Technical Specification Group Services and System Aspects
Meeting #25, Palm Springs, USA

TSGS#25(04)0620

Source: **SA WG3**

Title: **4 CRs to 33.221: Various changes to Security Certificates (Rel-6)**

Document for: **Approval**

Agenda Item: **7.3.3**

The following CRs were agreed by SA WG3 and are presented to TSG SA for approval.

TSG SA Doc number	Spec	CR	Rev	Phase	Subject	Cat	Version-Current	SA WG3 Doc number	Work item
SP-040620	33.221	001	-	Rel-6	User security settings	D	6.0.0	S3-040502	SEC1-SC
SP-040620	33.221	002	-	Rel-6	Editorial cleanup	D	6.0.0	S3-040505	SEC1-SC
SP-040620	33.221	003	-	Rel-6	Cleanup of procedure descriptions	F	6.0.0	S3-040506	SEC1-SC
SP-040620	33.221	004	-	Rel-6	Removal of unnecessary editor's notes	F	6.0.0	S3-040507	SEC1-SC

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

Tdoc ⌘S3-040502

CR-Form-v7

CHANGE REQUEST

⌘	**33.221**	**CR**	**001**	⌘**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:	⌘	User security settings		
Source:	⌘	SA WG3		
Work item code:	⌘	SEC1-SC	***Date:*** ⌘	29/06/2004
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 term "subscriber profile" is updated to "user security settings" to align the terminology with other 3GPP GAA related specifications.
Summary of change:	⌘	The term "subscriber profile" is updated "user security settings".
Consequences if not approved:	⌘	The term "subscriber profile" is still used in the specification instead of "user security settings".

Clauses affected:	⌘	4.3.2, 4.4, 4.4.4, 4.5.1.1,				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

===== BEGIN CHANGE =====

4.3.2 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 the PKI portal specific user security settings~~subscriber profile information~~ (i.e. whether subscriber is able to enrol a certain types of subscriber certificate).

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

4.4 Requirements and principles for issuing subscriber certificates

The following prerequisites for issuing of subscriber certificates exist:

- the UE and the mobile operator's PKI portal share key material to support the certificate request and operator CA certificate retrieval;
- the issuing of the requested certificate is allowed according to ~~the~~ subscriber's ~~profile~~PKI portal specific user security setting. The PKI portal is responsible for performing this check before issuing the subscriber certificate;
- in the case that the private key is stored on a WIM [8], which is 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.

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

4.4.4 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~~GBA user security settings. For each type of subscriber certificate, i.e. for different keyUsage in WAP Certificate and CRL Profile, subscriber's ~~profile~~PKI portal specific user security setting 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.

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

4.4.8 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's ~~profile~~PKI portal specific user security setting to check the certification policies. This means that the Zn interface TS 33.220 [11] shall support for retrieving a subset of the ~~subscriber profile~~GBA user security settings;
- 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.

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

4.5.1.1 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.

