3GPP TSG SA WG3 Security — S3#31 **S3-03684**
18th – 21th November, 2003, Munich, Germany

CR-Form-v7

CHANGE REQUEST

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

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

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

Title:	⌘	PSEUDO CR on enrollment of keys in a UICC application
Source:	⌘	Schlumberger, OCS, Gemplus
Work item code:	⌘	SSC
Date:	⌘	3/11/2003
Category:	⌘	**B**
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:	⌘	Mobile operators may implement a UICC application (e.g. WIM), which may be capable of providing a "Proof of key origin". This means that the UICC application can issue an assertion that the private keys are stored in a tamper resistant device. The assertion includes the public key and information that the key was generated on-board or injected into the device. The assertion is signed by pre-certified key in theUICC, which has a device certificate that identifies the device unique id (e.g. ICCID) and the device manufacturer. This assertion can be added in the PKCS#10 certificate request as defined in OMA [14]. The CA may consider this assertion to determine the CA policies (CPS) that are attributed to the delivered certificate. This may have an impact on the privileges that are attributed to the certificate and whether it is longed lived or short lived. Mobile operators may implement a WIM on the UICC. These operators may not allow enrollment for certificates of keys on this device unless it is triggered by an authorized entity (e.g. operator remote server or authorized PKI server). The authorization takes the form of an end-to-end challenge response between the UICC application and the authorized entity. This CR also describes the additional data and procedures that are needed in order to enable enrollment for certificates for keys in a UICC application in the GBA architecture.
Summary of change:	⌘	Addition of procedure to enable "proof of origin" mechanism in Ua interface.
Consequences if not approved:	⌘	"Proof of origin" will not be allowed in the Ua interface

Clauses affected:	⌘	

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

***** Begin of Change ****

4.1 Requirements and principles for issuing subscriber certificates

The following prerequisites for issuing of subscriber certificates exits:

- The shared key material is available for the UE application, which does the certificate request and operator CA certificate retrieval.
- The issuing of requested certificate is allowed according to subscriber profile. NAF is responsible for performing this check before issuing the subscriber certificate.
- In the case that the private key is stored in the UICC (e.g. in a WIM) being 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.

***** Next Change ****

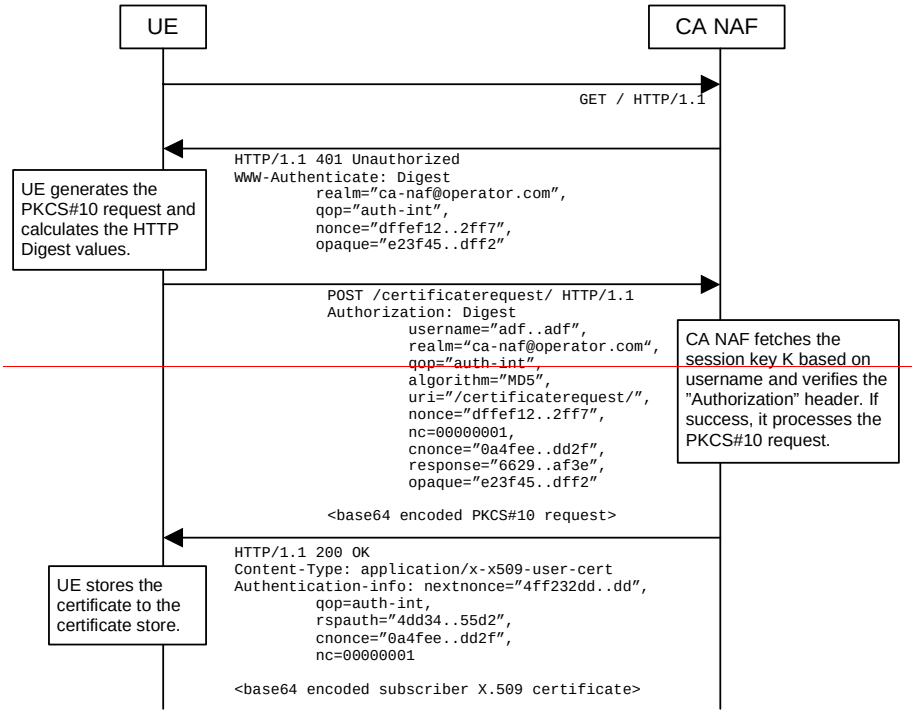
4.2 Certificate issuing procedure

4.4.1 Certificate issuing

Editor's note: From five alternatives investigated in S3-030073 and S3-030036, only the following two have been agreed to add to the present document as potentialsolutions.

document as potential solutions.

