 3 material, and necessary clarifications on the text is not done.

Clauses affected:	⌘	2, 3.2, 4.5.1.2, 4.5.1.2.1, 4.5.1.2.2, 4.6, 4.6.1, 4.6.2

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

Other comments: ⌘

===== **BEGIN CHANGE** =====

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

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

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

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

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

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

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

[20] 3GPP TS 24.109: "Bootstrapping interface (Ub) and Network application function interface (Ua); Protocol details".

[21] IETF Internet-Draft: "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", May 24, 2004, URL: http://www.ietf.org/internet-drafts/draft-ietf-tls-psk-00.txt

[22] IETF RFC 2797: "Certificate Management Messages over CMS".

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

3.2 Abbreviations

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

AK	Anonymity Key
AKA	Authentication and Key Agreement
B-TID	Bootstrapping Transaction Identifier
blob	Binary Large Object
BSF	Bootstrapping Server Function
CA	Certificate Authority
CMC	Certificate Management Messages over CMS
CMP	Certificate Management Protocols
CMS	Cryptographic Message Syntax
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
HSS	Home Subscriber System
IK	Integrity Key
MNO	Mobile Network Operator
NAF	Network Application Function
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
UE	User Equipment

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

4.5.1.2 Functionality and protocols

4.5.1.2.1 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. This section also needs to be aligned with annex A of the GBA TS.~~

~~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_NAF (base64 encoded) as the password. The session key Ks_NAF is derived from the key material Ks that resulted from bootstrapping procedure over 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~~PKI portal using a HTTP ~~POST~~ request, which shall be authenticated and integrity protected by HTTP Digest Authentication as specified in subclause 5.2 of TS 24.109 [20].

Editor's note: PSK TLS as specified in subclause 5.4 of TS 33.222 [12] is another solution to authenticate and protect the certificate enrolment. It is FFS, whether is should be used instead of HTTP Digest. Also, note that the use of PSK TLS in Release-6 is open in TS 33.222.

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 WPKI [9]. If a certificate chain is returned, then it is "application/pkix-pkipath" as specified in IETF RFC 3546 [15].

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 shall 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.

