ETSI TS 133 222 V7.2.0 (2006-09)

Technical Specification

Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
Generic Authentication Architecture (GAA);
Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)
(3GPP TS 33.222 version 7.2.0 Release 7)

Reference

RTS/TSGS-0333222v720

Keywords

GSM, SECURITY, UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp .

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

A number of services might be accessed over HTTP. For the Presence Service, it shall be possible to manage the data on the Presence Server over the Ut reference point, which is based on HTTP. Other services like conferencing, messaging, push, etc. might be accessed using HTTP.

Access to services over HTTP can be done in a secure manner. The present document describes how the access over HTTP can be secured using TLS in the Generic Authentication Architecture.

1 Scope

The present document specifies secure access methods to Network Application Functions (NAF) using HTTP over TLS in the Generic Authentication Architecture (GAA), and provides Stage 2 security requirements, principles and procedures for the access. The present document describes both direct access to an Application Server (AS) and access to an Application Server through an Authentication Proxy (AP).

NOTE: Any application specific details for access to Applications Servers are not in scope of this specification and are covered in separate documents. An example of such a document is TS 33.141 [5], which specifies the security for presence services.

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: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[4] 3GPP TR 33.919: "Generic Authentication Architecture (GAA); System description".

[5] 3GPP TS 33.141: "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: "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 RFC 4279 (2005) "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)".

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

[17] OMA WAP-211-WAPCert, 22.5.2001: http://www.openmobilealliance.org/tech/affiliates/wap/wap-211-wapcert-20010522-a.pdf.

[18] 3GPP TS 24.109: "Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details".

[19] 3GPP TS 29.109: "Generic Authentication Architecture (GAA), Zh and Zn Interface based on the Diameter protocol; Stage 3".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

HTTPS: For the purpose of this document, HTTPS refers to the general concept securing the HTTP protocol using TLS. In some contexts, like in the IETF, the term HTTPS is used to refer to the reserved port number (443) for HTTP/TLS traffic.

Reverse Proxy: A reverse proxy is a web server system that is capable of serving web pages sourced from other web servers (AS), making these pages look like they originated at the reverse proxy.

Session management mechanism: A mechanism for creating stateful sessions when using the HTTP protocol.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AP	Authentication Proxy
AS	Application Server
B-TID	Bootstrapping Transaction Identifier
BSF	Bootstrapping Server Functionality
FQDN	Fully Qualified Domain Name
GBA	Generic Bootstrapping Architecture
HSS	Home Subscriber System
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over TLS
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia Public Identity
NAF	Operator-controlled network application function functionality
TLS	Transport Layer Security
UE	User Equipment

4 Overview of the Security Architecture

The overall security architecture conforms to the architecture defined in TS 33.220 [3]. Details of the solution with an authentication proxy are given in clause 6.

5 Authentication schemes

5.1 Reference model

Figure 1 shows a network model of the entities that utilize the bootstrapped secrets, and the reference points used between them.

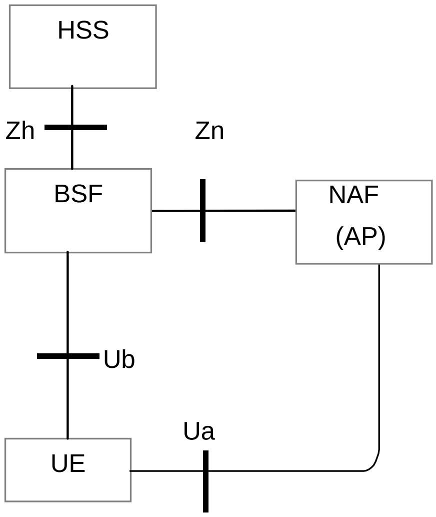

Figure 1: High level reference model for NAF using a bootstrapping service

5.2 General requirements and principles

This document is based on the architecture specified in TS 33.220 [3]. All notions not explained here can be found in TS 33.220 [3]. For the purposes of the present 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. Ks_int_NAF refers to the key shared between the UICC and a NAF.

The UE shall be able to indicate to the NAF which key (Ks_(ext)_NAF or Ks_int_NAF) the UE intends to use to secure the HTTPS Ua reference point.

The subscriber's home operator shall be able to require that a certain key (i.e., Ks_(ext)_NAF or Ks_int_NAF) shall be used to secure the HTTPS access between the UE and the NAF. This home operator control is exercised using USS.

5.2.1 Requirements on the UE

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].

The UE hosts the HTTPS client (i.e. both the HTTP client and the TLS client). The HTTP client and TLS client either resides both in the ME or in the UICC. The HTTPS client may reside in the ME or in the UICC or both might host an HTTPS client independently of each other. When the HTTPS capable client to be used is in the ME, Ks_(ext)_NAF shall be used as the shared key between the UE and the NAF. When the HTTPS capable client to be used is located in the UICC, Ks_int_NAF shall be used as the shared key between the UE and the NAF.

5.2.2 Requirements on the NAF

To utilise GBA as described in this document the NAF shall support the features of GBA as specified in TS 33.220 [3].

