3GPP TSG-SA WG3 Meeting #36
Shenzhen, China, November 23-26, 2004

Tdoc ⌘S3-040979

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.221** **CR** **006** ⌘ **rev** **-** ⌘ Current version: **6.1.0** ⌘

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

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

Title:	⌘	Editorial correction
Source:	⌘	Nokia
Work item code:	⌘	SEC1-SC
Date:	⌘	16/11/2004
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:
Ph2 *(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)*
Rel-7 *(Release 7)*

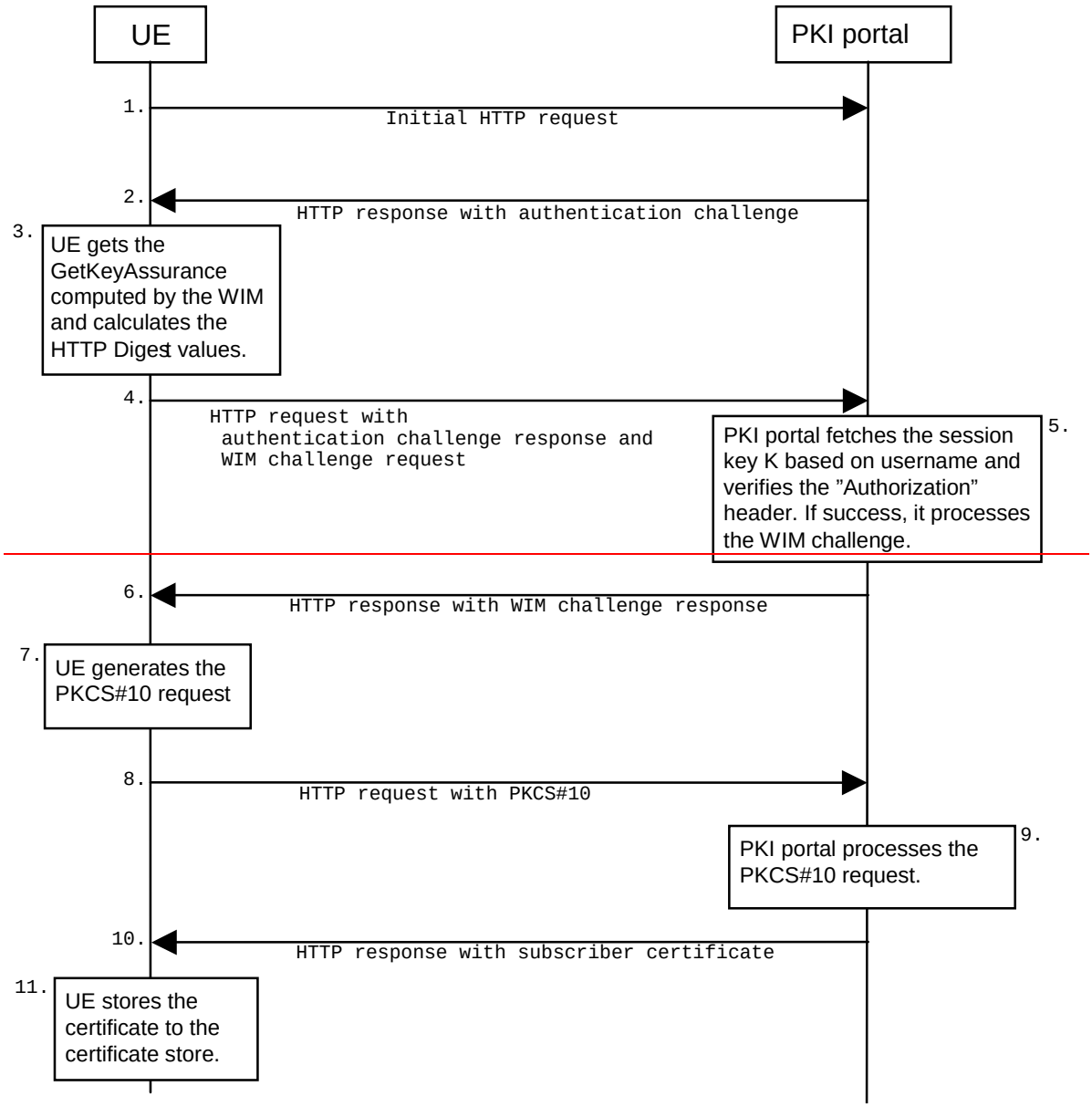
Reason for change:	⌘	Figures 2 and 3 talk about "session key K" when "session key Ks_NAF" is meant.
Summary of change:	⌘	"K" is deleted from the figures.
Consequences if not approved:	⌘	

