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

Tdoc ⌘S3-040547

CR-Form-v7

CHANGE REQUEST

⌘ **33.222 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: ⌘ Editorial change to section 5.3

Source: ⌘ Vodafone

Work item code: ⌘ TBA ***Date:*** ⌘ 28/06/2004

Category: ⌘ **F** ***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 meaning of the last sentence in section 5.3 is unclear.

Summary of change: ⌘ Editorial change to improve clarity of last sentence in section 5.3.

Consequences if not approved: ⌘ Lack of clarity in the specification.

Clauses affected: ⌘ 5.3

Other specs affected: ⌘

Y	N		
	N	Other core specifications	⌘
	N	Test specifications	
	N	O&M Specifications	

Other comments: ⌘

5.3 Shared key-based UE authentication with certificate-based NAF authentication

The authentication mechanism described in this section is mandatory to implement in UE and NAF.

This section explains how the procedures specified in TS 33.220 [3] have to be enhanced when HTTPS is used between a UE and a NAF. The following gives the complementary description with respect to the procedure specified in clause 4.5.3 of TS 33.220 [3], This document specifies the logical information carried in some header fields. The exact definition of header fields is left to stage 3 specifications.

1) When the UE starts communication via Ua reference point with the NAF, it shall establish a TLS tunnel with the NAF. The NAF is authenticated to the UE by means of a public key certificate. The UE shall verify that the server certificate corresponds to the FQDN of the NAF it established the tunnel with. No client authentication is performed as part of TLS (no client certificate necessary).

2) In response to the HTTPS (HTTP over TLS) request received from UE over the Ua reference point, the NAF shall invoke HTTP digest as specified in RFC 2617 [10] with the UE in order to perform client authentication using the shared key as specified in section 4.5.3 of TS 33.220 [3]. The realm attribute of the WWW-Authenticate header field shall contain the constant string "3GPP-bootstrapping" and the FQDN of the NAF, to indicate the GBA as the required authentication method.

3) On receipt of the response from the NAF, the UE shall verify that the FQDN in the realm attribute corresponds to the FQDN of the NAF it established the TLS connection with. On failure the UE shall terminate the TLS connection with the NAF.

4) In the following request to NAF the UE sends a response with an Authorization header field where Digest is inserted using the B-TID as username and the session key Ks_NAF as password.

5) On receipt of this request the NAF shall verify the value of the password attribute by means of the Ks_NAF retrieved from BSF over Zn using the B-TID received as user name attribute in the query.

6) After the completion of step 5), UE and NAF are mutually authenticated as the TLS tunnel endpoints.

NOTE: RFC 2617 [10] mandates in section 3.3 that all further HTTP requests to the same realm must contain the Authorization request header field, otherwise the server has to send a new "401 Unauthorized" with a new WWW-Authenticate header. In principle it is not necessary to send an Authorization header in each new HTTP request for security reasons as long as the TLS tunnel exists, but this would not conform to RFC 2617 [10].

In addition, there may be problems with the lifetime of a TLS session, as the TLS session may time-out at unpredictable (at least for the UE) times, so any request sent by UE can be the first request inside a newly established TLS tunnel requiring the NAF to re-check user credentials.