Technical Specification Group Services and System Aspects **TSGS#23(04)0163**

Meeting #23, Phoenix, USA, 15 - 18 March 2004

Presentation of Specification to TSG

Presentation to:	**TSG SA Meeting #23**
Documents for presentation:	**TR 33.141, Version 1.1.1**
Presented for:	**Information**

Abstract of document:

In TSGS#22(03)0719 SA WG3 presented the status of the security for Presence Services in TS33.141v100. At SA3#32 the TS was further progressed and is estimated to be complete to 75%. Hence some issues are left that need to be further elaborated, see below.

Changes since last presentation to SA Meeting:

- The term ISIM was removed and replaced with USIM.
- Reference to GAA TR was included
- Editorial changes and several Editors Notes were removed
- Confidentiality protection clarified to be optional for use
- SA3 made the working assumption that 3GPP shall re-use the TLS profiles from OMA and relevant references were included. Hence the support of AES cipher suites is under the responsibility of OMA
- Relevant text was included in Clause 6 and 7

Outstanding Issues:

There are open issues but it is the view of SA3 that all of the open issues are possible to resolve and SA3 assumes that it is feasible to submit the TS for approval to the SA#24 plenary meeting in June 2004..

- Some editors notes are still left e.g. the handling of user identities
- The use of Shared Key TLS is still FFS however SA3 aims to based on amongst other things the progress in IETF make a decision at the SA3#33 meeting
- SA3 has also identified that If 3GPP decides that ISIM-only UICCs are allowed then it needs to be studied further if also the ISIM may be used in the Generic Authentication Architecture

Contentious Issues:

None.

3GPP TS 33.141 V1.1.1 (2004-03)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Presence Service;
Security
(Release 6)

Keywords
Security, Presence

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

This technical specification defines the security architecture and requirements for the presence services. Presence services enable the spreading of presence information of a user to users or services. A presence entity or presentity comprises the user, users devices, services and services components. It is the intention that this platform will enable new services like e.g. enhancement to chat, multimedia messaging, cinema ticket information, the score of a football game and so on.

A user has the possibility to control if her or his information shall be available to other users or services. This control is possible to achieve with high granularity e.g. explicitly define which user or users and services that shall have access to presence information.

A presentity is an uniquely identifiable entity with the capability to provide with presence information and it has only one principal associated with it. Hence a principal is distinct from all other principals and can be e.g. a human, organisation, program or even a collection thereof. One example of such a relation is when the presentity is a terminal and the principal of the terminal is the subscriber. A watcher is also an uniquely identifiable entity but with the aim to fetch or request information about a presentity. There are access rules that set the rules for the presence service how presence information gets available to watchers.

Presence information consists of a number of elements or presence tuples as defined in 3GPP TS 23.141 [3].

1 Scope

The present document describes the Stage 2 security requirements for the Presence Service, which includes the elements necessary to realise the requirements in 3GPP TS 22.141 [2] and 3GPP TS 23.141 [3].

The present document includes information applicable to network operators, service providers and manufacturers.

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 TR 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.141: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Presence Service; Stage 1".

[3] 3GPP TS 23.141: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Presence Service; Architecture and functional description".

[4] 3GPP TS 33.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Access security for IP-based services".

[5] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2".

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

[7] 3GPP TS 23.002: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; Network architecture".

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

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

[10] 3GPP TS 33.210: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security; IP network layer security".

[11] 3GPP TS 33.220: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

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

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

[14] IETF -draft-ietf-tls-rfc2246-bis-05 (2003): "The TLS Protocol Version 1.1"

[15] 3GPP TR 33.919: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); System Description".

[16] 3GPP TS 24.cde: "3rd Generation Partnership Project; Technical Specification Group Core Network; Bootstrapping interface (Ub) and Network application function interface (Ua); Protocol details".

[17] IETF -RFC 2818 (2000): "HTTP over TLS".

3 Definitions and abbreviations

3.1 Definitions

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

Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Data integrity: The property that data has not been altered in an unauthorised manner.

Data origin authentication: The corroboration that the source of data received is as claimed.

Entity authentication: The provision of assurance of the claimed identity of an entity.