4.5.1.2.2 Key Generation

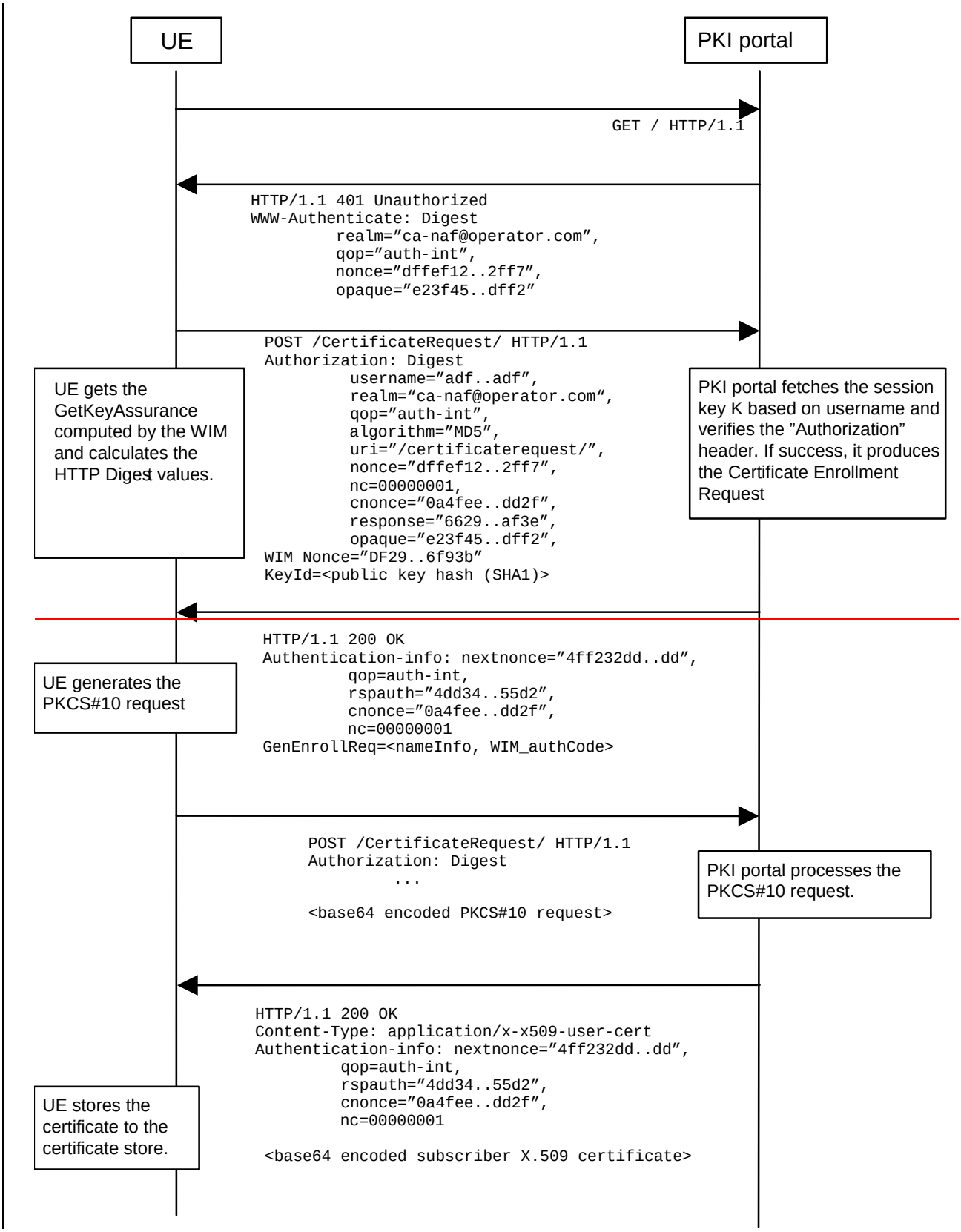
If the private key is stored in a UICC (e.g. in a WIM [8]) and the UICC demands a special authorization (e.g. from the Operator) to generate the key, the ME may need to perform an HTTP ~~POST~~ request, which ~~MAY~~may be authenticated and integrity protected by HTTP Digest Authentication, to the NAF 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. The exact key generation procedure is specified in OMA's "Crypto Object for the ECMAScript Mobile Profile" [14].

~~Editor's note: A reference to the relevant OMA specifications should be added.~~

4.6 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. This section also needs to be aligned with annex A of the GBA TS.~~

4.6.1 Certificate issuing


UE
PKI portal
GET / HTTP/1.1
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Digest
realm="ca-naf@operator.com",
qop="auth-int",
nonce="dffef12..2ff7",
opaque="e23f45..dff2"
POST /CertificateRequest/ HTTP/1.1
Authorization: Digest
username="adf..adf",
realm="ca-naf@operator.com",
qop="auth-int",
algorithm="MD5",
uri="/certificaterequest/",
nonce="dffef12..2ff7",
nc=00000001,
cnonce="0a4fee..dd2f",
response="6629..af3e",
opaque="e23f45..dff2",
WIM Nonce="DF29..6f93b"
KeyId=<public key hash (SHA1)>
UE gets the GetKeyAssurance computed by the WIM and calculates the HTTP Digest values.
PKI portal fetches the session key K based on username and verifies the "Authorization" header. If success, it produces the Certificate Enrollment Request
HTTP/1.1 200 OK
Authentication-info: nextnonce="4ff232dd..dd",
qop=auth-int,
rspauth="4dd34..55d2",
cnonce="0a4fee..dd2f",
nc=00000001
GenEnrollReq=<nameInfo, WIM_authCode>
UE generates the PKCS#10 request
POST /CertificateRequest/ HTTP/1.1
Authorization: Digest
...
<base64 encoded PKCS#10 request>
PKI portal processes the PKCS#10 request.
HTTP/1.1 200 OK
Content-Type: application/x-x509-user-cert
Authentication-info: nextnonce="4ff232dd..dd",
qop=auth-int,
rspauth="4dd34..55d2",
cnonce="0a4fee..dd2f",
nc=00000001
<base64 encoded subscriber X.509 certificate>
UE stores the certificate to the certificate store.

