Presentation of Specification to TSG

Presentation to: **TSG SA Meeting #24**

Document for presentation: **TS 33.222, Version 2.0.0**

Presented for: **Approval**

Abstract of document:

In TSGS#23(04)0166, SA WG3 presented the status of the Access to Network Application Functions using HTTPS, TS 33.222 version 1.0.0. At SA3#33, the TS was further progressed and is estimated to be complete to 85%. Hence some issues are left that need to be further elaborated, see below.

Changes since last presentation to SA Meeting:

- New text for section 5.2 "General Requirements and Principles";
- New text for section 5.3 "Shared key-based UE authentication with certificate-based NAF authentication";
- Definition of TLS profile for shared key based UE authentication according to clause 5.3 of TS 33.222 (moved from TS 33.141);
- New text for section 5.4 "Shared key-based mutual authentication between UE and NAF";
- New text for section 5.5 "Certificate based mutual authentication between UE and application server";
- Introducing text for sub-sections 6.4 "Interfaces" and 6.5 "Management of UE Identity";
- Defining mechanisms for AP-AS interface protection in section 6.4;
- Removal of Annex B (Optimised Sequence of Events for Access to co-located BSF and NAF via HTTPS);
- Introducing a new Annex on "Guidance on Certificate -based mutual authentication between UE and application server";
- Editorial updates.

Outstanding Issues:

The following issues are open in TS 33.222:

- Some open issues related to shared key TLS;
- It is FFS if this specification should mandate any of the AES cipher suites as specified in RFC 3268 (5.3.1);
- It is FFS what parts (if any) of the TLS extensions as specified in RFC 3546 [8] shall be implemented in this TS (5.3.1);
- Requirements for the Authentication Proxy architecture might be revisited after feasibility of shared-key TLS has been fully studied;
- If further information elements from the application specific user profile are transferred in standardised format to AS is ffs (6.4.2, 6.5.2);
- The changes made to handling of application specific user profiles in TS 33.220 may affect section 6.5;
- The text in Annex A may need to be revisited if changes in the main body of the text are made;
- The support of accessing an AS in the visited network is FFS in future release (new Annex B, Guidance on Certificate-based mutual authentication between UE and application server).

Contentious Issues:

None.

3GPP TS 33.222 V1.1~~0~~.1~~0~~ (2004-05~~3~~)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects Generic Authentication Architecture (GAA); Access to Network Application Functions using HTTPS (Release 6)

Keywords
<keyword[, keyword]>

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

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 ~~interface~~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 and principles for the access. The document describes both direct access to an Application Server (AS) and access to an Application Server through an Authentication Proxy (AP).

~~Editor's note: The present document provides a general description of HTTP over TLS for any service that requires secure access over HTTP. For release 6, the Presence TS describes more specifically how access to the Presence server is secured. It is FFS if TLS 1.1 should be specified for use in this document.~~

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: "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, 2004, URL: http://www.ietf.org/internet-drafts/draft-eronen-tls-psk-00.txt

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

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.

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

~~Editor’s note: A picture explaining the overall architecture and text supporting the picture should be added.~~

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 section 6.

5 Authentication Schemes

5.1 Reference model

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

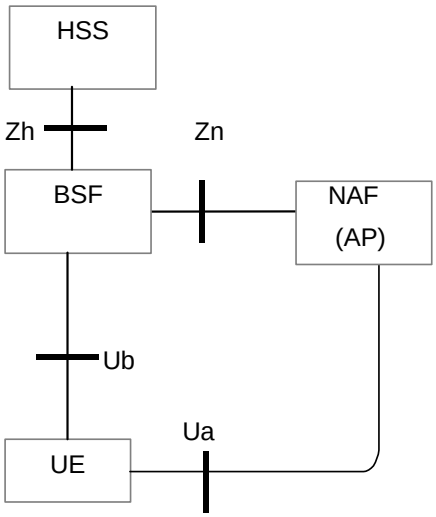

Figure 1: High level reference model for NAF using a bootstrapping service

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].

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].~~Editor's note: requirements on the UE are FFS~~

5.2.2 Requirements on the ~~Network~~NAF and BSF

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

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

~~Editor's note: care must be taken that this specification is in line with TS 33.141 on presence security.~~

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 ~~only enhancement required is the need to specify how the set up of a TLS tunnel is included in the general procedures specified in [3].~~ 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.