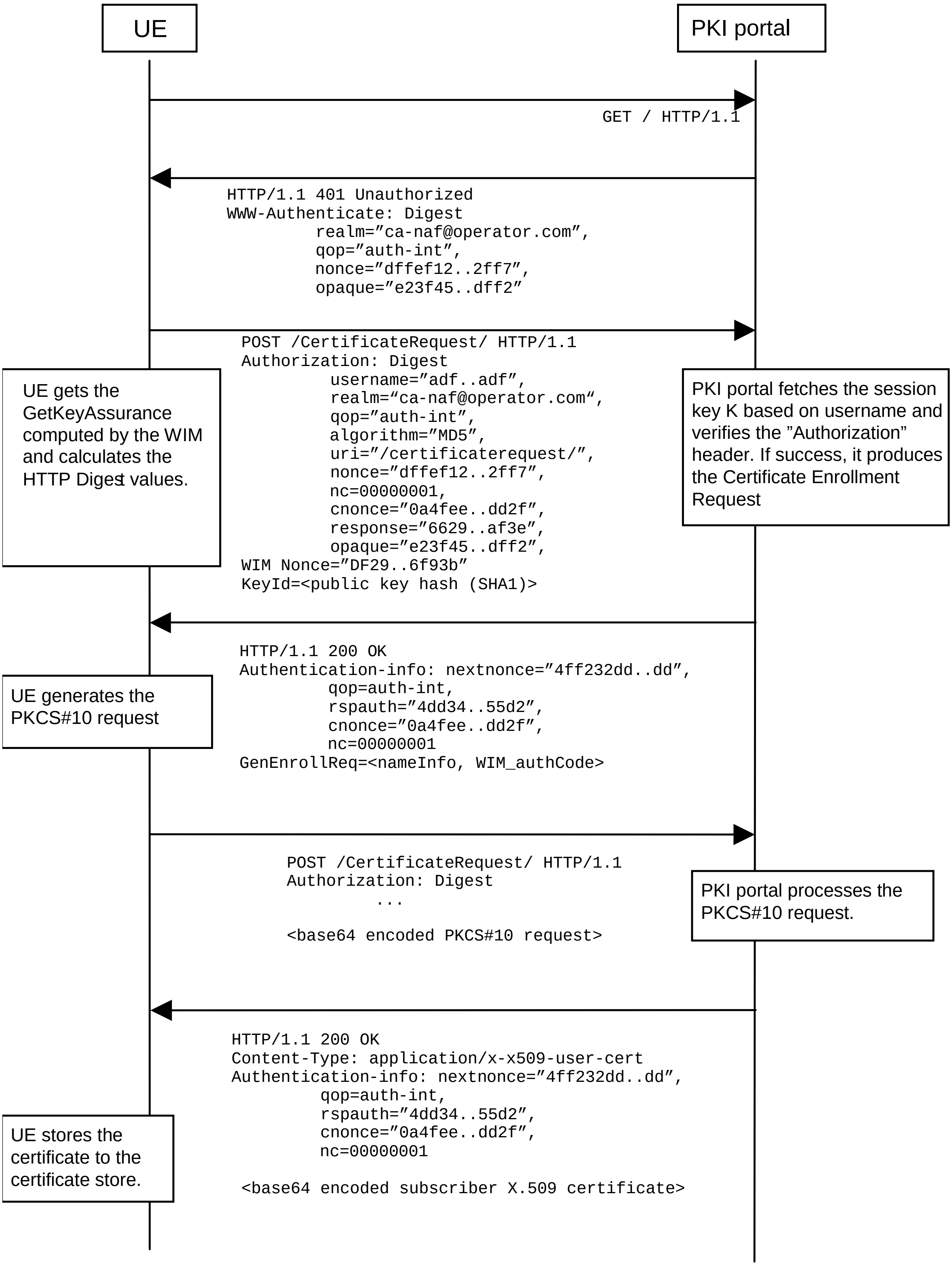
During subscriber certificate issuing, UE may request a certification of a public key. The supported request format shall be PKCS#10. It is used to encapsulate the public key and other attributes (i.e., subject name, intended key usage, etc.). The request is transported from the UE to the PKI Portal over Ua interface. Upon receiving the certification request, the PKI portal will certify the public key according to its own certification practice policies and subscriber's ~~profile~~PKI portal specific user security setting 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 according to the GBA in TS 33.220 [11], where the PKI portal acts as a Network Application Function (NAF).

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

4.6.1 Certificate issuing



```
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. The sequence starts with an empty HTTP request to PKI portal. 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.

The UE will generate the HTTP request by calculating the Authorization header values using the Transaction Identifier it received from the BSF as username and the session key Ks_NAF. 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 PKI portal, acting as an NAF, receives the request, it will verify the Authorization header by fetching the session key Ks_NAF from the bootstrapping server using the identifier, 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, the PKI portal may use the ~~subscriber profile~~PKI portal specific user security setting 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 PKI portal may use session key Ks_NAF 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. 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). 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, 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-path

<base64 encoded PkiPath blob>
```

The content-type header value for the certificate chain is "application/pkix-path" 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.