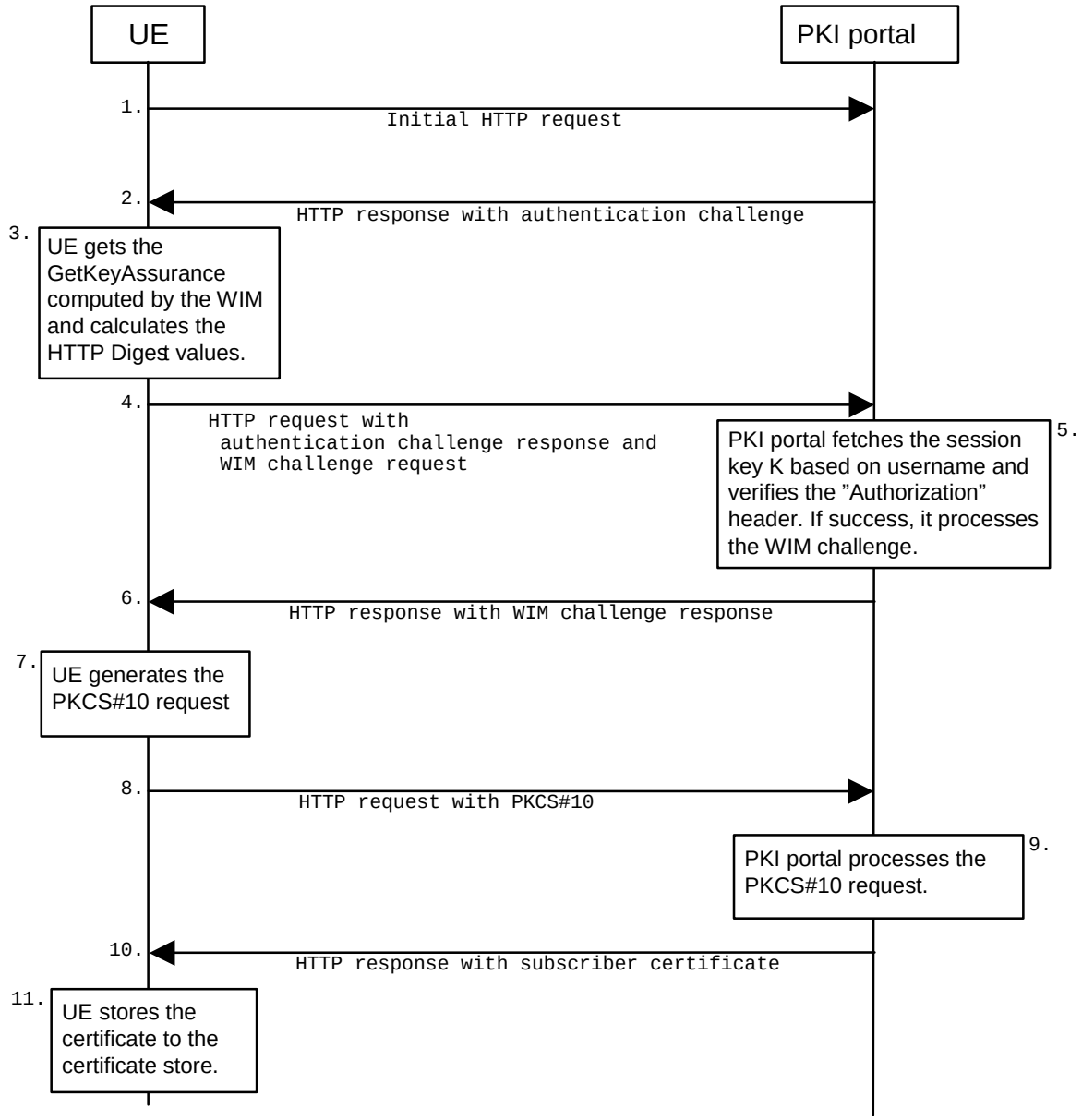


Figure 2: Certificate request using PKCS#10 with HTTP Digest Authentication

The sequence diagram above describes the certificate request when using PKCS#10 with HTTP Digest authentication. The actions involving WIM application in steps 3-6 shall be omitted if there is no WIM application in the UE. The procedure is secured as specified in subclause 5.2 of TS 24.109 [20]. The detailed definition of the messages is left to stage 3 specifications.