4.4.1.1 Certificate issuing using PKCS#10 with HTTP Digest Authentication



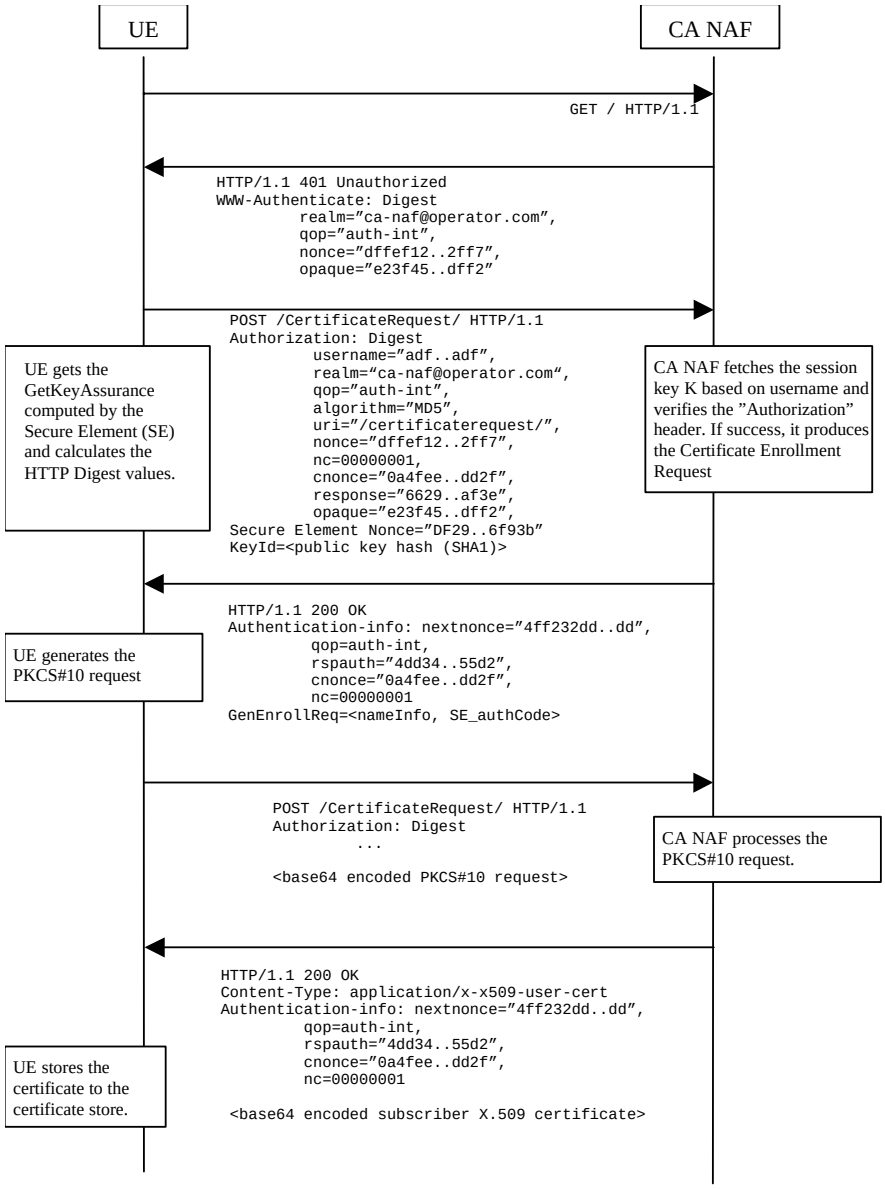


Figure 1: Certificate request using PKCS#10 with HTTP Digest Authentication.

The sequence diagram above describes the certificate request when using PKCS#10 with HTTP Digest. The sequence starts with an empty HTTP request to CA NAF. The CA NAF responds with HTTP response code 401 "Unauthorized" which contains a WWW-Authenticate header. The header instructs the UE to use HTTP Digest authentication.

The UE ~~generates a PKCS#10 request with the subject name, public key, additional attributes and extensions. Then it~~ will generate the HTTP request by calculating the Authorization header values using the identifier it received from the BSF as username and the session key K. If the certificate request needs extra assurance by a UICC application (e.g. WIM) for key Proof of Origin, the UE should include a secure element Nonce and the key id (i.e. SHA1 public key hash) in this request.

When CA NAF receives the request, it will verify the Authorization header by fetching the session key K from the bootstrapping server using the identifier, then calculating the corresponding digest values using K, and finally comparing the calculated values with the received values in the Authorization header. If the verification succeeds, the CA NAF may use the subscriber profile 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 CA NAF may use session key K 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 UICC application (e.g. WIM) the ME should request the AssuranceInfo from the Secure Element UICC and include it in the PKCS#10 request, if provided (see annex Y for all details). The AssuranceInfo provides a proof of origin for the key processing.(e.g. identifies the UICC application and provides a proof that the key is stored in it). If the CA NAF is actually a registration authority (RA NAF), the PKCS#10 request is forwarded to CA using any protocol available (e.g., CMC or CMP). After the PKCS#10 request has been processed and a certificate has been created, the new certificate is returned to the CA NAF. It will generate a HTTP response containing the certificate. The CA NAF may use session key K to integrity protect and authenticate the response.