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.

===== END CHANGE =====

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

Tdoc* ⌘*S3-040505

CR-Form-v7

CHANGE REQUEST

⌘	**33.221**	**CR**	**002**	⌘**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:	⌘	Editorial cleanup		
Source:	⌘	SA WG3		
Work item code:	⌘	SEC1-SC	***Date:*** ⌘	29/06/2004
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: ⌘ Cleanup is done to improve readability, and synchronize the notation style compared to other specifications (such as TS 33.220).

Summary of change: ⌘ The following changes are done:
- the name of the specification is added to reference number in the text to improve readability
- renamed “interfaces” to “reference points”
- the format of references unified (removed version numbering, and publication dates)

Consequences if not approved: ⌘ Clarifications on the text is not done.

Clauses affected: ⌘ 2, 4.2, 4.3.2, 4.3.3, 4.4.3, 4.4.6, 4.4.7, 4.4.8, 4.5.1, 4.5.1.1, 4.7.1, 4.7.2

		Y	**N**		
Other specs affected:	⌘		**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] IETF RFC 2510~~Adams C., Farrell S.~~: "Internet X.509 Public Key Infrastructure Certificate Management Protocols"~~, RFC 2510, March 1999~~.

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

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

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

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

[7] OMA: “WAP Certificate and CRL Profiles”.~~WAP-211-WAPCert, 22.5.2001: http://www1.wapforum.org/tech/terms.asp?doc=WAP-211-WAPCert-20010522-a.pdf~~

[8] OMA: “Wireless Identity Module; Part: Security”.~~WAP-260-WIM-20010712, 12.7.2001: http://www1.wapforum.org/tech/documents/WAP-260-WIM-20010712-a.pdf~~

[9] OMA: “Wireless Application Profile; Public Key Infrastructure Definition”.~~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] OMA: "Crypto Object for the ECMAScript Mobile Profile".~~Open Mobile Alliance ECMA Crypto Library http://www.openmobilealliance.org.~~

[15] IETF RFC 3546~~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] IETF RFC 3039~~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~~.

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

4.2 Reference model

Figure 1 shows a simple network model of the entities involved in the certificate issuing, and the ~~interfaces~~reference points used between the network entities.

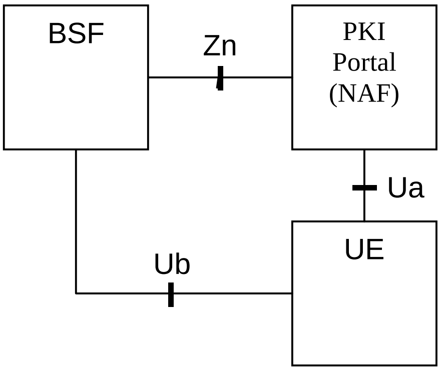


Figure 1: Simple network model for certificate issuing

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

4.3.2 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).

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

4.3.3 User Equipment

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

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

4.4.6 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 IETF RFC 3280 [6] and ITU-T X.509 [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.

~~IETF's and ETSI's~~ Qualified certificate profiles by IETF [17]~~,~~ and ETSI [18] may also be used as the subscriber certificate profile if the certification practices followed by the certificate issuing operator fulfil all of the requirements stated in [16,17,18].

The following certificate extensions may 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.

4.4.7 Service Discovery

To enable the certificate enrollment procedure, the addresses of bootstrapping server and PKI portal should be configured to the UE. The BSF discovery method is specified in TS 33.220 [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 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 OMA's "Provisioning Content Version 1.1" [19].