Key freshness: A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply, 3GPP TR 21.905 [1] contains additional applicable abbreviations:

AKA	Authentication and key agreement
CSCF	Call Session Control Function
HSS	Home Subscriber Server
IM	IP Multimedia
IMPI	IM Private Identity
IMPU	IM Public Identity
IMS	IP Multimedia Core Network Subsystem
ISIM	IM Services Identity Module
MAC	Message Authentication Code
ME	Mobile Equipment
SA	Security Association
SEG	Security Gateway
SDP	Session Description Protocol
SIP	Session Initiation Protocol
UA	User Agent

4 Overview of the security architecture

An IMS operator using the CSCFs as Watcher Presence proxies and Presentity Presence proxies may offer the Presence services on top of the IMS network, cf. 3GPP TS 22.141 [2]. The access security for IMS is specified in 3GPP TS 33.203 [4] ensuring that SIP signalling is integrity protected and that IMS subscribers are authenticated through the use of IMS AKA. The security termination point from the UE towards the network is in the P-CSCF utilising IPsec ESP.

A watcher can ~~by~~ be sending a SIP SUBSCRIBE over IMS towards the network to subscribe ~~to~~ or to fetch presence information, i.e. the Presence Service supports SIP-based communications for publishing presence information. The

presence information is provided by the Presence Server to the Watcher Application using SIP NOTIFY along the dialogue setup by SUBSCRIBE. This traffic is protected in a hop-by-hop fashion using a combination of SEGs as specified in 3GPP TS 33.210 [10] with the access security provided in 3GPP TS 33.203 [4].

The Presence Server is responsible for managing presence information on behalf of the presence entity and it resides in the presentity's home network. Furthermore the Presence Server provides with a subscription authorization policy that is used to determine which watchers are allowed to subscribe to certain presence information. Also the Presence Server shall before subscription is accepted try to verify the identity of the watcher before the watcher subscribes to presence information. Optionally, depending on the implementation, the Presence Server may authenticate an anonymous watcher depending on the Subscription Authorization Policy.

A Presence List Server is responsible of storing grouped lists of watched presentities and enable a Watcher Application to subscribe to the presence of multiple presentities using a single SIP SUBSCRIBE transaction. The Presence List Server also stores and enables management of filters in the presence list, cf. Figure 1.

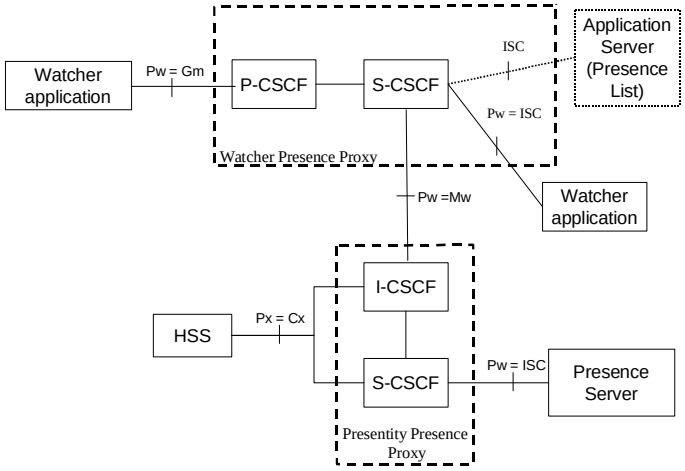

Figure 1: The Location of the Presence Server and the Presence List Server from an IMS point of view

A Presence User Agent shall be able to manage the data on the AS over the Ut interface, cf. 3GPP TS 23.002 [7], which is based on HTTP. This interface is not covered in 3GPP TS 33.203 [4] and it is mainly this interface for Presence use, which is covered in this specification. Before manipulation is allowed the user needs to be authenticated.

Note: In the text below the term Presence Server refers to both the Presence Server and the Presence List Server as depicted in Figure 1 above. For definitions of the Application Servers for Presence services the reader should consult 3GPP TS 23.141 [3]

The Ut interface needs the following security features:

1. it shall be possible to provide with mutual authentication between the Presence Server and the Watcher/Presentity;

2. a secure link and security association shall be established between the Presence Server and the Watcher/Presentity. Data origin authentication shall be provided as well as confidentiality protection.

Editors Note The specification need to consider [6], [8] and [9] and make appropriate profiling of these TLS protocols and the TLS version 1.1. need to be considered also.

Editors Note: The exact details of the security architecture is FFS and dependant on decisions related with the ongoing work on GBA (Generic Bootstrapping Architecture).

