3GPP TSG-SA WG3 Meeting #33
10th – 14th May 2004, Beijing, China

Tdoc ⌘S3-040333

CR-Form-v7

CHANGE REQUEST

⌘ **33.220** **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:	⌘	Removal of Annex A
Source:	⌘	Siemens
Work item code:	⌘	SSC-GBA
Date:	⌘	10/05/2004
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 informative Annex A gives an example for a realisation of the Ua interface, which was probably useful at the time of writing. Now TSs 33.222, and 33.141 give this kind of information. Additionally, to get an impression of the information content and flow of the messages involved, stage 3 documents TSs 24.109 and 29.109 may be more helpful to the reader.
Summary of change:	⌘	Removal of Annex A
Consequences if not approved:	⌘	Duplication of material which is standardised and more up-to-date elsewhere.

Clauses affected:	⌘	Annex A

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

⌘

Other comments:	⌘	

********** begin change **********

~~Annex A (informative):~~
~~Generic secure message exchange using HTTP Digest Authentication~~

~~A.1 Introduction~~

~~This annex describes how HTTP Digest Authentication can be used between UE and any NAF where the protocol over Ua interface is based on HTTP messaging.~~

~~HTTP Digest Authentication can also be used as a generic authentication and integrity protection method towards any new NAF The Generic Bootstrapping Architecture specified in this document enables the NAF and the UE to mutually authenticate each other and integrity protect any payload being transferred between NAF and UE. As a generic method, it will speed up the specification of new NAFs since the authentication and message integrity protection part of Ua interface are taken care of by HTTP Digest Authentication. It will also ease the implementation of GBA based authentication in NAFs because there would be one well defined way to do it.~~

~~A.2 Generic protocol over Ua interface description~~

~~Editor's note: a cross check with the corresponding stage 3 spec TS 24.cde shall be performed in order to avoid duplication.~~

~~The sequence diagram in Figure A.1 describes the generic secure message exchange with HTTP Digest Authentication. The conversation may take place inside a server authenticated TLS (RFC 2246 [6]) tunnel in which case TLS handshake has taken place before step 1.~~

