3GPP TSG-SA WG3 Meeting S3#34
Acapulco, Mexico, July 6-9, 2004

Tdoc ⌘S3-040656

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:	⌘	GBA supported indication and NAF hostname transfer in HTTP and in PSK TLS
Source:	⌘	Nokia, Siemens
Work item code:	⌘	GBA-SSC
Date:	⌘	29/06/2004
Category:	⌘	**C**
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 UE should be able to indicate to the NAF that it supports GBA based authentication. Also, the UE should be able to send NAF's hostname to the NAF.
Summary of change:	⌘	In order to ease the authentication method decision, the UE should be able to indicate to the NAF that it supports GBA based authentication. Also, in certain cases (e.g., virtual name based hosting) the hostname used by the UE when accessing the NAF is not unique, thus a method to transfer the hostname of the NAF used by the UE is needed. In HTTP case (subclause 5.3) these requirements are fulfilled by using HTTP headers "Host" and "User-Agent". In PSK TLS case (subclause 5.4) there requirements are fullfilled by using PSK-based ciphersuites, and the server_name TLS extension. The PSK TLS is now IETF TLS WG draft, thus the corresponding reference is updated.
Consequences if not approved:	⌘	The UE is not able to indicate to the NAF that is supports GBA-based authentication in HTTP and in PSK TLS. The UE is not required to send the hostname of the NAF to the NAF.

Clauses affected:	⌘	2, 5.3, 5.4

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

Other comments:	⌘	

===== BEGIN CHANGE =====

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TS 23.002: “Network architecture”.

[2] 3GPP TS 22.250: “IP Multimedia Subsystem (IMS) group management”; Stage 1”.

[3] 3GPP TS 33.220: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[4] 3GPP TR 33.919: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); System description".

[5] 3GPP TS 33.141: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Presence Service; Security"

[6] IETF RFC 2246 (1999): "The TLS Protocol Version 1".

[7] IETF RFC 3268 (2002): "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)".

[8] IETF RFC 3546 (2003): "Transport Layer Security (TLS) Extensions".

[9] IETF RFC 2818 (2000): “HTTP Over TLS ”.

[10] IETF RFC 2617 (1999): "HTTP Authentication: Basic and Digest Access Authentication"

[11] IETF RFC 3310 (2002): "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)"

[12] IETF RFC 2616 (1999): "Hypertext Transfer Protocol (HTTP) – HTTP/1.1"

[13] 3GPP TS 33.210: “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security; IP network layer security”

[14] OMA WAP-219-TLS, 4.11.2001: http://www.openmobilealliance.org/tech/affiliates/wap/wap-219-tls-20010411-a.pdf

[15] IETF Internet-Draft: “Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)”, ~~February 6~~ May 24, 2004, URL: http://www.ietf.org/internet-drafts/draft-~~eronen~~ietf-tls-psk-00.txt

[16] 3GPP TS 33.221: “Generic Authentication Architecture (GAA); Support for subscriber certificates”.

===== BEGIN NEXT 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 section 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. 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.

~~2~~3. In response to the ~~-~~HTTP~~S (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~~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.

~~4~~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 session key Ks_NAF as password.

~~5~~6. 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~~7. After the completion of step ~~5~~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.

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, any request sent by UE can be the first request inside a newly established TLS tunnel requiring the NAF to re-check user credentials.

===== BEGIN NEXT 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 3GPP 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 PKS-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 CientHello message, according to the procedure specified in subclause 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 subclause 5.3 or subclause 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 3GPP TS 33.220 [3].

   The UE derives the TLS premaster secret from the NAF specific key (Ks_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 (Ks_NAF) from the BSF using the B-TID.

   The NAF derives the TLS premaster secret from the NAF specific key (Ks_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 CHANGE =====