~~Editor's note: The sequence of events needs to be updated to reflect the initiation of bootstrapping as described in TS 33.220, section 4.3.1.~~

~~When the UE accesses a NAF, with which it does not yet share a key, then the sequence of events is as follows:~~

~~1. the UE runs http digest aka [11] with the BSF over the Ub interface.~~

~~2. If the BSF has no authentication vectors for the UE it fetches authentication vectors from the HSS over the Zh interface.~~

~~After the completion of step 1), the UE and the BSF share a secret key. This shared key is identified by a transaction identifier supplied by the BSF to the UE over the Ub interface key, cf. [3, section 4.3.1].~~

~~3~~1. When the UE starts communication via Ua reference point with the NAF, it shall ~~The UE~~ establish~~es~~ 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).

~~Editor's note: TLS needs to be profiled in an appropriate section of this specification.~~

~~4. The UE sends an http request to the NAF.~~

~~5~~2. In response to the HTTPS (HTTP over TLS) request received from UE over the Ua reference point, t~~T~~he NAF shall invoke~~s~~ ~~http~~ HTTP digest as specified in RFC 2617 [10] with the UE ~~over the Ua interface~~ in order to perform client authentication using the shared key ~~agreed in step 1),~~ as specified in section 4.5.3 of TS 33.220 [3~~, Annex A~~]. 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.

~~Editor's note: bullet 5 references Annex A in TS 33.220, which is informative.~~

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~~n~~ 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. While executing step 5), the NAF fetches the shared key from the BSF over the Zn interface, as specified in [3, Annex A and section 4.3.2].~~

~~7~~6. After the completion of step ~~4~~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.

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.

~~The UE may now run an appropriate application protocol with the NAF through the authenticated tunnel.~~

~~When the UE accesses a NAF, with which it already shares a key, steps 1), 2), 5) and 6) may be omitted, as specified in [3].~~

~~Editor's note: the above procedure is generally applicable and conforms to [TS 33.220]. For the case of a co-located BSF and NAF an optimisation is possible which is currently located in the informative Annex Z. SA3 still needs to decide whether the material in the annex should be moved to the main body, or remain in an informative or normative annex, or be deleted.~~

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: The management of Root Certificates is out of scope ~~for~~of this Technical Specification.

5.3.1.1 Protection Mechanisms

The UE shall support the CipherSuite TLS_RSA_WITH_3DES_EDE_CBC_SHA. All other Cipher Suites as defined in RFC 2246 [6] are optional for implementation for the UE.

The NAF shall support the CipherSuite TLS_RSA_WITH_3DES_EDE_CBC_SHA and the CipherSuite TLS_RSA_WITH_RC4_128_SHA. All other Cipher Suites as defined in RFC 2246 [6] are optional for implementation for the NAF.

Editors Note: It is FFS if this specification should mandate any of the AES cipher suites as specified in RFC 3268.

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.

Editors Note: It is FFS what parts (if any) of the TLS extensions as specified in RFC 3546 [8] shall be implemented in this TS.

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

5.4 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 ~~thus~~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 ~~to~~in the ClientHello message.

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: 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.

