3GPP TSG SA WG3 Security — S3#31 **S3-03685**
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⌘ ☒ ME ☒ Radio Access Network □ Core Network □

Title:	⌘	PSEUDO CR on on-board key generation in a UICC.			
Source:	⌘	Schlumberger, OCS, Gemplus			
Work item code:	⌘	SSC	***Date:***	⌘	3/11/2003
Category:	⌘	**B**	***Release:***	⌘	Rel-6

Use one of the following categories:	*Use one of the following releases:*
F *(correction)*	*2 (GSM Phase 2)*
A *(corresponds to a correction in an earlier release)*	*R96 (Release 1996)*
B *(addition of feature),*	*R97 (Release 1997)*
C *(functional modification of feature)*	*R98 (Release 1998)*
D *(editorial modification)*	*R99 (Release 1999)*
Detailed explanations of the above categories can	*Rel-4 (Release 4)*
be found in 3GPP TR 21.900.	*Rel-5 (Release 5)*
	Rel-6 (Release 6)

Reason for change:	⌘	Mobile operators may implement a UICC application dealing with on-board key generation (e.g. WIM). These operators may not allow on-board key generation 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 and the authorized entity. This CR describes the procedures that are needed in order to enable on-board key generation in the UICC in the GBA architecture.
Summary of change:	⌘	Description of procedure to enable authorization for key generation in a UICC application.
Consequences if not approved:	⌘	Authorization for on-board key generation will not be allowed in the Ua interface.

Clauses affected:	⌘	4.3.3.1.2.1				
		Y	**N**			
Other specs affected:	⌘		**N**	Other core specifications	⌘	
			N	Test specifications		
			N	O&M Specifications		
Other comments:	⌘					

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

4.3.3.1.2.1 PKCS#10 with HTTP Digest Authentication

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 K (base64 encoded) as the password. The session key K is has been previously derived from the key material Ks that resulted from using 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 using a HTTP POST request, which MUST be authenticated and integrity protected by HTTP Digest Authentication.

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 is either “application/x-x509-user-cert” or “application/vnd.wap.cert-response” as specified in [9].

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 MUST 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.

Key Generation

If the private key is stored in a UICC (e.g.in a WIM) and the UICC demands a special authorization (e.g. from the Operator) to generate the key, the ME may need to peroform an HTTP POST request, which 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.

***** End of Change ****