1. The sequence starts with the UE sending an empty HTTP request to the PKI portal.

2. The PKI portal responds with HTTP response code 401 "Unauthorized" which contains a WWW-Authenticate header. The header instructs the UE to use HTTP Digest authentication.

3. The UE will generate the HTTP request by calculating the Authorization header values using the bootstrapping ~~T~~transaction ~~i~~identifier (B-TID) it received from the BSF as username and the NAF specific session key Ks_NAF. If the certificate request needs extra assurance by a WIM application for key ~~P~~proof ~~-~~-of ~~-~~-~~O~~origin, the UE generates a WIM challenge request containing parameters needed for key proof-of-origin generation [14].~~should~~

4. The UE sends HTTP request to the PKI portal and includes ~~a~~the WIM ~~Nonce~~challenge request~~and the key id (i.e. SHA-1 public key hash)~~ in this request.

5. When the PKI portal, acting as an NAF, receives the request, it will verify the Authorization header by fetching the NAF specific session key Ks_NAF from the ~~bootstrapping server~~BSF using the ~~identifier~~B-TID, then

calculating the corresponding digest values using Ks_NAF, and finally comparing the calculated values with the received values in the Authorization header. If the verification succeeds and the extra assurance for WIM application is needed, the PKI portal may use the subscriber profile to compute the WIM challenge response [14].~~and~~

6. The PKI portals sends back a ~~GenEnrollReq attribute~~WIM challenge response containing additional parameters that are needed for the following PKCS#10 request generation ~~(e.g. nameInfo, WIM_authCode, ...)~~. The PKI portal may use session key Ks_NAF to integrity protect and authenticate this response.

7. The UE will then generate the PKCS#10 request and send it to the ~~CA NAF~~PKI portal 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. 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]. 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).

8. 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~~PKI portal 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.

9. The incoming PKCS#10 request is taken in for further processing. If the ~~CA NAF~~PKI portal is actually a registration authority (RA ~~NAF~~), the PKCS#10 request is forwarded to CA using any protocol available (e.g., CMC as specified in IETF RFC 2797 [22] or CMP as specified in IETF RFC 2510 [2] and RFC 2511 [3]). After the PKCS#10 request has been processed and a certificate has been created, the new certificate is returned to the ~~CA NAF~~PKI portal. It will generate a HTTP response containing the certificate, or the pointer to the certificate as defined subclause 7.4 of WPKI [9], or a full certificate chain from issued certificate to the root certificate.

10. 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, the CertResponse structure defined in subclause 7.3.5 of the OMA WPKI [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 in PkiPath structure as defined in [15] and it shall be base64 encoded:

```
HTTP/1.1 200 OK
```

Content-Type: application/pkix-pkipath

<base64 encoded PkiPath blob>

The content-type header value for the certificate chain is "application/pkix-pkipath" as specified in [15].