It shall be possible that the NAF is configured to restrict the access to the service based on which key is used, (e.g., access is allowed only for those HTTPS capable clients that reside in the UICC and use Ks_int_NAF). The key selection indication given in the USS shall overrule the local policy of the NAF.

NOTE: The support of GBA_U is optional for the NAF. However, as indicated in TS 33.220 [3], the use of Ks_ext_NAF is supported by NAFs, which are GBA_U unaware.

Additionally in the scope of this specification, HTTP and TLS shall be supported by the NAF for the UE-NAF reference point (Ua).

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

The authentication mechanism described in this section for ME-based application is mandatory to implement in ME and NAF.

The authentication mechanism described in this section for UICC-based application is optional to implement in the UICC and the NAF.

This section explains how the procedures specified in TS 33.220 [3] have to be enhanced when HTTPS is used between a ME and a NAF or between the UICC and the NAF. The following gives the complementary description with respect to the procedure specified in clauses 4.5.3 and 5.3.3 of TS 33.220 [3]. This document specifies the logical information carried in some header fields. The exact definition of header fields and key selection logic in case of GBA_U (i.e., whether Ks_ext_NAF or Ks_int_NAF shall be used) in the NAF is part of TS 29.109 [19] and TS 24.109 [18]. In the text below, the HTTPS client can reside in the ME or in the UICC.

1) When the HTTPS client starts communication via Ua reference point with the NAF, it shall establish a TLS tunnel with the NAF. The NAF is authenticated to the HTTPS client by means of a public key certificate. The HTTPS client 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 HTTPS client sends an HTTP request to the NAF inside the TLS tunnel (HTTPS, i.e. HTTP over TLS). The HTTPS client shall indicate to the NAF that GBA-based authentication is supported by adding a constant string to the "User-Agent" HTTP header as a product token as specified in IETF RFC 2616 [12]. This constant string shall be either "3gpp-gba" for ME-based applications or "3gpp-gba-uicc" for UICC based applications. 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 HTTPS client used to contact the NAF. The hostname is needed by the BSF during key derivation.

3) In response to the HTTP request received from HTTPS client over the Ua reference point, the NAF shall invoke HTTP digest as specified in RFC 2617 [10] with the HTTPS client in order to perform client authentication using the shared key as specified in clauses 4.5.3 and 5.3.3 of TS 33.220 [3].

   The NAF first verifies that the type of application received in the HTTP request ("3gpp-gba" for a ME-based application or "3gpp-gba-uicc" for a UICC-based application). Then the NAF verifies if the right realm attribute within the WWW-Authenticate header field has been used i.e. the realm attribute shall contain the constant string "3GPP-bootstrapping" (in the case of a ME-based application) or "3GPP-bootstrapping-uicc" (in the case of a UICC-based application) and the FQDN of the NAF (for both cases), shall indicate GBA as the required authentication method.

   If the NAF has been configured to forbid the access to the service for the requested GBA mode (e.g. the HTTP request contains "3gpp-gba" whilst the NAF configuration for this service requires that Ks_int_NAF shall be used) or if the NAF does not support the requested GBA mode (i.e. when a NAF, which is GBA_U unaware receives an HTTP request with "3gpp-gba-uicc" in "User-Agent" HTTP header) then the NAF shall respond with the appropriate error code and terminate the TLS connection with the UE.

4) On receipt of the response from the NAF, the HTTPS client 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 HTTPS client shall terminate the TLS connection with the NAF.

5) In the following request to NAF the HTTPS client sends a response with an Authorization header field where Digest is inserted using the B-TID as username.The NAF-specific key (Ks_(ext)_NAF in the case of ME-based application or Ks_int_NAF in the case of UICC-based application) is used as password in the Digest calculation.

6) On receipt of this request the NAF shall verify the value of the password attribute by means of the NAF-specific key (Ks_(ext)_NAF or Ks_int_NAF) retrieved from BSF over Zn using the B-TID received as user name attribute in the query.

   If the NAF has requested a USS, and the USS indicates to the NAF that the Ks_int_NAF shall be used for HTTPS, then the NAF shall only accept the use of Ks_int_NAF as the NAF specific key. Therefore, if the Ks_(ext)_NAF was used as the NAF specific key with the HTTPS client, then the NAF shall respond with the appropriate error code and terminate the TLS connection with the UE. For information on usage of USS see Annex C in TS 33.220 [3].

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 clauses 4.5.3 and 5.3.3 of TS 33.220 [11],.

5.3.1 TLS profile

The UE and the NAF shall support the TLS version as specified in RFC 2246 [6] and WAP-219-TLS [14] or higher. Earlier versions are not allowed.

NOTE 1: The management of Root Certificates is out of scope of this Technical Specification.

The UE and the NAF shall support the server_name TLS extension. All other TLS extensions as specified in RFC 3546 [8] are optional for implementation.

NOTE 2: If the NAF is doing virtual name based hosting (e.g. in the case of authentication proxy, see Annex A), the NAF needs to either have a TLS server certificate that contains all the hostnames that the NAF can be addressed with (i.e. virtual hostnames), or have one TLS server certificate for each of the hostnames mentioned above. In the latter case, the server_name extension is needed because the NAF needs to be able to select the correct TLS server certificate.