An overview of the security architecture for Presence Ut Interface is depicted in figure 2:

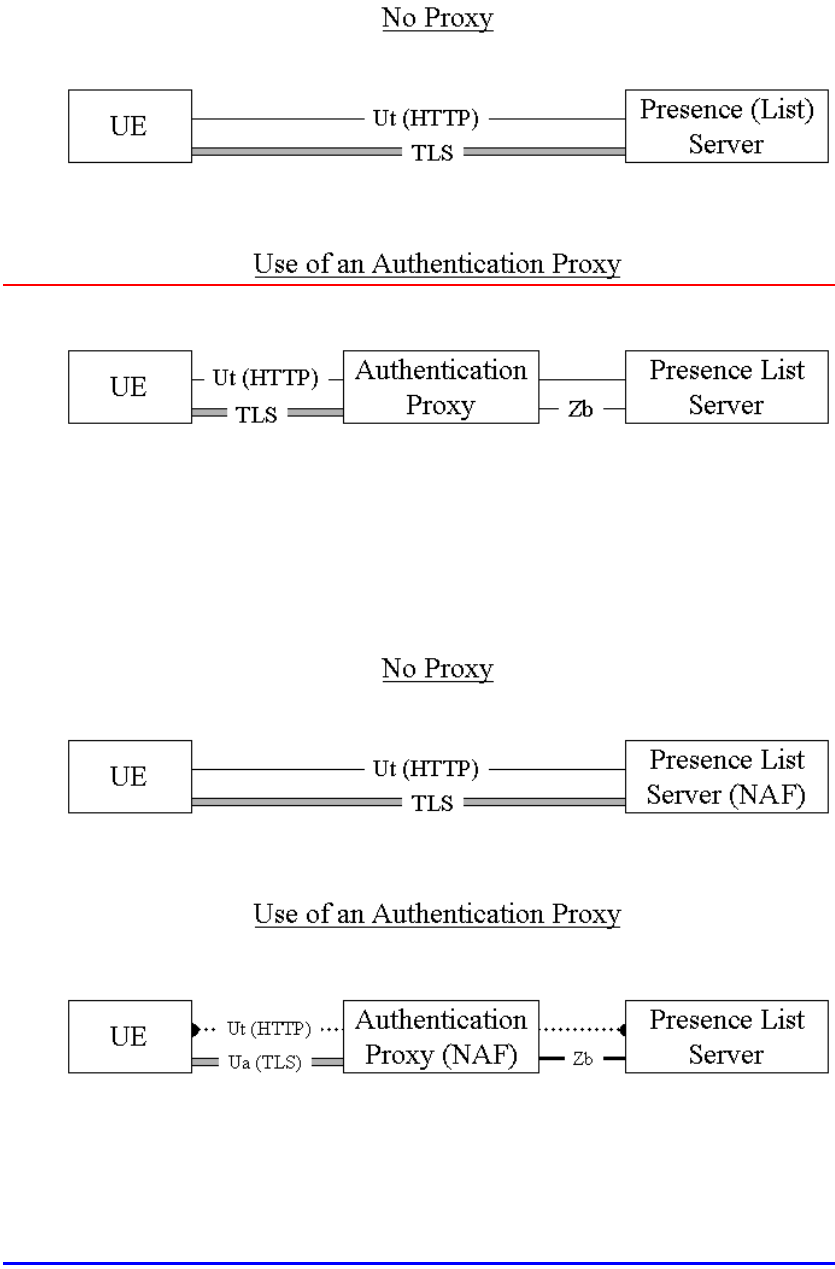

Figure 2: An overview of the Security architecture for the Ut interface including the support of an Authentication Proxy

Editors Note: The exact requirements on the Zb interface the use of NDS/IP for Presence Security are FFS.

5 Security features

5.1 Secure Access to the Presence Server~~/Presence List Server~~

5.1.1 Authentication of the subscriber and the network

A ~~user~~ subscriber shall be authenticated before accessing user data in a server. The ~~user~~ subscriber shall only be able to manipulate data that is associated with that particular subscriber~~user~~.

Editors note: Relationship between ~~TID~~Transaction Identifier and subscriber identity is ffs. In the case of Presence Ut interface, there are several potential identities that are related to ~~TID~~the Transaction Identifier, i.e. IMPI and IMPUs. The subscriber may have several Presence accounts related to same IMPI. ~~TID~~Transaction Identifier does not carry enough information on which IMPU the end-user is trying to use.