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

11. When UE receives the subscriber certificate or the URL to 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.

4.6.2 CA Certificate delivery

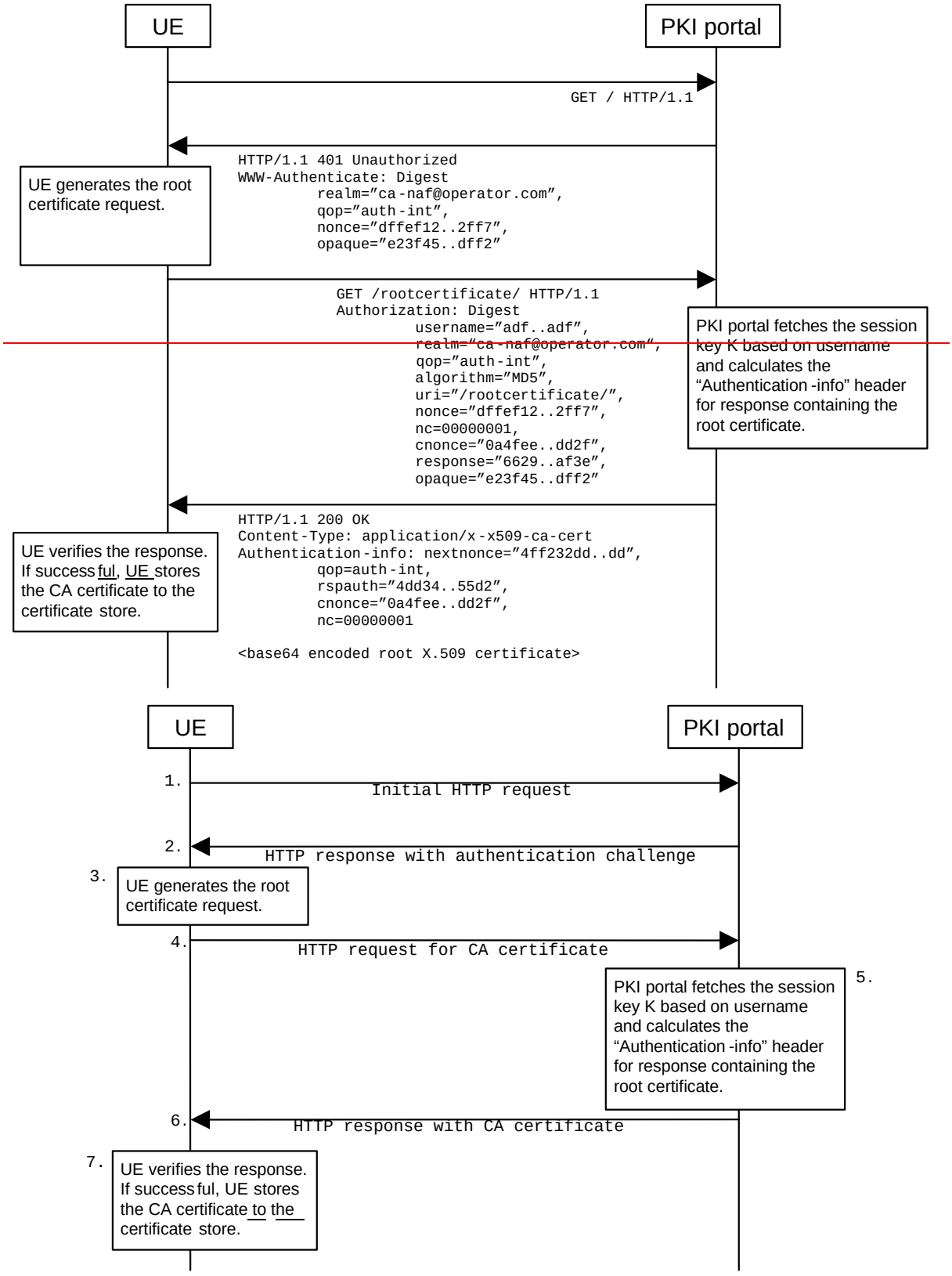


Figure 3: CA certificate delivery with HTTP Digest authentication

The sequence diagram above describes the CA certificate delivery when using HTTP Digest authentication. The procedure is secured as specified in subclause 5.2 of TS 24.109 [20]. The detailed definition of the messages is left to stage 3 specifications.

1. The sequence starts with an empty HTTP request to ~~CA NAF~~the PKI portal.

2. The ~~CA NAF~~PKI portal responds with HTTP response code 401 "Unauthorized" which contains a WWW-Authenticate header. The header instructs the UE to use HTTP Digest for authentication.

3. 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 WPKI [9]. The serial number field shall be omitted. The Authorization header values are calculated using the identifier and the session key Ks_NAF. 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~~PKI portal.~~ A request of subscriber's certificate is specified in subclause 4.4.1.1.~~

4. 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.

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

6. 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-----

7. 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.

===== **END CHANGE** =====