5.5 Certificate based mutual authentication between UE and ~~NAF~~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

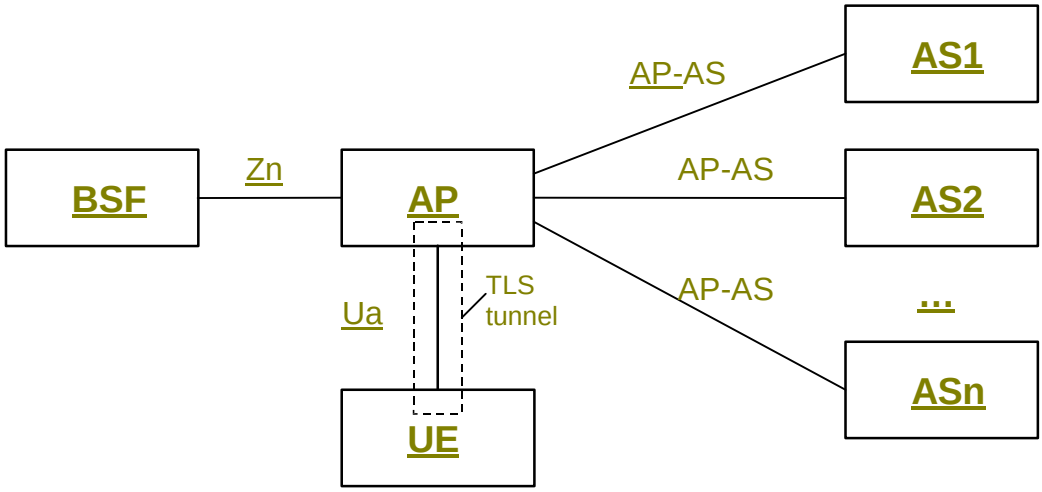

Figure 2: Environment and reference points of AP

The use of an authentication proxy (AP) is fully compatible with the architecture specified in TS 33.220 [3] and in section 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.

Figure 3~~2~~ 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 ~~interface~~reference point. The ~~interface~~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].

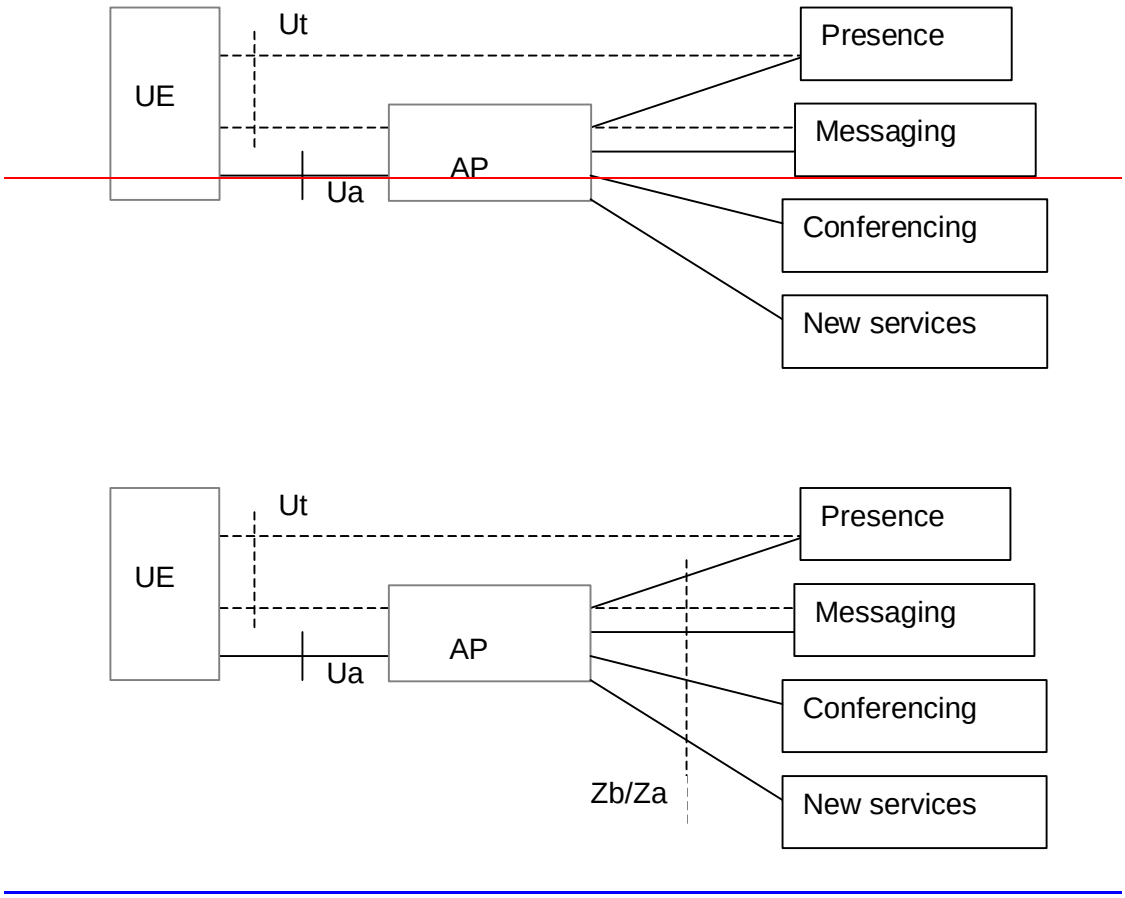

Figure 32: The architectural view using Authentication Proxy for IMS SIP based services

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 NAF as depicted in Figure 2 in section 6.1. 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 aAuthentication proxy shall send itthe authenticated identity of the UE to the application server belonging to the trust domain with every HTTP requestat the beginning of new HTTP session.
- 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.