When UE receives the subscriber certificate, it is stored to local certificate management system.

NOTE: On board key generation is already defined in the WIM specification [8] issued by Open Mobile Alliance (OMA) group."

4.4.1.2 Certificate issuing with CMP

CMP defines two methods to do the certificate issuing: basic authenticated scheme and centralized scheme. In the basic authenticated scheme the key generation happens in the UE while in the centralized scheme the key generation is done in the CA (or RA). CMP states that the support for the basic authenticated scheme for certificate issuing is mandatory for CAs while the support for the centralized scheme is optional. See more details in chapters 2.2 and B8 of [2].

The messages can be transported using various methods such as file based protocol, (such files can be used to transport PKI messages e.g. using FTP, HTTP, email etc.), direct TCP-based management protocol, management protocol via e-mail, and management protocol via HTTP mentioned in section 5 of [2].

4.4.1.2.1 Basic authenticated scheme

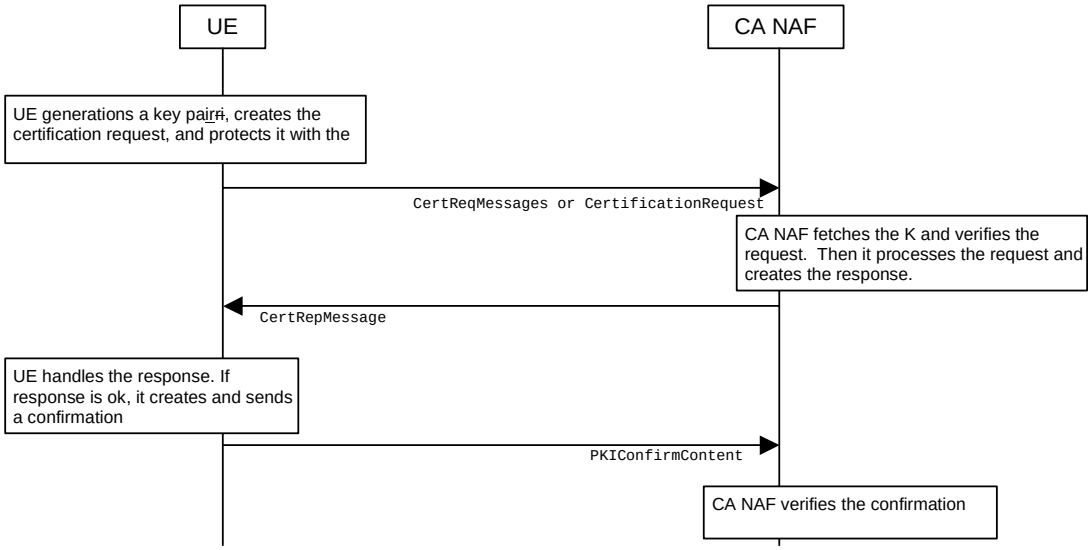


Figure 2: Certificate request using basic authentication scheme of CMP.

The sequence diagram above describes the certificate request and delivery procedure when using CMP and basic authenticated scheme [2]. The sequence starts with UE generating a key pair, creating the certificate request message format (CRMF) message, inserting it to CertReqMessages message, and integrity protecting this message with the initial authentication key (IAK). The session key K, which has been derived earlier using Ub interface, can be used as IAK.

The certificate request message is sent to CA NAF who fetches the corresponding K based on the identifier received in the request. CA NAF verifies the request with the K. If the verification succeeds, the CA NAF processes the request, i.e. generates and signs the certificate and sends the certification response to the UE.

UE verifies the certificate response message with the K. If the message verification is successful, the issued certificate is stored to the device, and UE sends a confirmation message to the CA NAF.

CA NAF verifies the confirmation message. If the verification fails or CA NAF never receives the confirmation message, CA NAF must revoke the newly issued certificate if it has been already published.

If the certificate request needs extra assurance for key Proof of Origin, or if the key generation in a UICC application needs a special authorization from the NAF (e.g. Operator authorization), additional messages may be needed to allow the UE to include a secure element Nonce and key id (i.e. SHA1 public key hash) for authorization and key Proof of Origin delivery.

***** Next Change ****

2 References

[...]

[14] Open Mobile Alliance ECMA Crypto Library http://www.openmobilealliance.org

NEXT CHANGE*****

Annex <Y>:
Enrolment request that includes AssuranceInfo from the Secure Element

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].

END OF CHANGES****