

## CHANGE REQUEST

33.222 CR 018 rev 1 Current version: 6.3.0

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

<b>Title:</b>	Clarify the GBA requirements for https supporting applications at Ua reference point		
<b>Source:</b>	Gemplus, Axalto, OCS		
<b>Work item code:</b>	GBA-SSC	<b>Date:</b>	16/02/2005
<b>Category:</b>	<b>F</b>	<b>Release:</b>	Rel-6
	<i>Use one of the following categories:</i> <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		<i>Use one of the following releases:</i> <b>Ph2</b> (GSM Phase 2) <b>R96</b> (Release 1996) <b>R97</b> (Release 1997) <b>R98</b> (Release 1998) <b>R99</b> (Release 1999) <b>Rel-4</b> (Release 4) <b>Rel-5</b> (Release 5) <b>Rel-6</b> (Release 6) <b>Rel-7</b> (Release 7)

<b>Reason for change:</b>	TS 33.222 reads the following in the "Requirements on the UE" section: <i>"To utilise GBA as described in this document the UE shall be equipped with a HTTPS capable client (e.g. browser) implementing the particular features of GBA as specified in TS 33.220 [3]"</i>  Additionally, TS 33.220 reads like this: <i>"A GBA-aware ME shall support both GBA_U, as specified in clause 5.2.1 and GBA_ME procedures, as specified in clause 4.5"</i>  Therefore, the reference to the GBA_ME specific procedures in TS 33.222 is inconsistent with these requirements and may be misleading. It should be possible to benefit from GBA_U security advantages to secure the access to services over HTTP.
<b>Summary of change:</b>	- Correct the references to TS 33.220 in section 5.3. - Clarify that GBA_U NAF-specific keys could also be used for TS 33.222 authentication schemes.
<b>Consequences if not approved:</b>	Inconsistency in TS 33.222. Incomplete references to TS 33.220

<b>Clauses affected:</b>	5.3, 5.4										
<b>Other specs affected:</b>	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;">X</td> </tr> </table> Other core specifications Test specifications O&M Specifications	Y	N	X	X	X	X	X	X		
Y	N										
X	X										
X	X										
X	X										
<b>Other comments:</b>											

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

## 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 [and 5.3.3](#) of TS 33.220 [3]. [For the purposes of this document Ks\\_\(ext\) NAF refers to the key shared between the UE and a NAF. In the case of GBA U, Ks\\_\(ext\) NAF refers to Ks\\_ext NAF, and in the case of GBA ME, Ks\\_\(ext\) NAF refers to Ks NAF.](#) 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) The UE sends an HTTP request to the NAF inside the TLS tunnel (HTTPS, i.e. HTTP over TLS). The UE shall indicate to the NAF that GBA-based authentication is supported by adding a constant string "3gpp-gba" to the "User-Agent" HTTP header as a product token as specified in IETF RFC 2616 [12]. The UE shall send the hostname of the NAF in "Host" HTTP header.

NOTE 1: The ability to send the hostname of the NAF is particularly necessary if a NAF can be addressed using different hostnames, and the NAF cannot otherwise discover what is the hostname that the UE used to contact the NAF. The hostname is needed by the BSF during key derivation.

- 3) In response to the HTTP 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 [and 5.3.3](#) 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.
- 4) 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.
- 5) 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 [NAF-specific key \(e.g. ~~session key~~ Ks\\_\(ext\) NAF\)](#) as password.
- 6) On receipt of this request the NAF shall verify the value of the password attribute by means of the [NAF-specific key ~~Ks\\_NAF~~](#) retrieved from BSF over Zn using the B-TID received as user name attribute in the query.
- 7) After the completion of step 6), UE and NAF are mutually authenticated as the TLS tunnel endpoints.

NOTE 2: 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.

It shall be possible for the AP/AS to request a re-authentication of an active UE, see TS 33.220 [11], clauses [4.5.3 and 5.3.3](#).

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

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

## 5.4 Shared key-based mutual authentication between UE and NAF

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

**Editor's note:** If the "Pre-Shared Key Ciphersuites for TLS" Internet Draft [15] does not reach the RFC status by the time when Release 6 is frozen, this subclause shall be removed and the support for the Pre-Shared Key TLS is postponed to Release 7.