NOTE1: The used session management mechanism is out of the scope of 3GPP specifications.

- 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 ~~base~~basis.

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

NOTE2: 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.

[Editors' note: The above requirements may be revisited after the following issues are fully studied:

- feasibility of shared-key TLS;

terminal configurability]

6.3 Authentication proxy architecture

The use of an authentication proxy (AP) is fully compatible with the architecture specified in [3] and in section 4 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 behind an authentication proxy (AP), the AP terminates the TLS tunnel and performs UE authentication. The AP proxies the http request to the application server.

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

6.4 ~~6.4 Interfaces~~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 [12]. 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 shall 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.

Editor's Note: If further information elements from the application specific user profile are transferred in standardised format to AS is ffs.

6.5 Management of UE identity

Editor's Note: The changes made to handling of application specific user profiles in TS 33.220 may aeffect this clause.

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 profile. This user profile may contain the public user identities.

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 UE sends a valid B-TID and performs digest authentication with the Ks_NAF received from BSF.

The AP is configured not to request an application specific user profile 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 profile from the BSF. Depending on the policy of the BSF, the AP receives the application specific user profile and the private user identity (IMPI) from the BSF. Access is granted if allowed according to the application specific user profile received from BSF.

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

This case shall be supported by AP.

NOTE: If there is no application specific user profile configured for an application, this case reduces to authentication according to subclause 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.

Editor's Note: It is ffs if further information elements from application specific user profile may be transferred 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 profile received from BSF. No user identity shall be transferred to AS.

This case may 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.

Depending on the application specific user profile 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 profile (e.g. an IMPU), or ~~it is~~may be a pseudonym chosen by AP (e.g. Random, B-TID).

This case may be supported by AP.

NOTE: 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: If the AP is configured not to request an application specific user profile 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 subclause 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 profile 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 profile.

Depending on the application specific user profile 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: 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: 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~~s~~ this feature as mandatory in ~~its~~their scope.

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

Editors' note: The text in this informative annex may need to be revisited if changes in the main body of the text are made.

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;

- 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].

Editor’s note: The shared-key TLS based authentication does not require server’s certificate, but the possession of the key for authentication. The procedure is ffs.

Annex B (informative): Optimised Sequence of Events for Access to co-located BSF and NAF via HTTPS

Editor's note: SA3 still needs to decide whether the material in the annex should be moved to the main body, or remain in an informative or normative annex, or be deleted.

Editor's note: the material in this annex is based on the information flow in S3-030371, Annex A.

Editor's note: The impact on implementation when co-locating BSF and NAF is for further study.

Editor's note: The sequence of events needs to be updated to reflect the initiation of bootstrapping as described in TS 33.220, section 4.3.1.

When the UE accesses a NAF, and the NAF is co-located with the BSF, then the optimised sequence of events is as follows:

1. The UE establishes a TLS tunnel with the NAF. The NAF is authenticated to the UE by means of a public key certificate.

Editor's note: TLS needs to be profiled in an appropriate section of this specification.

2. If the UE does not share a key with the NAF, the UE sends an http request to a NAF, containing the UE's identity.

3. If the NAF receives an http request from the UE without an Authorization header, or with an Authorization header it does not accept, the NAF contacts the (co-located) BSF to obtain a challenge and a password, computed from an AKA authentication vector according to [draft-torvinen-http-digest-aka-v2].

4. If the BSF has no authentication vectors for the UE it fetches authentication vectors from the HSS over the Zh interface.

5. The NAF replies to the UE by sending a 401 "unauthorized" message with a WWW-Authenticate header according to [draft-torvinen-http-digest-aka-v2].