Authentication between the subscriber and the network shall be performed as specified in clause 6.1.

Subscriber authentication can be made by the operator using proprietary or non-3G standardized methods. ~~[Editors Note: An Editors note will be included in TR33.919 clarifying that an AS or an AP should decide on what parts of GAA shall be used if any. This might need to be reflected in this TS which is left FFS, cf. S3-030722].~~

In case 3GPP authentication mechanisms are used, the authentication of the subscriber shall be based on the USIM. The authentication of the subscriber and the network shall be based on Generic Authentication Architecture as defined in 3GPP TR 33.919 [15]. Generic Authentication Architecture enables the use of different authentication methods to be used for the authentication of the subcriber by using:

- subscriber certificates (e.g., TLS, cf. [6,8,9]), or
- shared secrets (e.g., TLS with HTTP Digest, cf. [17]).

The server certificate to be used for application server authentication shall be based on WAPCert [12].~~The authentication of the subscriber shall be based on the ISIM as defined in 3GPP TS 33.203 [4]. The authentication of the subscriber shall be HTTP based.~~

~~Editors Note: It is FFS what the detailed requirements are on profiling TLS. The following requirements are FFS:~~
~~*The Server is authenticated by means of asymmetric cryptography using a Server Certificate. The authentication of the Server shall be based on strong security. The use of anonymous Diffie Hellman is not allowed.*~~

NOTE: The interleaving attack shall not be possible.

~~Editors Note: The exact details on Server Certificate are FFS cf. X509v3 certificate and PKIX~~

~~Editors Note: It is FFS how the user is authenticated the methods that are FFS are:~~
~~A Presence Subscriber may be authenticated with the use of Subscriber Certificates~~
~~The use of TLS and Shared keys i.e. the IETF draft on Shared Key TLS~~
~~The use of Authentication Proxy is an option~~
~~The user can also be authenticated through the use of the BSF and the creation of a shared secret etc.~~

Editors Note: It is agreed that the shared key TLS draft need to be more mature in IETF before being considered for Presence. It is FFS and a decision is expected at SA3#32, cf. also S3-030721 and S3-030732.

Editors Note: If 3GPP decides that ISIM-only UICCs are allowed then it needs to be studied further if also the ISIM may be used in the Generic Authentication Architecture

A UE may contact the Presence Server/~~Presence List Server~~Presence Server for further instructions on authentication procedures.

The consumption of Authentication Vectors should be minimized. The architecture shall ensure that SQN synchronization failures is minimized.

5.1.2 Confidentiality protection

It shall be possible to apply~~The Ut interface shall be~~ confidentiality protection over the Ut interface ~~protected~~ using TLS and with~~using~~ effective key size of at least 128 bits. The terminal shall in the negotiation phase include protection alternatives that include at least one alternative with encryption algorithm support. The terminal and the server shall be able to resume a previous session and to perform an abbreviated handshake.

5.1.3 Integrity protection

The Ut interface shall be integrity protected. The terminal and the server shall be able to resume a previous session and to perform an abbreviated handshake.

5.1.4 Authentication Proxy

The ~~authentication proxy~~Authentication Proxy may reside between the UE and the Presence Server~~/Presence List Server~~ 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.

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

- ~~Authentication proxy~~Authentication Proxy ~~shall be able to~~may authenticate the UE using the means of Generic Bootstrapping Architecture.
- ~~Authentication proxy~~Authentication Proxy shall send the authenticated identity of the UE to the application server belonging to the trust domain at the beginning of new HTTP session.
- ~~Authentication proxy~~Authentication Proxy may not reveal the authenticated identity of the UE to the application server not belonging to the trust domain if required.
- 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~~Authentication Proxy towards different application servers.
- Activation of transfer of asserted user identity shall be configurable in the Authentication Proxy on a per AS base.
- Implementation of check of asserted user identity in the AS is optional.

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

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

NOTE 2: This requirement implies that the ~~authentication proxy~~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
- Terminal Configurability]

6 Security Mechanisms

The UE and the ~~AP/Server~~AP/Presence Server shall support the TLS version as specified in RFC 2246 [6] and WAP-219-TLS [13] or higher. Earlier versions are not allowed.

Editors Note: It is FFS if it is possible to base the Presence Security on TLSv1.1 [14], which is currently in draft status in IETF.