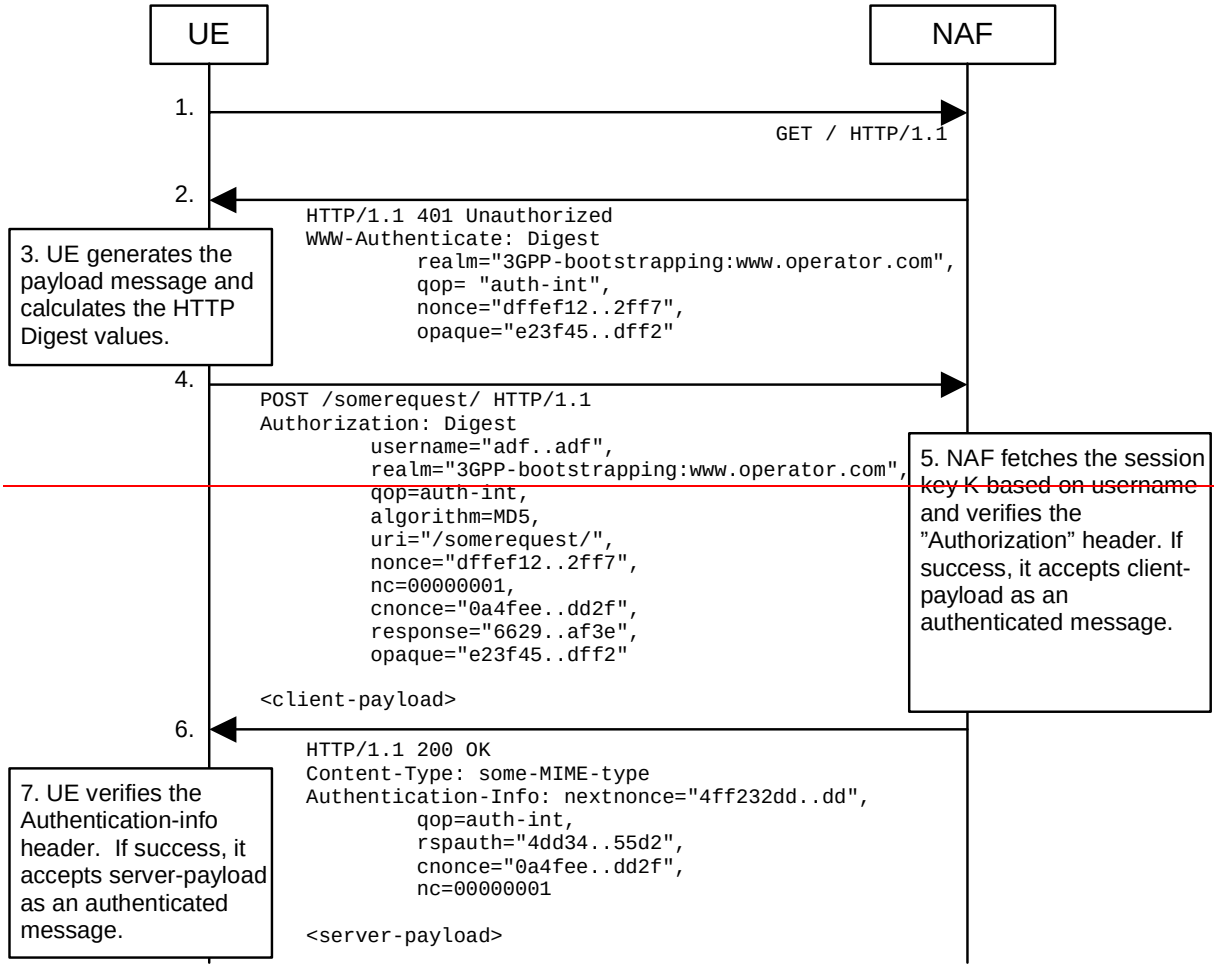
~~In step 1, UE sends an empty HTTP request to a NAF. In step 2, NAF responds with HTTP response code 401 "Unauthorized" which contains a WWW Authenticate header. The header instructs the UE to use HTTP Digest Authentication with a bootstrapped security association. Quality of protection (qop) attribute is set to "auth int" meaning that the payload of the following HTTP requests and responses should integrity protected. The realm attribute contains two parts. The first part is a constant string "3GPP bootstrapping" instructing the UE to use a bootstrapped security association. The second part is the DNS name of the NAF.~~

~~In step 3, the UE shall verify that the second part of the realm attribute does in fact correspond to the server it is talking to. In particular, if the conversation is taking place inside a server authenticated TLS tunnel, the UE shall verify that the server name in the server's TLS certificate matches the server name in the realm attribute of the WWW Authenticate header. The UE generates client payload containing the message it wants to send to the server. Then it 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 as the password, and send the request to NAF in step 4.~~

~~When NAF receives the request in step 5, it will verify the Authorization header by fetching the session key Ks_NAF from the bootstrapping server using Zn interface and the Transaction Identifier. After successful retrieval, NAF calculates the corresponding digest values using K, and compares the calculated values with the received values in the Authorization header. The NAF shall also verify that the DNS name in the realm attribute matches its own. If the conversation is taking place inside a server authenticated TLS tunnel, the NAF shall also verify that this DNS name is the same as that of the TLS server. If the verification succeeds, the incoming client payload request is taken in for further processing. Thereafter, the NAF will generate a HTTP response containing the server payload it wants to send back to the client in step 6. The NAF may use session key Ks_NAF to integrity protect and authenticate the response.~~

~~In step 7, UE receives the response and verifies the Authentication Info header. If the verification succeeds, the UE can accept the server payload for further processing.~~

~~Additional messages can be exchanged using steps 3 through 7 as many times as is necessary. The following HTTP request and responses shall be constructed according to RFC 261 [3] (e.g., nc parameter shall be incremented by one with each new HTTP request made by UE).~~



~~**Figure A.1: Generic secure message exchange using HTTP Digest Authentication and bootstrapped security association**~~

********** end change **********