6. The UE sends an http request to the NAF with an Authorization header according to [draft-torvinen-http-digest-aka-v2].

7. The NAF verifies the Authorization header.

After the completion of step 7), UE and NAF are mutually authenticated as the TLS tunnel endpoints.

8. The NAF replies to the http request returning the requested information to the UE, if any.

The UE may now run an appropriate application protocol with the NAF through the authenticated tunnel.

Editor's note: the transport of of key derivation information from NAF/BSF to UE needs further study.

Note on co-location of BSF and NAF: a BSF and a NAF may be combined on one machine in such a way that the BSF is accessed through http, not using TLS, and the NAF is accessed through https. From a functional point of view, this case is identical to the general case described in section 4.2. It is even possible to functionally duplicate the BSF on one machine in such a way that the BSF is accessed through http, when TLS is not required, and accessed through https, when access to the NAF requires TLS.

~~Editor's note on carrying identities: the first http request after TLS set-up needs to contain the identity of the UE. The reason is that for http digest the server can issue a challenge without knowing the client's identity, whereas for http digest aka the challenge is specific to a particular client. There seem to be at least two solutions for this:~~

~~a) use a specially formed http GET request, as described for the Ub interface in [TS33.220].~~

~~b) use an Authorization header with dummy values (to be defined). The server will not accept the credentials, and will reply with a 401 "unauthorised". For maximum harmonisation, the UE identity, which needs to be included by the UE at the start of the http digest aka protocol run, should be carried in the same way in the general and the optimised case.~~

~~Note on tunnelled authentication and the use of http digest aka:~~

~~In this annex and in section 4.2 respectively, different versions of http digest aka are used. This prevents man-in-the-middle attacks with tunnelled authentication. Version 1 of http digest aka [11] is used between the UE and the BSF when http digest aka is NOT used to authenticate the client endpoint of a TLS tunnel extending between UE and BSF. Version 1 may be run inside or outside a TLS tunnel, as long as it is not used for client authentication. Version 2 [draft-torvinen-http-digest-aka-v2] is used when http digest aka IS used to authenticate the client endpoint of a TLS tunnel. Version 2 is always run inside a TLS tunnel.~~

~~[Editor'Note on tunnelled authentication and the use of http digest aka:~~

~~Instead of using different versions of http digest aka to distinguish whether http digest aka is used for client authentication of a TLS tunnel or not, this distinction could be provided by different means. Possibilities suggested on the SA3 mailing list include to extend the specification of http digest akav2 to include a "situation" (or "context") parameter in the computation of the password, then always use http digest akav2, but with different values for the "situation" parameter for the two different uses.]~~

~~Note on transaction identifiers: the general approach, as specified in section 4, which is based on [3], requires the use of a transaction identifier over the interfaces Ua, Ub and Zn. The use of such a transaction identifier is neither possible nor necessary in the optimised case described in this annex.~~

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

This section explains how subscriber certificates (cf. 3GPP TS 33.221 [16]) are used in certificate-based mutual authentication between a~~n~~ UE and an application server. The certificate-based mutual authentication between a~~n~~ 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 3GPP 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 IETF RFC 2246 [6] and IETF RFC 3546 [8].

The AS may indicate to the UE, that it supports client certificate-based authentication by sending a CertificateRequest message as specifi~~c~~ed 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~~d~~ the certification authority of the subscriber certificate. This is done by sending the subscriber certificate as the Certificate message as specified in section 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: 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 subclause 5.3 of the present specification, where after establishing the server--authenticated TLS tunnel, the procedure continues from step 4.

NOTE: 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.

Editor's note: The support of accessing an AS in the visited network is FFS in future release.