Note 1: The management of Root Certificates is out of scope for this Technical Specification

~~Editors Note: This should be a profiling of [6] and [8]~~

~~Editors Note: The clause 6 and 7 do not include much text. During the work with the security for Presence a TR was developed from which much of the content was moved to TS 33.203 Access Security for IMS Release 6. SA3 has an agreed working assumption on the use of TLS (some version of it). When the decision is taken there are no known issues available that should make it technically difficult to stabilise these clauses . The basis for this work is already outlined in S3-030749, which is approved in SA3 for inclusion in TS 33.222.~~

6.1 Authentication and key agreement

~~6.1.1 Authentication of the user~~6.1.1 Authentication of the ~~UE~~Subscriber

From a TLS point of view the UE shall be considered as un-authenticated, cf. RFC 2246 [6].

The authentication of the UE may take place in either the Authentication Proxy or the Server. However the AP or the Server may given the policy of the operator conclude that the ~~AP/Server~~AP/Presence Server shall not authenticate the UE using GBA i.e. the UE is considered as authenticated already or the UE is authenticated by other means.

Otherwise if the ~~AP/Server~~AP/Presence Server concludes that the authentication shall take place in the ~~AP/Server~~AP/Presence Server then the UE may be authenticated as specified in TS 33.220 [11] (where the Ua interface is between the UE and the ~~AP/Server~~AP/Presence Server).

It shall be possible for the operator at any time to request a re-authentication of an active UE.

Editors Note: A clean up what item is used for authentication purposes might be needed i.e. User, Subscriber and UE.

6.1.2 Authentication of the ~~AP/Server~~AP/Presence Server

The ~~AP/Server~~AP/Presence Server is authenticated by the Client as specified in WAP-219-TLS [13], which in turn is based on RFC 2246 [6].

The ~~AP/Server~~AP/Presence Server certificate profile shall be based on WAP Certificate and CRL Profile as defined in WAP-211-WAPCert [12].

6.1.3 Authentication Failures

If the UE receives a Server Hello Message from the ~~AP/Server~~AP/Presence Server 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/Server~~AP/Presence Server upon receiving this message may respond with a failure alert, however if the ~~AP/Server~~AP/Presence Server shall authenticate the UE as configured by the policy of the operator the ~~AP/Server~~AP/Presence Server 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 initated 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/Server~~AP/Presence Server 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/Server~~AP/Presence Server shall re-authenticate the UE and not give access to the ~~AP/Server~~AP/Presence Server unless the authentication was successful.

6.2 Protection~~Confidentiality~~ 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 ~~AP/Server~~AP/Presence Server 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 ~~AP/Server~~AP/Presence Server.

Editors Note: It is FFS is 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 [9] that shall be implemented in this TS

~~6.3 Integrity mechanisms~~

6.3 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 for Presence Services:

– 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

–

7 Security parameters agreement

7.1 Set-up of Security parameters

The TLS Handshake Protocol negotiates a session, which is identified by a Session ID. The Client and the ~~AP/Server~~AP/Presence Server 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.

7.2 Error cases

The ~~AP/Server~~AP/Presence Server shall consider the following cases as a fatal error:

– If the received ciphersuites only includes all or some of the Ciphersuites in Clause 6.4

– If the received ciphersuites do not include any integrity protection

If none of the received ciphersuites include encryption

–

– If the policy of the operator stipulates that encryption is required and the common set of supported ciphersuites only include key material less than 128 bits for confidentiality protection

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~~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 with an AP, the following two solutions could also be used to identify the host during the TLS handshaking phase:

1. Extension of TLS is specified in RFC 3546 [9]. This RFC supports the UE to indicate a virtual host that it intends to connect in the very initial TLS handshaking message;

2. 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 [17].

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.

Editors Note: The text in this informative annex may need to be revisited if changes in the main body of the text are made and when a final solution have been chosen.