4.4.8 Requirements on reference point Ua ~~interface~~

The requirements for reference point 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 reference point Zn ~~interface~~ TS 33.220 [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.

4.5 Certificate issuing architecture

4.5.1 Reference point Ua ~~interface~~

4.5.1.1 General description

In the certificate issuing, reference point 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 format shall be 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 reference point Ua ~~interface~~. Upon receiving the certification request, the 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 reference point 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 reference point Ua ~~interface~~ are based on the BSF generated shared secret according to the GBA in TS 33.220 [11], where the PKI portal acts as a Network Application Function (NAF).

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

4.7.1 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 WPKI [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 OMA's WIM [8], WPKI [9], and ECMA script [14] specifications).

4.7.2 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 OMA's WIM [8], WPKI [9], and ECMA script [14] specifications).

NOTE: The pre-shared symmetric key discussed in this chapter is not the same as the shared key associated with GBA.

===== END CHANGE =====

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

Tdoc ⌘S3-040506

CR-Form-v7

CHANGE REQUEST

⌘	**33.221**	**CR 003**	⌘**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:	⌘	SA WG3		
Work item code:	⌘	SEC1-SC	***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				
		Y	N			
Other specs affected:	⌘		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

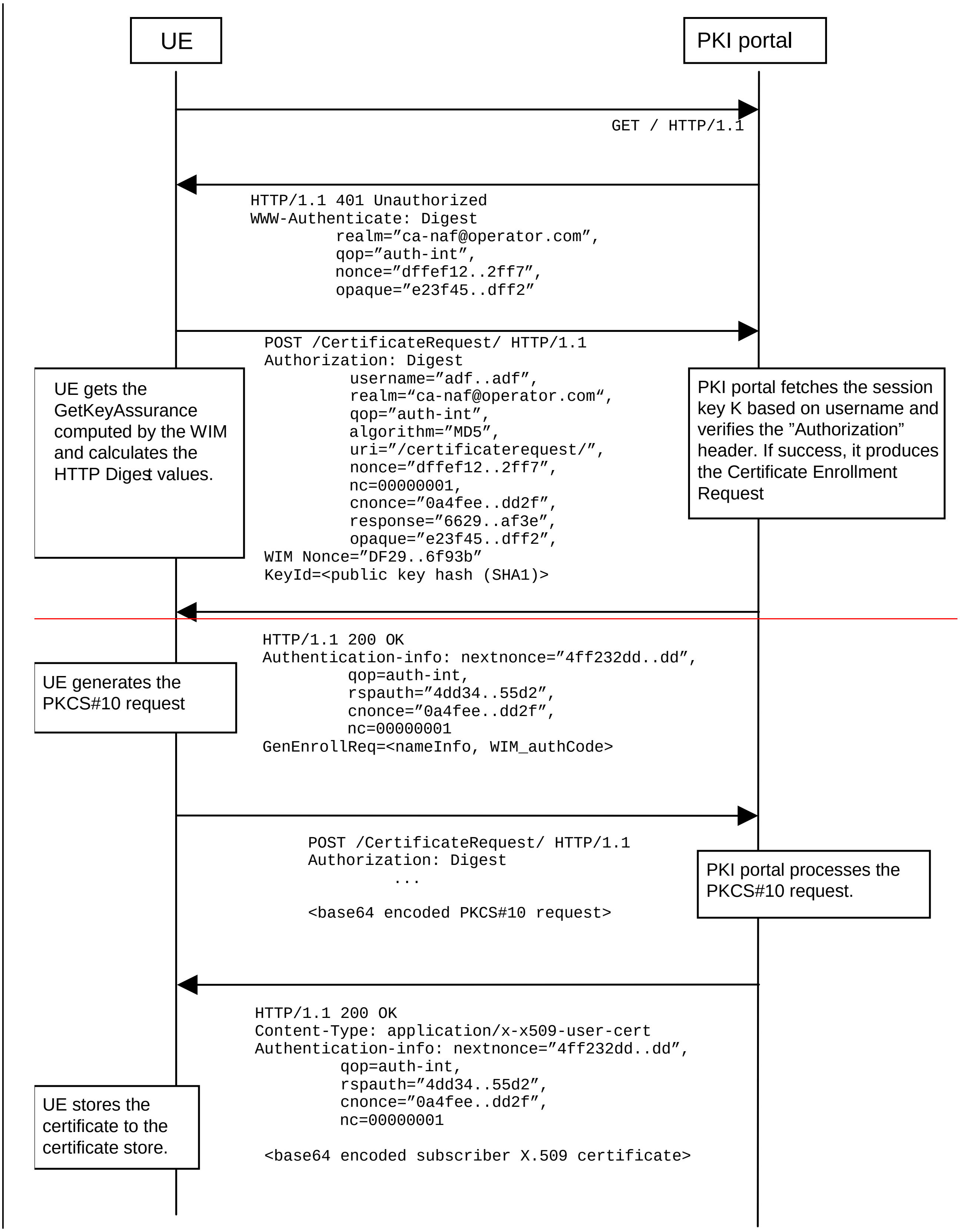
If the private key is stored in a UICC (e.g. in a WIM [8]) and the UICC demands a special authorization (e.g. from the Operator) to generate the key, the ME may need to perform an HTTP ~~POST~~ request, which ~~MAY~~may be authenticated and integrity protected by HTTP Digest Authentication, to the NAF 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



```
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.

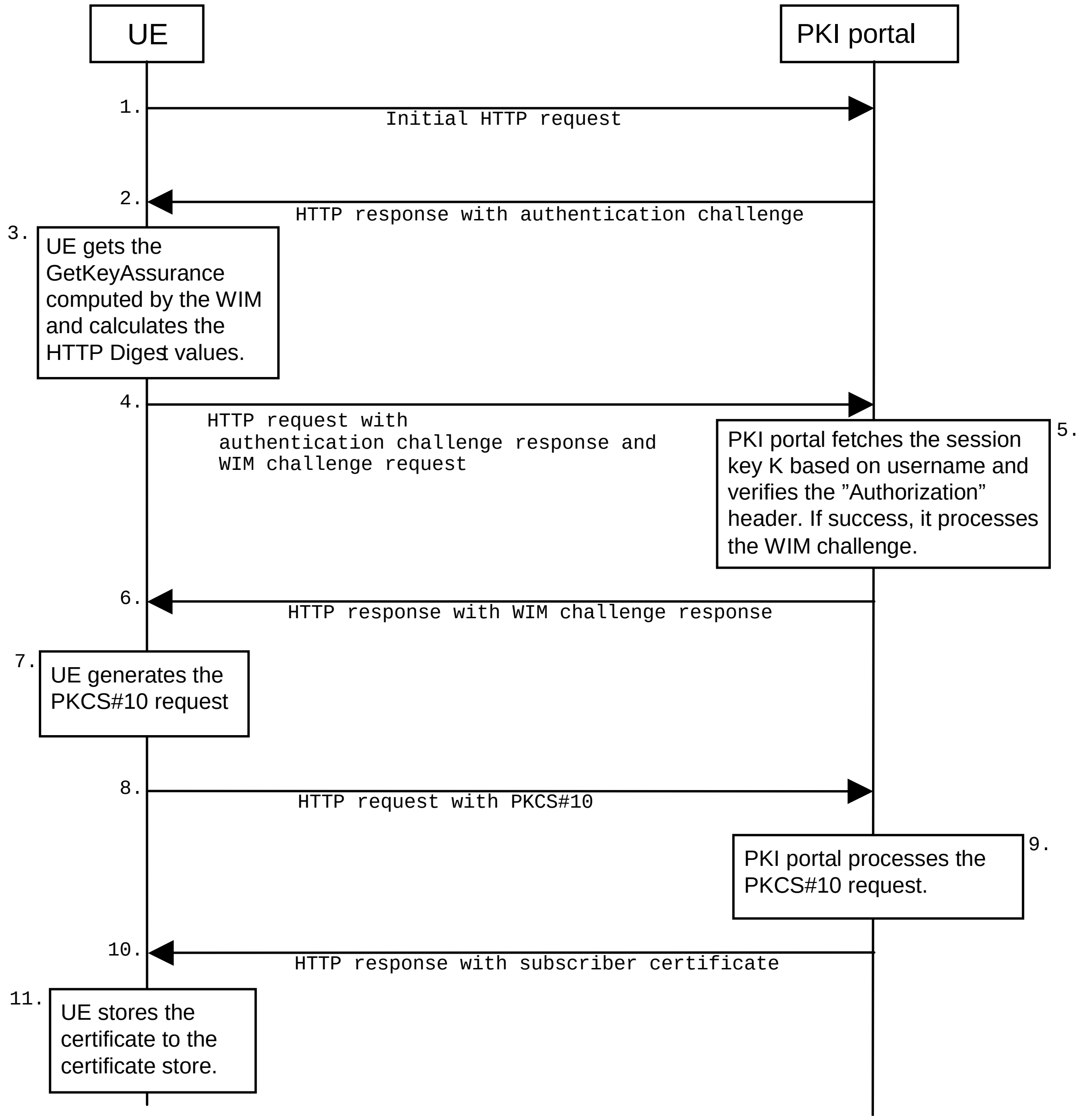

UE
PKI portal
1.
Initial HTTP request
2.
HTTP response with authentication challenge
3.
UE gets the GetKeyAssurance computed by the WIM and calculates the HTTP Digest values.
4.
HTTP request with authentication challenge response and WIM challenge request
5.