5.3.1.1 Protection mechanisms

The UE shall support the CipherSuite TLS_RSA_ WITH_3DES_EDE_CBC_SHA and the CipherSuite TLS_RSA_WITH_AES_128_CBC_SHA. All other Cipher Suites as defined in RFC 2246 [6] and RFC 3268 [7] are optional for implementation for the UE.

The NAF shall support the CipherSuite TLS_RSA_ WITH_3DES_EDE_CBC_SHA the CipherSuite TLS_RSA_WITH_RC4_128_SHA and the CipherSuite TLS_RSA_WITH_AES_128_CBC_SHA. All other Cipher Suites as defined in RFC 2246 [6] and RFC 3268 [7] are optional for implementation for the NAF.

Cipher Suites with NULL encryption may be used. The UE shall always include at least one cipher suite that supports encryption during the handshake phase.

Cipher Suites with NULL integrity protection (or HASH) are not allowed.

5.3.1.2 Key agreement

The Key exchange method shall not be anonymous. Hence the following cipher suites as defined in RFC 2246 [6] are not allowed for protection of a session:

- CipherSuite TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
- CipherSuite TLS_DH_anon_WITH_RC4_128_MD5
- CipherSuite TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
- CipherSuite TLS_DH_anon_WITH_DES_CBC_SHA
- CipherSuite TLS_DH_anon_WITH_3DES_EDE_CBC_SHA

5.3.1.3 Authentication of the AP/AS

The AP/AS is authenticated by the Client as specified in WAP-219-TLS [14], which in turn is based on RFC 2246 [6].

The AP/AS certificate profile shall be based on WAP Certificate and CRL Profile as defined in WAP 211 WAPCert [17].

5.3.1.4 Authentication Failures

If the UE receives a Server Hello Message from the AP/AS that requests a Certificate then the UE shall respond with a Certificate Message containing no Certificate if it does not have a certificate. The AP/AS upon receiving this message may respond with a failure alert, however if the AP/AS shall authenticate the UE as configured by the policy of the operator the AP/AS should continue the dialogue and assume that the UE will be authenticated as specified in TS 33.220 [11].

If there is no response within a given time limit from a network initiated re-authentication request an authentication failure has occurred after that the request has been attempted for a limited number of times. This failure can be due to several reasons, e.g. that the UE has powered off or due to that the message was lost due to a bad radio channel. The AP/AS shall then still assume that if a TLS session is still valid that it can be re-used by the UE at a later time. Should then the UE re-use an existing session then the AP/AS shall re-authenticate the UE and not give access to the AP/AS unless the authentication was successful.

5.3.1.5 Set-up of Security parameters

The TLS Handshake Protocol negotiates a session, which is identified by a Session ID. The Client and the AP/AS shall allow for resuming a session. This facilitates that a Client and Server may resume a previous session or duplicate an existing session. The lifetime of a Session ID is maximum 24 hours. The Session ID shall only be used under its lifetime and shall be considered by both the Client and the Server as obsolete when the Lifetime has expired.

5.3.1.6 Error cases

The AP/AS shall consider the following cases as a fatal error:

- if the received ciphersuites only includes all or some of the ciphersuites in clause 5.3.1.2;
- if the received ciphersuites do not include any integrity protection.

5.4 Shared key-based mutual authentication between UE and NAF

The authentication mechanism described in this section for ME-based application is optional to implement in ME and NAF.

The authentication mechanism described in this section for UICC-based application is optional to implement in UICC and NAF.

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].

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 [15]. The HTTPS client may reside in the ME or in the UICC. In former case, Ks_(ext)_NAF shall be used to establish the TLS session keys. In latter case, Ks_int_NAF shall be used to establish the TLS session keys.

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 PSK-based TLS. 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 CientHello 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 list of PSK-identity hints. A constant string "3GPP-bootstrapping" is used as PSK-identity hint to indicate that the local configuration in the NAF i.e. that the NAF accepts that Ks_(ext)_NAF is used establish the TLS session keys. A constant string "3GPP-bootstrapping-uicc" is used as PSK-identity hint to indicate that the local configuration in the NAF accepts that Ks_int_NAF is used to establish the TLS sessions keys. One of these PSK-identity hints shall be present in the ServerKeyExchange message, and it shall indicate the GBA as the required authentication method. If the local configuration in the NAF allows both authentication methods to be used to access its service then the ServerKeyExchange message shall include both of the PSK-identity hints, i.e., one identity hint contains the constant string "3GPP-bootstrapping" and the other contains "3GPP-bootstrapping-uicc". Also other PSK-identity hints may be supported, however, they are out of the scope of this specification. 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", or "3GPP-bootstrapping-uicc", or both 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].

   If the HTTPS client resides in the ME, Ks_(ext)_NAF shall be used as the GBA shared key. If the HTTPS client resides in the UICC, Ks_int_NAF shall be used as the GBA shared key.

   The UE derives the TLS premaster secret from the NAF specific key (Ks_(ext)_NAF if the initiating HTTPS client resides on the ME or Ks_int_NAF if the initiating HTTP client resides on the UICC) as specified in RFC 4279 [15].