Annex B (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
12-2003	SP-22	SP-030719	-	-	Presentation to TSG SA#22 for Information	0.3.1	1.0.0
02-2004	SA3#32	S3-040169			Text to empty the empty clauses 6 and 7 included. ISIM removed and changed to USIM.	1.0.0	1.1.0
03-2004	SA3#32	-			After email review over SA3 reflector some editorial changes were made. Included also an Editors Note on only ISIM application support on the UICC and its relation to GAA. Inclusion of TD S3-040069 in the informative Annex A as it was agreed to be included in the HTTPS TS.	1.1.0	1.1.1

3GPP TS 33.141 V1.1.1 (2004-03)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Presence Service;
Security
(Release 6)

Keywords
Security, Presence

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

This technical specification defines the security architecture and requirements for the presence services. Presence services enable the spreading of presence information of a user to users or services. A presence entity or presentity comprises the user, users devices, services and services components. It is the intention that this platform will enable new services like e.g. enhancement to chat, multimedia messaging, cinema ticket information, the score of a football game and so on.

A user has the possibility to control if her or his information shall be available to other users or services. This control is possible to achieve with high granularity e.g. explicitly define which user or users and services that shall have access to presence information.

A presentity is an uniquely identifiable entity with the capability to provide with presence information and it has only one principal associated with it. Hence a principal is distinct from all other principals and can be e.g. a human, organisation, program or even a collection thereof. One example of such a relation is when the presentity is a terminal and the principal of the terminal is the subscriber. A watcher is also an uniquely identifiable entity but with the aim to fetch or request information about a presentity. There are access rules that set the rules for the presence service how presence information gets available to watchers.

Presence information consists of a number of elements or presence tuples as defined in 3GPP TS 23.141 [3].

1 Scope

The present document describes the Stage 2 security requirements for the Presence Service, which includes the elements necessary to realise the requirements in 3GPP TS 22.141 [2] and 3GPP TS 23.141 [3].

The present document includes information applicable to network operators, service providers and manufacturers.

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 TR 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.141: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Presence Service; Stage 1".

[3] 3GPP TS 23.141: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Presence Service; Architecture and functional description".

[4] 3GPP TS 33.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Access security for IP-based services".

[5] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2".

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

[7] 3GPP TS 23.002: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; Network architecture".

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

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

[10] 3GPP TS 33.210: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security; IP network layer security".

[11] 3GPP TS 33.220: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

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

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

[14] IETF draft-ietf-tls-rfc2246-bis-05 (2003): "The TLS Protocol Version 1.1"

[15] 3GPP TR 33.919: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); System Description".

[16] 3GPP TS 24.cde: "3rd Generation Partnership Project; Technical Specification Group Core Network; Bootstrapping interface (Ub) and Network application function interface (Ua); Protocol details".

[17] IETF RFC 2818 (2000): "HTTP over TLS".

3 Definitions and abbreviations

3.1 Definitions

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

Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Data integrity: The property that data has not been altered in an unauthorised manner.

Data origin authentication: The corroboration that the source of data received is as claimed.

Entity authentication: The provision of assurance of the claimed identity of an entity.

Key freshness: A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply, 3GPP TR 21.905 [1] contains additional applicable abbreviations:

AKA	Authentication and key agreement
CSCF	Call Session Control Function
HSS	Home Subscriber Server
IM	IP Multimedia
IMPI	IM Private Identity
IMPU	IM Public Identity
IMS	IP Multimedia Core Network Subsystem
ISIM	IM Services Identity Module
MAC	Message Authentication Code
ME	Mobile Equipment
SA	Security Association
SEG	Security Gateway
SDP	Session Description Protocol
SIP	Session Initiation Protocol
UA	User Agent

4 Overview of the security architecture

An IMS operator using the CSCFs as Watcher Presence proxies and Presentity Presence proxies may offer the Presence services on top of the IMS network, cf. 3GPP TS 22.141 [2]. The access security for IMS is specified in 3GPP TS 33.203 [4] ensuring that SIP signalling is integrity protected and that IMS subscribers are authenticated through the use of IMS AKA. The security termination point from the UE towards the network is in the P-CSCF utilising IPsec ESP.

A watcher can be sending a SIP SUBSCRIBE over IMS towards the network to subscribe or to fetch presence information, i.e. the Presence Service supports SIP-based communications for publishing presence information. The presence information is provided by the Presence Server to the Watcher Application using SIP NOTIFY along the

dialogue setup by SUBSCRIBE. This traffic is protected in a hop-by-hop fashion using a combination of SEGs as specified in 3GPP TS 33.210 [10] with the access security provided in 3GPP TS 33.203 [4].