Annex C (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2003-10	SA3 #30	S3-030646			First Draft TS: Generic Authentication Architecture; Access to Network Application Function using HTTPS (Release 6), table of contents added		0.1.0
2003-10					Updated based on editorial comments on the SA3 e-mail list	0.1.0	0.1.1
2004-01	SA3 #31	S3-030744 S3-030745 S3-030746 S3-030749			Updated based on agreements at SA3 #31	0.1.1	0.2.0
2004-03	SA3 #32	S3-040166 S3-040069 S3-040192			Updated based on agreements at SA3 #32	0.2.0	1.0.0
2004-05	SA3 #33	S3-040319 S3-040321 S3-040323 S3-040348 S3-040320 S3-040336 S3-040337 S3-040322			Updated based on agreements at SA3 #33	1.0.0	1.1.0
2004-05	SA3 #33				After email review over SA3 reflector, the following changes were made editorial changes update of figure 2 new text in 5.3, 5.4 and 5.5 to indicate what is mandatory and optional for implementation in the UE and the NAF	1.1.0	1.1.1

3GPP TS 33.222 V2.0.0 (2004-05)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Access to Network Application Functions using HTTPS (Release 6)

Keywords
Security, Authentication, Architecture

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

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

Editor's Note: 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 and principles for the access. The 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: "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, 2004, URL: http://www.ietf.org/internet-drafts/draft-eronen-tls-psk-00.txt.

[16] 3GPP TS 33.221: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Support for subscriber certificates".

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.

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.

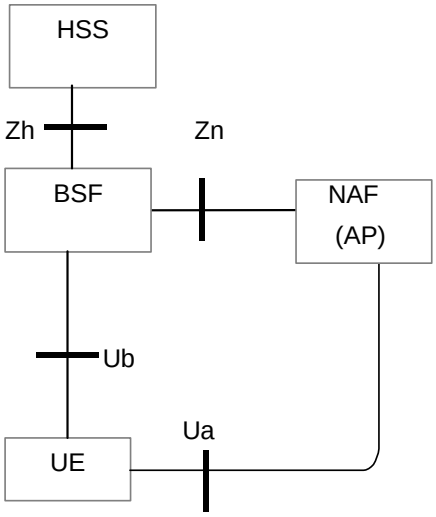

Figure 1: High level reference model for NAF using a bootstrapping service

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].

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].

5.2.2 Requirements on the NAF and BSF

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

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

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

5.3.1.1 Protection Mechanisms

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

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

Editors Note: It is FFS if this specification should mandate any of the AES cipher suites as specified in RFC 3268 [7].

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.

Editors Note: It is FFS what parts (if any) of the TLS extensions as specified in RFC 3546 [8] shall be implemented in this TS.

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

5.4 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.

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: 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 (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.

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

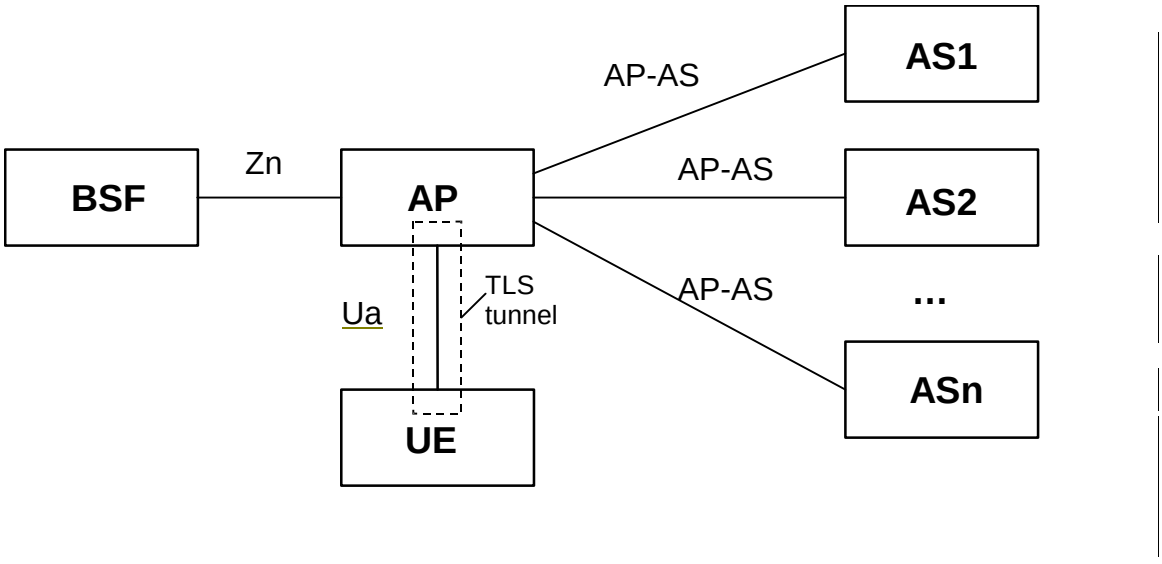

Figure 2: Environment and reference points of AP

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.