   The UE shall send a ClientKeyExchange message. The PSK identity in the ClientKeyExchange message shall include a prefix indicating the PSK-identity name space that was selected (i.e. "3GPP-bootstrapping-uicc" or "3GPP-bootstrapping"), and the B-TID. The prefix shall match one of the PSK-identity hints that NAF offered in ServerKeyExchange message. The precise format of the PSK identity is specified in TS 24.109 [18]. The UE concludes the TLS handshake by sending the ChangeCipherSuite and Finished messages to the NAF.

4. If the NAF receives the "3GPP-bootstrapping" prefix and the B-TID in the ClientKeyExchange messages it fetches the NAF specific shared secret (Ks_(ext)_NAF) from the BSF using the B-TID, else the NAF receives the "3GPP-bootstrapping-uicc" prefix and the B-TID in the ClientKeyExchange messages it fetches the NAF specific shared secret (Ks_int_NAF) from the BSF using the B-TID.

   If the NAF has requested a USS, and the USS indicates to the NAF that only the Ks_int_NAF shall be allowed, then the NAF shall only accept the Ks_int_NAF as the NAF specific key. If the Ks_(ext)_NAF was used as the NAF specific key, the NAF shall respond with the appropriate error code and terminate the TLS connection with the UE.

   The NAF derives the TLS premaster secret from the NAF specific key (Ks_(ext)_NAF or Ks_int_NAF) as specified in [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.

5.4.1 TLS Profile

If the PSK TLS based authentication mechanism is supported, the HTTPS client in the UE or the NAF shall support the TLS version as specified in RFC 2246 [6], WAP 219 TLS [14], PSK TLS [15], or higher. Earlier versions are not allowed.

The HTTPS client in the UE and the NAF shall support the server_name TLS extension. All other TLS extensions as specified in RFC 3546 [8] are optional for implementation.

NOTE: If the NAF is doing virtual name based hosting (e.g. in the case of authentication proxy, see Annex A), the NAF needs to be able to discover the correct server name to indicate the correct NAF_ID to the BSF. Otherwise the BSF is not able derive the correct NAF specific keys.

5.4.1.1 Protection mechanisms

The UE shall support the CipherSuite TLS_PSK_WITH_3DES_EDE_CBC_SHA and the CipherSuite TLS_PSK_WITH_AES_128_CBC_SHA. All other Cipher Suites as defined in PSK TLS [15] are optional for implementation for the UE.

The NAF shall support the CipherSuite TLS_PSK_WITH_3DES_EDE_CBC_SHA, the CipherSuite TLS_PSK_WITH_RC4_128_SHA and the CipherSuite TLS_PSK_WITH_AES_128_CBC_SHA. All other Cipher Suites as defined in PSK TLS [15] are optional for implementation for the NAF.

Cipher Suites with NULL encryption may be used. The UE shall always include at least one cipher suite that supports encryption during the handshake phase.

Cipher Suites with NULL integrity protection (or HASH) are not allowed.

5.4.1.2 Authentication of the AP/AS

The AP/AS is authenticated by the Client as specified in PSK TLS [15].

5.4.1.3 Authentication Failures

If there is no response within a given time limit from a network initiated re-authentication request an authentication failure has occurred after that the request has been attempted for a limited number of times. This failure can be due to several reasons, e.g. that the UE has powered off or due to that the message was lost due to a bad radio channel. The AP/AS shall then still assume that if a TLS session is still valid that it can be re-used by the UE at a later time. Should then the UE re-use an existing session then the AP/AS shall re-authenticate the UE and not give access to the AP/AS unless the authentication was successful.

If the AP/AS, acting as NAF, has requested a USS, and the USS indicates to the NAF that only the Ks_int_NAF shall be allowed, then the NAF shall only accept the Ks_int_NAF as the NAF specific key therefore if the Ks_(ext)_NAF was used as the NAF specific key, then the NAF shall respond with the appropriate error code and terminate the TLS connection with the UE.

5.4.1.4 Set-up of Security parameters

The TLS Handshake Protocol negotiates a session, which is identified by a Session ID. The Client and the AP/AS shall allow for resuming a session. This facilitates that a Client and Server may resume a previous session or duplicate an existing session. The lifetime of a Session ID is the lifetime of the GAA shared secret or maximum of 24 hours. The Session ID shall only be used under its lifetime and shall be considered by both the Client and the Server as obsolete when the Lifetime has expired.

5.5 Certificate based mutual authentication between UE and application server

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

The certificate based mutual authentication between an UE and an application server shall be based on TLS as specified in IETF RFC 2246 [6] and IETF RFC 3546 [8].

Annex B of this specification provides guidance on certificate mutual authentication between UE and application server.

6 Use of Authentication Proxy

An Authentication Proxy (AP) is an HTTP proxy which takes the role of a NAF for the UE. It handles the TLS security relation with the UE and relieves the application server (AS) of this task. Based on GBA the AP can assure the ASs that the request is coming from an authorized subscriber of the MNO.