Clauses affected:	⌘	4.6.1, 4.6.2

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

Other comments: ⌘

4.6.1 Certificate issuing



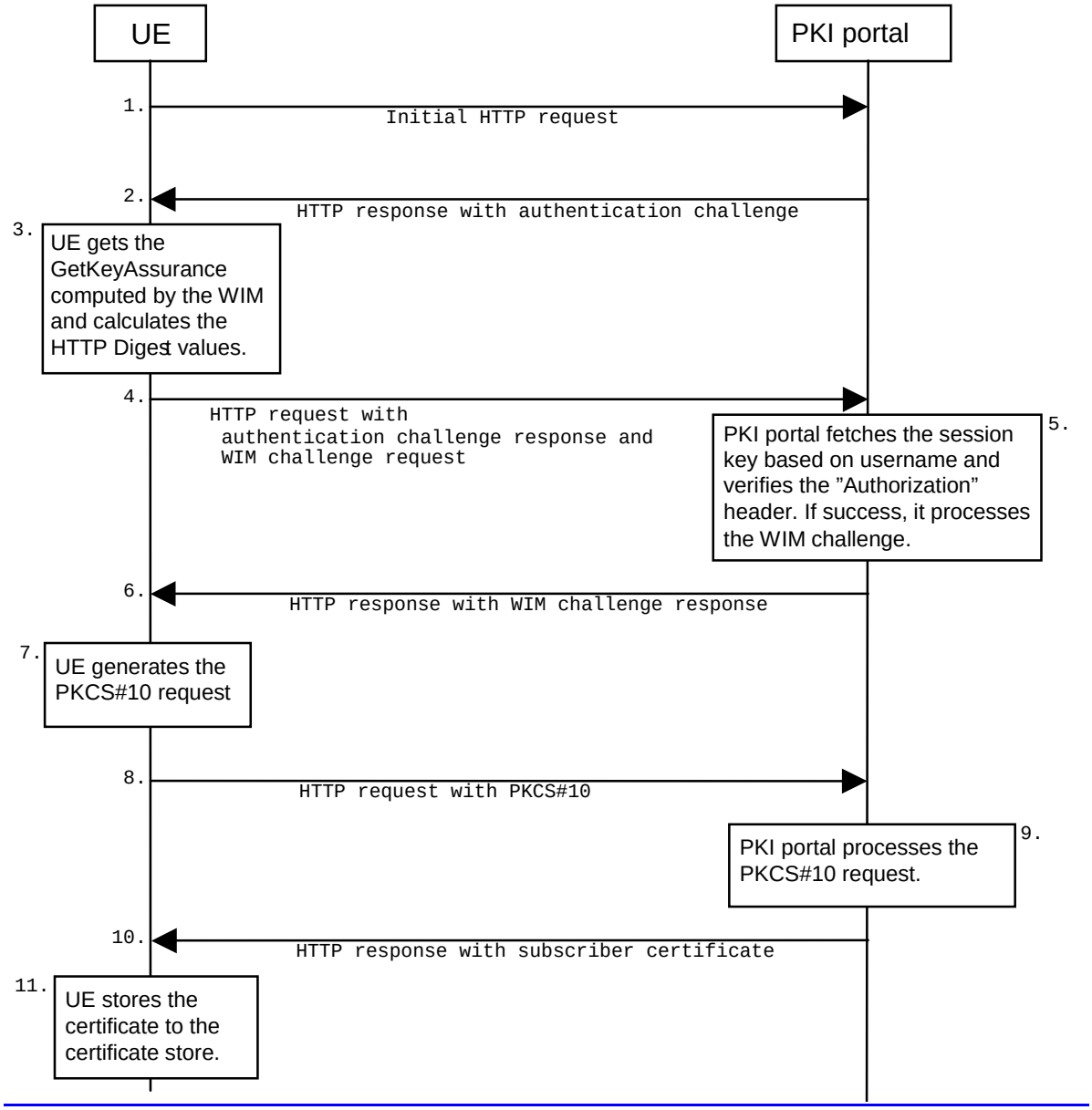


Figure 2: Certificate request using PKCS#10 with HTTP Digest Authentication

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 clause 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 transaction 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 proof-of-origin, the UE generates a WIM challenge request containing parameters needed for key proof-of-origin generation [14].

4. The UE sends HTTP request to the PKI portal and includes the WIM challenge request 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 BSF using the 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 PKI portal specific user security setting to compute the WIM challenge response [14].