PKI portal fetches the session key K based on username and verifies the "Authorization" header. If success, it processes the WIM challenge.
6.
HTTP response with WIM challenge response
7.
UE generates the PKCS#10 request
8.
HTTP request with PKCS#10
9.
PKI portal processes the PKCS#10 request.
10.
HTTP response with subscriber certificate
11.
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>

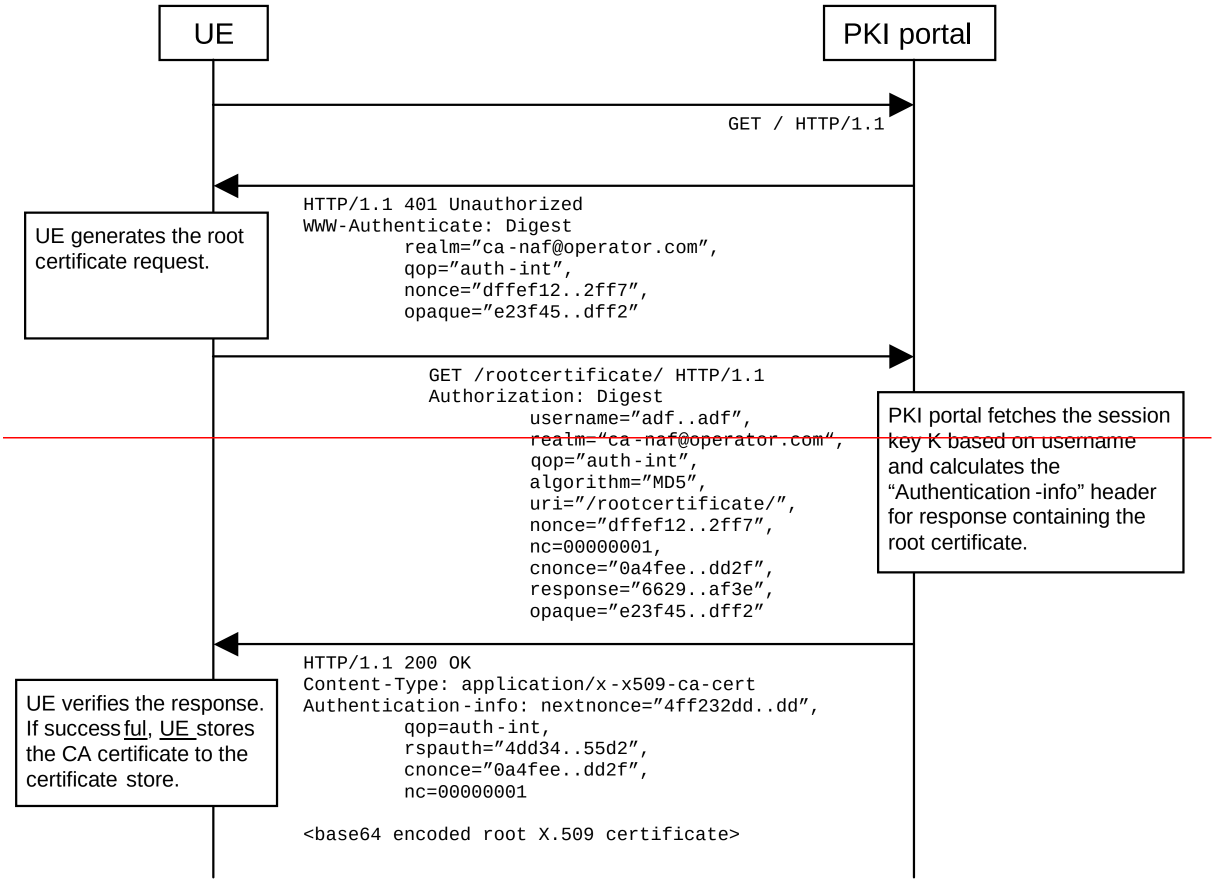
The content-type header value for the certificate chain is "application/pkix-pkipath" as specified in [15].

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


UE
PKI portal
UE generates the root certificate request.
PKI portal fetches the session key K based on username and calculates the "Authentication-info" header for response containing the root certificate.
UE verifies the response. If successful, UE stores the CA certificate to the certificate store.