6.1 Architectural view

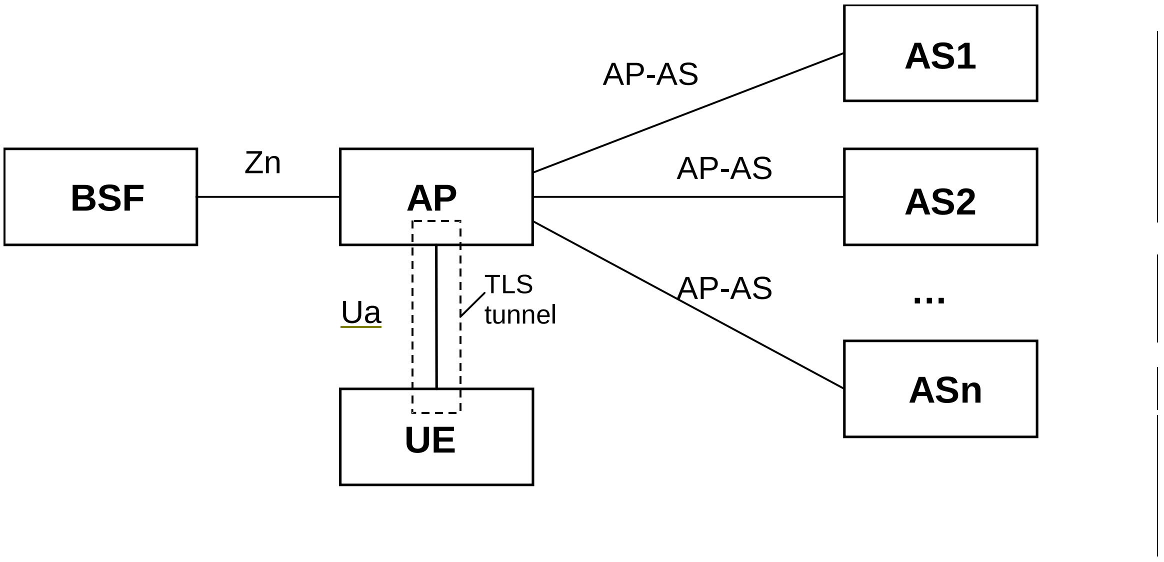

Figure 2: Environment and reference points of AP

The use of an authentication proxy (AP) is fully compatible with the architecture specified in TS 33.220 [3] and in clauses 4 and 5 of this specification. When an AP is used in this architecture, the AP takes the role of a NAF. When an HTTPS request is destined towards an application server (AS) behind an AP, the AP terminates the TLS tunnel and performs UE authentication. The AP proxies the HTTP requests received from UE to one or many application servers. The AP may add an assertion of identity of the subscriber for use by the AS, when the AP forwards the request from the UE to the AS.

NOTE: As an example, the following condition allows accessing multiple application servers AS(s) through one shared TLS tunnel (over the Ua interface) AS_n hostname = AP hostname = NAF_ID (e.g.: *services.operator.com*). There might be alternative ways to access multiple ASs behind an AP.

Figure 3 presents an architectural view of using Authentication Proxy, for example, for IMS SIP based services. The UE shall manipulate own data such as groups, through the Ua/Ut reference point. The reference point Ut specified in TS 23.002 [1] shall be applicable to data manipulation of IMS based SIP services, such as Presence, Messaging and Conferencing services. The stage 1 requirements are specified in TS 22.250 [2].

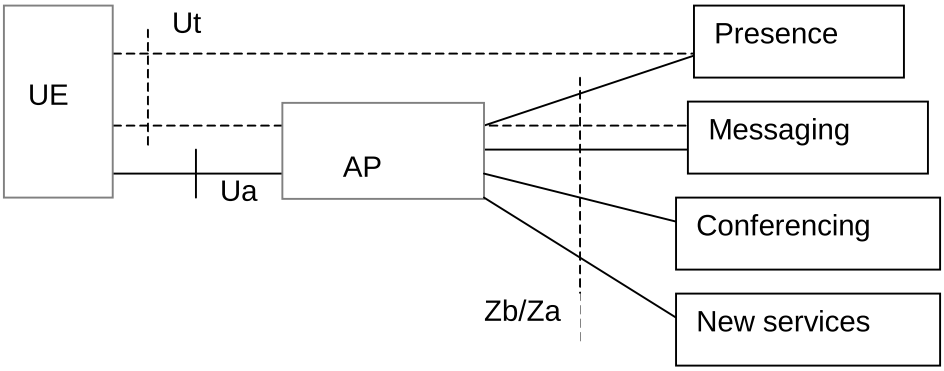

Figure 3: The architectural view using Authentication Proxy for IMS SIP based services

Management of UE identities is described in clause 6.5.

Annex A contains further guidance on technical solutions for authentication proxies.

6.2 Requirements and principles

The authentication proxy may reside between the UE and the AS as depicted in figure 2. The usefulness of an Authentication Proxy may be to reduce the consumption of authentication vectors and/or to minimize SQN synchronization failures. Also the AP relieves the AS of security tasks.