6. The PKI portals send back a WIM challenge response containing additional parameters that are needed for the following PKCS#10 request generation. 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 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 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 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 PKI portal is actually a registration authority (RA), 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 IETF RFC 2511 [3]). After the PKCS#10 request has been processed and a certificate has been created, the new certificate is returned to the PKI portal. It will generate a HTTP response containing the certificate, or the pointer to the certificate as defined clause 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

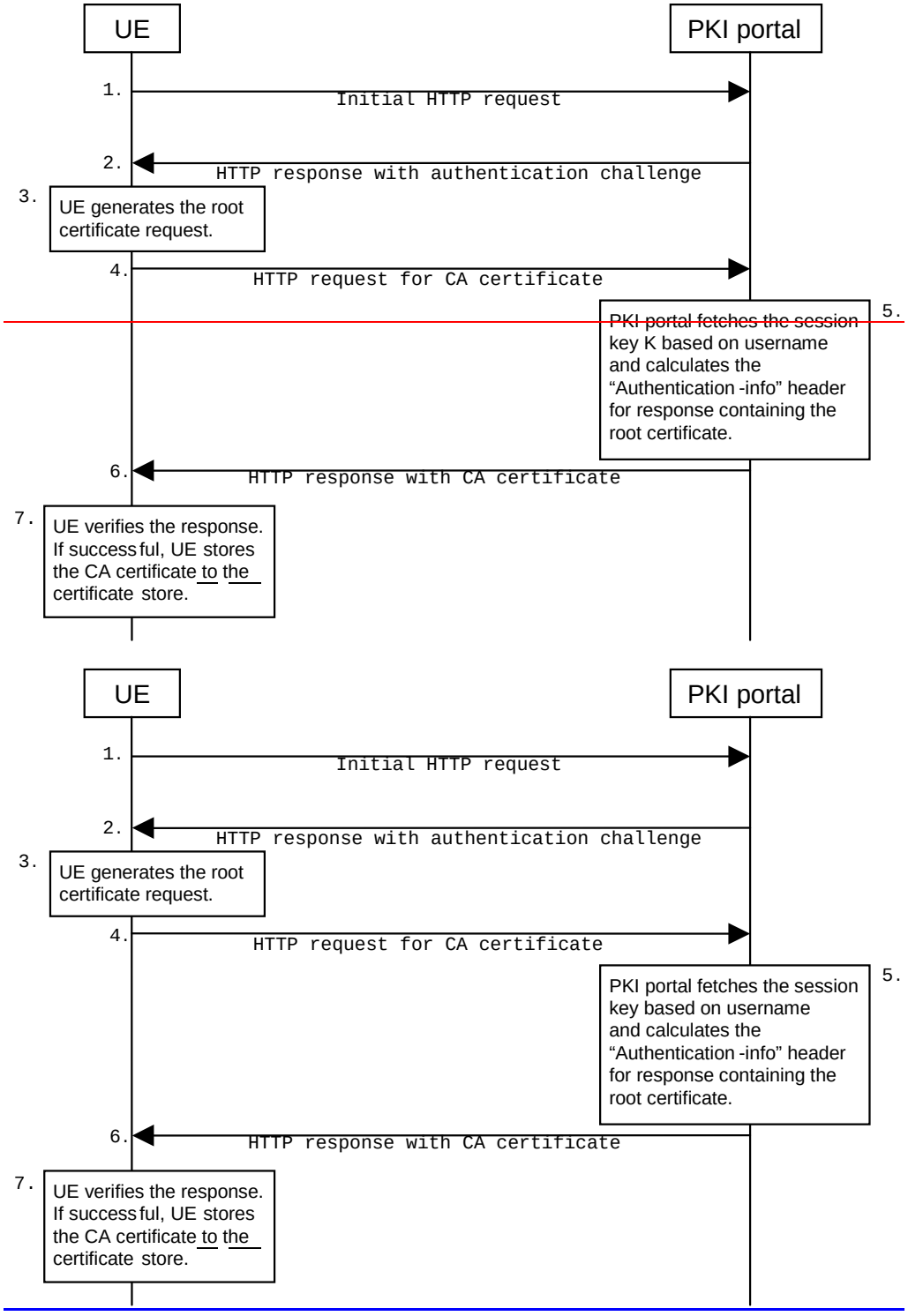


Figure 3: CA certificate delivery with HTTP Digest authentication

The sequence diagram above describes the CA certificate delivery when using HTTP Digest authentication. The procedure is secured as specified in clause 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 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 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 PKI portal.

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 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. 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.