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].

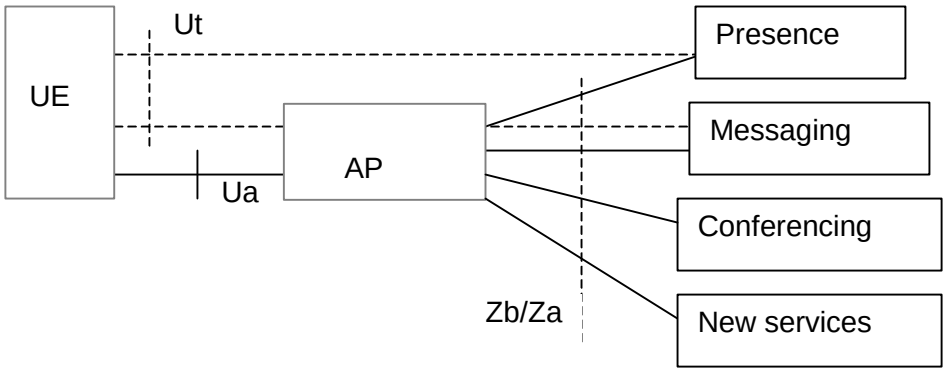

Figure 3: The architectural view using Authentication Proxy for IMS SIP based services

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 NAF 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.

- 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 2: 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.

Editors' note: The above requirement may be revisited after the following issues are fully studied:

- feasibility of shared-key TLS

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 [12]. 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 shall 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.

Editor's Note: If further information elements from the application specific user profile are transferred in standardised format to AS is ffs.

6.5 Management of UE identity

Editor's Note: The changes made to handling of application specific user profiles in TS 33.220 may affect this clause.

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 profile. This user profile may contain the public user identities.

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 UE sends a valid B-TID and performs digest authentication with the Ks_NAF received from BSF.

The AP is configured not to request an application specific user profile 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 profile from the BSF. Depending on the policy of the BSF, the AP receives the application specific user profile and the private user identity (IMPI) from the BSF. Access is granted if allowed according to the application specific user profile 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 profile 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.

Editor's Note: It is ffs if further information elements from application specific user profile may be transferred 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 profile received from BSF. No user identity shall be transferred to AS.

This case may 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.

Depending on the application specific user profile 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 profile (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: 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: If the AP is configured not to request an application specific user profile 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 profile 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 profile.

Depending on the application specific user profile 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: 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: 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

Editors' note: The text in this informative annex may need to be revisited if changes in the main body of the text are made.

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;

- 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].

Editor's note: The shared-key TLS based authentication does not require server's certificate, but the possession of the key for authentication. The procedure is ffs.

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: 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: 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.

Editor's note: The support of accessing an AS in the visited network is FFS in future Release.

Annex C (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2003-10	SA3 #30	S3-030646			First Draft TS: Generic Authentication Architecture; Access to Network Application Function using HTTPS (Release 6), table of contents added		0.1.0
2003-10					Updated based on editorial comments on the SA3 e-mail list	0.1.0	0.1.1
2004-01	SA3 #31	S3-030744 S3-030745 S3-030746 S3-030749			Updated based on agreements at SA3 #31	0.1.1	0.2.0
2004-03	SA3 #32	S3-040166 S3-040069 S3-040192			Updated based on agreements at SA3 #32	0.2.0	1.0.0
2004-05	SA3 #33	S3-040319 S3-040321 S3-040323 S3-040348 S3-040320 S3-040336 S3-040337 S3-040322			Updated based on agreements at SA3 #33	1.0.0	1.1.0
2004-05	SA3 #33				After email review over SA3 reflector, the following changes were made editorial changes update of figure 2 new text in 5.3, 5.4 and 5.5 to indicate what is mandatory and optional for implementation in the UE and the NAF	1.1.0	1.1.1
05-2004	SP-24	SP-040368	-	-	Revision marks removed and editorial updated for Presentation for Approval	1.1.1	2.0.0