The following requirements apply for the use of an Authentication Proxy:

- authentication proxy shall be able to authenticate the UE using the means of Generic Bootstrapping Architecture, as specified in TS 33.220 [3];
- if the application server requires an authenticated identity of the UE the authentication proxy shall send it to the application server belonging to the trust domain with every HTTP request;
- if required, the authentication proxy may not reveal the authenticated identity of the UE to the application server not belonging to the trust domain;
- the authenticated identity management mechanism shall not prevent the application server to use an appropriate session management mechanisms with the client;
- the UE shall be able to create multiple parallel HTTP sessions via the authentication proxy towards different application servers;

NOTE 1: The used session management mechanism is out of the scope of 3GPP specifications.

NOTE 2: One motivation for having AP between UE and AS's is to minimize the number of TLS connections. However, there are situations when UE and AP may end-up having parallel TLS connections, e.g. if two applications in the UE are not able to share the same TLS connection.

- implementation of check of asserted user identity in the AS is optional;
- activation of transfer of asserted user identity shall be configurable in the AP on a per AS basis.

The use of an authentication proxy should be such that there is no need to manage the authentication proxy configuration in the UE.

NOTE 3: This requirement implies that the authentication proxy should be a reverse proxy in the following sense: A reverse proxy is a web server system that is capable of serving web pages sourced from other web servers - in addition to web pages on disk or generated dynamically by CGI - making these pages look like they originated at the reverse proxy.

6.4 Reference points

6.4.1 Ua reference point

The Ua reference point is standardised in specification TS 33.220 [3] and in clauses 4 and 5 of this specification.

NOTE: The optional introduction of an AP has advantages which are stated elsewhere. However, the following consequences should be taken into account to decide whether an AP is to be used:

- The AP terminates TLS and HTTP digest. This relieves the AS of the burden to handle TLS and HTTP digest, but it should be noted that then the UE is not able to establish an additional end-to-end TLS tunnel to the AS, nor can the UE additionally authenticates itself to AS by use of client authentication within TLS. Furthermore, if GBA authentication uses HTTP Digest Authentication, then the UE cannot use Basic or Digest Authentication directly with AS.

6.4.2 AP-AS reference point

The HTTP protocol is run over the AP-AS reference point.

Confidentiality and integrity protection can be provided for the reference point between the AP and the AS using NDS/IP mechanisms as specified in TS 33.210 [13]. For traffic between different security domains, the Za reference point shall be operated. For traffic inside a security domain, it is up to the operator to decide whether to deploy the Zb reference point. As AP terminates the TLS tunnel from UE, also a TLS tunnel is possible.

The AP may support the transfer of an identity of the UE authenticated by the AP from AP to AS in a standardised format. The format of this information element in the HTTP request header is left to stage 3 specifications.

6.5 Management of UE identity

Different ASs need different kinds of authentication information. To support the requirements of different servers, the AP needs to perform authentication with varying granularity and with varying degree of assertion to the AS. The authentication and the corresponding assertion is therefore AS specific and has to be configured in the AP per AS.

6.5.1 Granularity of Authentication and Access Control by AP

The AP is configured per AS if the particular application or applications served by the AS is in need of an application specific user security setting, see definitions in TS 33.220 [3]. This user security setting may contain the public user identities in the authentication part of the USS. The authorisation part of the USS may contain indications, which of the applications residing on the AP, and the Application Servers behind the AP, a user is allowed to access.

6.5.1.1 Authorised Participant of GBA

The AP checks that the UE is an authorised participant of GBA. Access is granted on success of the basic GBA mechanism, i.e. the HTTPS client in the UE sends a valid B-TID and performs digest authentication with the NAF specific keys received from BSF.

The AP is configured not to request an application specific user security setting from BSF for the AS named in the request. Depending on configuration of BSF the AP may receives the private user identity (IMPI) from BSF.

This case shall be supported by AP.

NOTE: This case may apply when all subscribers of an operator, but no other users, are allowed access to operator defined services. The BSF may not send the IMPI out of privacy considerations or because the AP does not need it. If the BSF does not send the IMPI to the AP, the user remains anonymous towards the AP; or more precisely, the B-TID functions as a temporary user pseudonym.

6.5.1.2 Authorised User of Application

The AP is configured to request an application specific user security setting from the BSF. Depending on the policy of the BSF, the AP receives the application specific user security setting and the private user identity (IMPI) from the BSF. Access is granted if allowed according to the application specific user security setting received from BSF.

The AP may do further checks on user inserted identities in the HTTP request if required according to clause 6.5.2.4.

This case shall be supported by AP.

NOTE: If there is no application specific user security setting configured for an application, this case reduces to authentication according to clause 6.5.1.1.

6.5.2 Transfer of Asserted Identity from AP to AS

The AP is configured per AS to perform authentication and access control according to one of the following subclauses: if required in the subclause, the user identity is transferred to AS in every HTTP request proxied to AS.

6.5.2.1 Authorised Participant of GBA

The AP checks that the UE is an authorised participant of GBA. If the authentication of the UE by the AP fails, the AP does not forward the request of the UE to the AS.

This case shall be supported by AP.

NOTE: This case simply implies that the NAF checks that the user is known to, and has established a valid key, with the BSF, according to the GBA procedures described in TS 33.220 [3].

6.5.2.2 Authorised User of Application Anonymous to AS

The AP checks that the UE is an authorised user of the application according to application specific user security setting received from BSF. No user identity shall be transferred to AS.