The HTTP client and server may authenticate each other based on the shared key generated during the bootstrapping procedure. The shared key shall be used as a master key to generate TLS session keys, and also be used as the proof of secret key possession as part of the authentication function. The exact procedure is specified in Pre-Shared Key Ciphersuites for Transport Layer Security (TLS) [15].

**Editor's note:** The exact procedure of "Pre-Shared Key Ciphersuites for TLS" is under inspection in IETF. When the procedure is ready in IETF, the description how it is used in GAA should be added to TS 24.109, and this subclause should refer to it. The following gives general guidelines for how the TLS handshake may be accomplished using a GBA-based shared secret. The exact definitions of the message fields are left to the stage 3 specifications.

This section explains how a GBA-based shared secret that is established between the UE and the BSF as specified in TS 33.220 [3] is used with Pre-Shared Key (PSK) Ciphersuites for TLS as specified in IETF Internet-Draft [15].

1. When an UE contacts a NAF, it may indicate to the NAF that it supports PSK-based TLS by adding one or more PSK-based ciphersuites to the ClientHello message. The UE shall include ciphersuites other than PSK-based ciphersuites in the ClientHello message. The UE shall send the hostname of the NAF using the server\_name extension to the ClientHello message as specified in IETF RFC 3546 [8].

NOTE 1: The ability to send the hostname of the NAF is particularly necessary if a NAF can be addressed using different hostnames, and the NAF cannot otherwise discover what is the hostname that the UE used to contact the NAF. The hostname is needed by the BSF during key derivation.

NOTE 2: When the UE adds one or more PSK-based ciphersuites to the ClientHello message, this can be seen as an indication that the UE supports GBA-based authentication. If the UE supports PSK-based ciphersuites but not GBA-based authentication, the TLS handshake will fail if the NAF selected the PSK-based ciphersuite and suggested to use GBA (as described in step 2). In this case, the UE should attempt to establish the TLS tunnel with the NAF without including PSK-based ciphersuites to the ClientHello message, according to the procedure specified in clause 5.3. This note does not limit the use of PSK TLS to HTTP-based services.

2. If the NAF is willing to establish a TLS tunnel using a PSK-based ciphersuite, it shall select one of the PSK-based ciphersuites offered by the UE, and send the selected ciphersuite to the UE in the ServerHello message. The NAF shall send the ServerKeyExchange message with a PSK-identity that shall contain a constant string "3GPP-bootstrapping" to indicate the GBA as the required authentication method. The NAF finishes the reply to the UE by sending a ServerHelloDone message.

NOTE 3: If the NAF does not wish to establish a TLS tunnel using a PSK-based ciphersuite, it shall select a non-PSK-based ciphersuite and continue TLS tunnel establishment based on the procedure described either in clause 5.3 or clause 5.5.

3. The UE shall use a GBA-based shared secret for PSK TLS, if the NAF has sent a ServerHello message containing a PSK-based ciphersuite, and a ServerKeyExchange message containing a constant string "3GPP-bootstrapping" as the PSK identity hint. If the UE does not have a valid GBA-based shared secret it shall obtain one by running the bootstrapping procedure with the BSF over the Ub reference point as specified in TS 33.220 [3].

The UE derives the TLS premaster secret from the NAF specific key (e.g. Ks\_(ext)\_NAF) as specified in IETF Internet Draft [15].

The UE shall send a ClientKeyExchange message with the B-TID as the PSK identity. The UE concludes the TLS handshake by sending the ChangeCipherSuite and Finished messages to the NAF.

4. When the NAF receives the B-TID in the ClientKeyExchange messages it fetches the NAF specific shared secret (~~K<sub>s</sub>\_NAF~~) from the BSF using the B-TID.

The NAF derives the TLS premaster secret from the NAF specific key (~~K<sub>s</sub>\_NAF~~) as specified in IETF Internet Draft [15].

The NAF concludes the TLS handshake by sending the ChangeCipherSuite and Finished messages to the UE.

The UE and the NAF have established a TLS tunnel using GBA-based shared secret, and then may start to use the application level communication through this tunnel.

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