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

Tdoc ⌘S3-040502

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: ⌘	User security settings			
Source: ⌘	Nokia, Siemens			
Work item code: ⌘	GBA-SSC		***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.

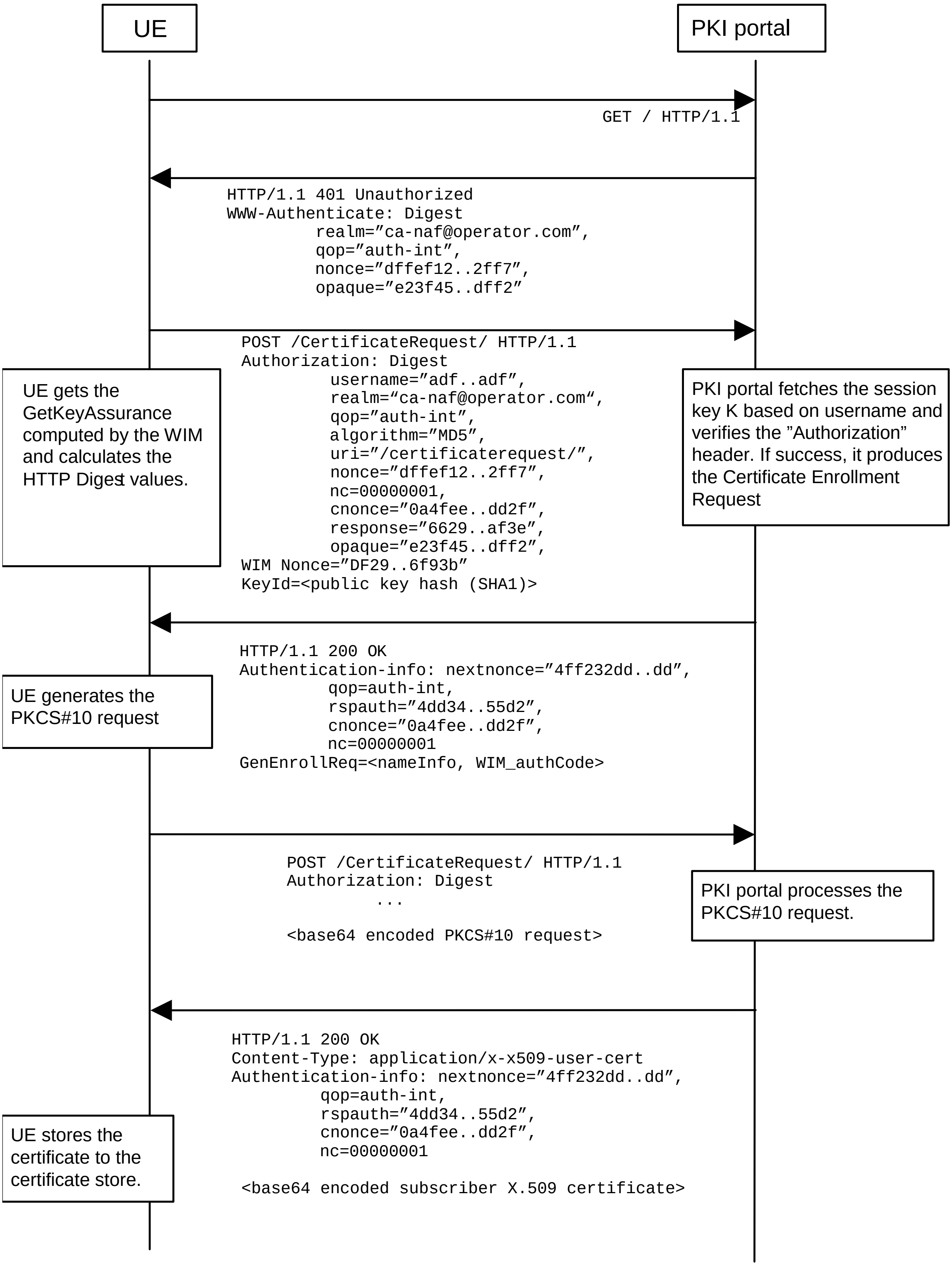
During subscriber certificate issuing, UE may request a certification of a public key. The supported request format shall be PKCS#10. It is used to encapsulate the public key and other attributes (i.e., subject name, intended key usage, etc.). The request is transported from the UE to the PKI Portal 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 =====