This case shall be supported by AP.

6.5.2.3 Authorised User of Application with Transferred Identity asserted to AS

The AP checks that the UE is an authorised user of the application. The user identity (or user identities) received from the BSF shall be transferred to AS. Based on AS-specific configuration of the AP, any authorization flags existing in application-specfic user security settings shall also be transferred to AS.

Depending on the application specific user security setting and the AS-specific configuration of the AP, the transferred user identity (or identities) may be the private user identity (IMPI), or may be taken from the application specific user security setting (e.g. an IMPU), or may be a pseudonym chosen by AP (e.g. Random, B-TID).

This case may be supported by AP.

NOTE 1: If the AP is configured to transfer a pseudonym to AS, any binding of this pseudonym to the user identity (e.g. for charging purposes by AS) is out of scope of this specification.

NOTE 2: If the AP is configured not to request an application specific user security setting from BSF, only the private user identity (IMPI) or a pseudonym may be transferred to AS. In this case any authorised participant of GBA is supposed to be an authorised user of the application.

6.5.2.4 Authorised User of Application with Transferred Identity asserted to AS and Check of User Inserted Identity

This case resembles clause 6.5.2.3 with the following extension:

Based on the user identity received from BSF, the AP authenticates user related identity information elements as sent from UE. These "user inserted identities" may occur within header fields or within the body of the HTTP request.

Depending on application specific user security setting and AS-specific configuration of AP, all user-inserted identities (or a subset thereof) are authenticated by checking against the private user identity (IMPI) or the application specific user security setting.

Depending on the application specific user security setting and the AS-specific configuration of AP, the transferred user identity (or identities) may also be selected from the authenticated user inserted identities.

This case may be supported by AP.

NOTE 1: If AP authenticates certain or all user related identity information elements of a request, and the AS shall rely on the check of these elements, then a corresponding policy between the AP and the AS needs to be in place between the AP and the AS.

NOTE 2: Any application specific details are beyond the scope of this document and may be specified within the application, e.g. for Presence in TS 33.141 [5]. This specification does not preclude that any other application specific specifications (e.g. Presence) declare this feature as mandatory in their scope.

Annex A (informative): Technical Solutions for Access to Application Servers via Authentication Proxy and HTTPS

This annex gives some guidance on the technical solution for authentication proxies so as to help avoid misconfigurations. An authentication proxy acts as reverse proxy which serves web pages (and other content) sourced from other web servers (AS) making these pages look like they originated at the proxy.

To access different hosts with different DNS names on one server (in this case the proxy) the concept of virtual hosts was created.

One solution when running HTTPS is to associate each host name with a different IP address (IP based virtual hosts). This can be achieved by the machine having several physical network connections, or by use of virtual interfaces which are supported by most modern operating systems (frequently called "*ip aliases*"). This solution uses up one IP address per AS and it does not allow the notion of "one TLS tunnel from UE to AP-NAF" for all applications behind a NAF together.

If it is desired to use one IP address only or if "one TLS tunnel for all" is required, only the concept of name-based virtual hosts is applicable. Together with HTTPS, however, this creates problems, necessitating workarounds which may deviate from standard behaviour of proxies and/or browsers. Workarounds, which affect the UE and are not generally supported by browsers, may cause interoperability problems. Other workarounds may impose restrictions on the attached application servers.

To access virtual hosts where different servers with different DNS names are co-located on AP, either of the solutions could be used to identify the host during the handshaking phase:

- Extension of TLS is specified in RFC 3546 [8]. This RFC supports the UE to indicate a virtual host that it intends to connect in the very initial TLS handshaking message (see clause 5.3.1);
- The other alternative is to issue a multiple-identities certificate for the AP. The certificate will contain identities of AP as well as each server that rely on AP's proxy function. The verification of this type of certificate is specified in RFC 2818 [9].

Either approach may be chosen by the operator who operates the authentication proxy.

Annex B (informative):
Guidance on Certificate-based mutual authentication between UE and application server

This section explains how subscriber certificates (see TS 33.221 [16]) are used in certificate-based mutual authentication between a UE and an application server. The certificate-based mutual authentication between a UE and an application server shall be based TLS as specified in IETF RFC 2246 [6] and IETF RFC 3546 [8].

When a UE and an application server (AS) want to mutually authenticate each other based on certificates, the UE has previously enrolled a subscriber certificate as specified in TS 33.221 [16]. After UE is in the possession of the subscriber certificate it may establish a TLS tunnel with the AS as specified in RFC 2246 [6] and RFC 3546 [8].

The AS may indicate to the UE, that it supports client certificate-based authentication by sending a CertificateRequest message as specified in section 7.4.4 of IETF RFC 2246 [6] during the TLS handshake. This message includes a list of certificate types and a list of acceptable certificate authorities. The AS may indicate to the UE that it supports subscriber certificate-based authentication if the list of acceptable certificate authorities includes the certification authority of the subscriber certificate (i.e. the operator's CA certificate).