```
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"
```

```
GET /rootcertificate/ HTTP/1.1
Authorization: Digest
         username="adf..adf",
         realm="ca-naf@operator.com",
         qop="auth-int",
         algorithm="MD5",
         uri="/rootcertificate/",
         nonce="dffef12..2ff7",
         nc=00000001,
         cnonce="0a4fee..dd2f",
         response="6629..af3e",
         opaque="e23f45..dff2"
```

```
HTTP/1.1 200 OK
Content-Type: application/x-x509-ca-cert
Authentication-info: nextnonce="4ff232dd..dd",
         qop=auth-int,
         rspauth="4dd34..55d2",
         cnonce="0a4fee..dd2f",
         nc=00000001

<base64 encoded root X.509 certificate>
```

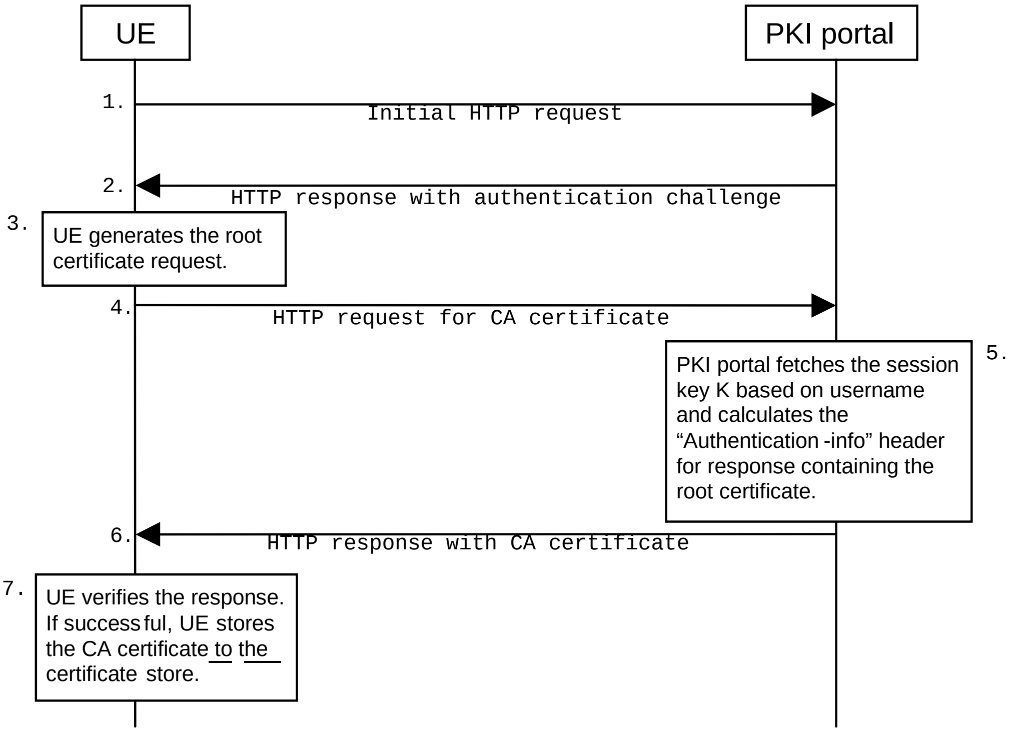

UE
PKI portal
1.
Initial HTTP request
2.
HTTP response with authentication challenge
3.
UE generates the root certificate request.
4.
HTTP request for CA certificate
5.
PKI portal fetches the session key K based on username and calculates the "Authentication-info" header for response containing the root certificate.
6.
HTTP response with CA certificate
7.
UE verifies the response. If successful, UE stores the CA certificate to the certificate store.

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 =====

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

Tdoc ⌘S3-040507

CR-Form-v7

CHANGE REQUEST

⌘ **33.221 CR 004** ⌘**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:	⌘	Removal of unnecessary editor's notes
Source:	⌘	SA WG3
Work item code:	⌘	SEC1-SC
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: ⌘ Editor's notes that are not needed or are unnecessary are removed or changed.

Summary of change: ⌘ Reason for removal:
4.4.4 - 1st editor's note: text is added to the proceeding paragraph reflecting the content of the editor's note (editor's note deleted)
4.4.4 - 2nd editor's note: there are no phases any more because NAF can be in visited network in release 6 (cf. TS 33.220) (editor's note modified)
4.4.5 - The charging mechanism does not have to addressed in this specification (editor's note deleted)
4.4.7 - The more flexible solutions are already specified below the editor's note (editor's note deleted)
4.7 - The material has been added thus this editor's note is obsolete (editor's note deleted)

Consequences if not approved: ⌘ Unnecessary editor's note are deleted.

Clauses affected: ⌘ 4.4.4, 4.4.5, 4.4.7, 4.7

Other specs affected: ⌘

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

Other comments: ⌘

===== BEGIN CHANGE =====

4.4.4 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 key ~~U~~usage in WAP Certificate and CRL Profile [7], subscriber profile shall contain a flag that allows or disallows the issuing of that type of certificate to subscriber. According to WAP Certificate and CRL Profile [7], there are two types of certificates for users (i.e., subscribers): user certificates for authentication and user certificates for digital signatures (i.e., non-repudiation).

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

4.4.5 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.~~

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

4.4.7 Service Discovery

To enable the certificate enrollment procedure, the addresses of bootstrapping server and PKI portal should be configured to the UE. The BSF discovery method is specified in TS 33.220 [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 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 [19].

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

4.7 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.~~

4.7.1 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]).

4.7.2 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.

===== END CHANGE =====