The UE may continue with the subscriber certificate-based authentication if the list of acceptable certificate authorities includes the certification authority of the subscriber certificate. This is done by sending the subscriber certificate as the Certificate message as specified in sections 7.4.6 and 7.4.2 of IETF RFC 2246 [6] during the TLS handshake. If the list of acceptable certificate authorities does not include the certification authority of the subscriber certificate, then UE shall send a Certificate message that does not contain any certificates.

NOTE 1: Due to the short lifetime of the subscriber certificate, the usage of the subscriber certificate does not require on-line interaction between the AS and the PKI portal that issued the certificate.

If the AS receives a Certificate message that does not contain any certificates, it can continue the TLS handshake in two ways:

- if subscriber certificate-based authentication is mandatory according to the AS's security policy, it shall response with a fatal handshake failure alert as specified in IETF RFC 2246 [6], or

- if subscriber certificate-based authentication is optional according to AS's security policy, AS shall continue with TLS handshake as specified in IETF RFC 2246 [6].

In the latter case, if the AS has NAF functionality, the NAF may authenticate the UE as specified in clause 5.3 of the present specification, where after establishing the server-authenticated TLS tunnel, the procedure continues from step 4.

NOTE 2: In order to successfully establish a TLS tunnel between the UE and the AS using certificates for mutual authentication, the UE must have the root certificate of the AS's certificate in the UE's certificate store, and the AS must have the root certificate of the UE's subscriber certificate (i.e. operator's CA certificate) in the AS's certificate store. The root certificate is the root of the certification path, and should be marked trusted in the UE and the AS.

NOTE 3: In order to enable access to an AS in a visited network with subscriber certificates requires that the AS has the CA certificate of subscriber's home operator and it is marked trusted in the visited AS. The procedure to do this is outside the scope of this specification.

Annex C (informative): Change history

Change history									
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**Old**	**New**	**WI**
05-2004	SP-24	SP-040368	-	-		Presentation to TSG SA for Approval	1.1.1	2.0.0	
06-2004	SP-24	-	-	-		Approved at TSG SA #24 (Release 6)	2.0.0	6.0.0	
09-2004	SP-25	SP-040621	0001	-		GBA User Security Settings	6.0.0	6.1.0	SEC1-SC
09-2004	SP-25	SP-040621	0002	-		GBA supported indication and NAF hostname transfer in HTTP and in PSK TLS	6.0.0	6.1.0	SEC1-SC
09-2004	SP-25	SP-040621	0003	-		Editorial clean-up of TS 33.222	6.0.0	6.1.0	
09-2004	SP-25	SP-040621	0004	-		Further modifications to TLS profile related text in 33.222	6.0.0	6.1.0	SEC1-SC
12-2004	SP-26	SP-040889	0005	-		GBA supported indication in PSK TLS	6.1.0	6.2.0	GBA-SSC
12-2004	SP-26	SP-040889	0007	1		Adding Support for AES in the TLS Profile	6.1.0	6.2.0	GBA-SSC
12-2004	SP-26	SP-040889	0010	1		Authorization flag transfer between AP and AS	6.1.0	6.2.0	GBA-SSC
12-2004	SP-26	SP-040889	0012	-		Correction of inconsistencies within AP specification	6.1.0	6.2.0	GBA-SSC
12-2004	SP-26	SP-040889	0013	1		TLS extensions support	6.1.0	6.2.0	SEC1-SC
12-2004	SP-26	SP-040889	0014	-		Visited AS using subscriber certificates	6.1.0	6.2.0	SEC1-SC
03-2005	SP-27	SP-050141	0015	3		Keeping PSK TLS in 3GPP Rel-6	6.2.0	6.3.0	SEC1-SC
03-2005	SP-27	SP-050141	0016	1		Clarification to TS 33.222	6.2.0	6.3.0	SEC1-SC
03-2005	SP-27	SP-050166	0017	3		Clarify the GBA requirements for https supporting applications at Ua reference point	6.2.0	6.3.0	GBA-SSC
2005-06	SP-28	SP-050264	0019	-	F	Removal of editor"s note	6.3.0	6.4.0	SEC1-SC
2005-09	SP-29	SP-050558	0020	-	F	Adding additional mandatory CipherSuites for PSK TLS	6.4.0	6.5.0	SEC1-SC
2005-09	SP-29	SP-050568	0021	-	F	Removing an inconsistence within TS 33.222 (Section 6.2)	6.4.0	6.5.0	GBA-SSC
2005-09	SP-29	SP-050568	0023	-	F	Adding a clarification to TS 33.222 (Section 6.1)	6.4.0	6.5.0	GBA-SSC
2005-09	SP-29	SP-050575	0022	-	B	Usage of Ks_int_NAF for HTTPS connection between a UICC and a NAF	6.4.0	7.0.0	GBA-SSC
2006-03	SP-31	SP-060054	0025	-	A	Update PSK TLS Reference	7.0.0	7.1.0	SEC7-GAA2 (GAAExt)
2006-09	SP-33	SP-060501	0026	-	F	Clarification of using HTTP digest with HTTPS	7.1.0	7.2.0	SEC1-SC

History

Document history		
V7.0.0	September 2005	Publication
V7.1.0	March 2006	Publication
V7.2.0	September 2006	Publication