The Presence Server is responsible for managing presence information on behalf of the presence entity and it resides in the presentity's home network. Furthermore the Presence Server provides with a subscription authorization policy that is used to determine which watchers are allowed to subscribe to certain presence information. Also the Presence Server shall before subscription is accepted try to verify the identity of the watcher before the watcher subscribes to presence information. Optionally, depending on the implementation, the Presence Server may authenticate an anonymous watcher depending on the Subscription Authorization Policy.

A Presence List Server is responsible of storing grouped lists of watched presentities and enable a Watcher Application to subscribe to the presence of multiple presentities using a single SIP SUBSCRIBE transaction. The Presence List Server also stores and enables management of filters in the presence list, cf. Figure 1.

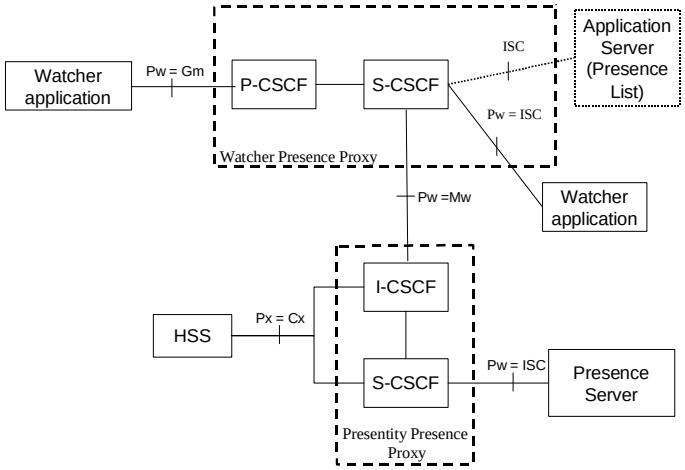

Figure 1: The Location of the Presence Server and the Presence List Server from an IMS point of view

A Presence User Agent shall be able to manage the data on the AS over the Ut interface, cf. 3GPP TS 23.002 [7], which is based on HTTP. This interface is not covered in 3GPP TS 33.203 [4] and it is mainly this interface for Presence use, which is covered in this specification. Before manipulation is allowed the user needs to be authenticated.

Note: In the text below the term Presence Server refers to both the Presence Server and the Presence List Server as depicted in Figure 1 above. For definitions of the Application Servers for Presence services the reader should consult 3GPP TS 23.141 [3]

The Ut interface needs the following security features:

1. it shall be possible to provide with mutual authentication between the Presence Server and the Watcher/Presentity;

2. a secure link and security association shall be established between the Presence Server and the Watcher/Presentity. Data origin authentication shall be provided as well as confidentiality protection.

Editors Note The specification need to consider [6], [8] and [9] and make appropriate profiling of these TLS protocols and the TLS version 1.1. need to be considered also.

Editors Note: The exact details of the security architecture is FFS and dependant on decisions related with the ongoing work on GBA (Generic Bootstrapping Architecture).

An overview of the security architecture for Presence Ut Interface is depicted in figure 2:

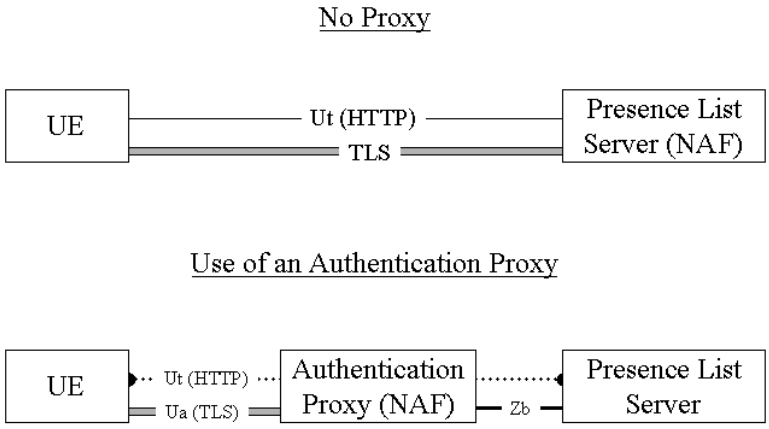

Figure 2: An overview of the Security architecture for the Ut interface including the support of an Authentication Proxy

Editors Note: The exact requirements on the Zb interface the use of NDS/IP for Presence Security are FFS.

5 Security features

5.1 Secure Access to the Presence Server

5.1.1 Authentication of the subscriber and the network

A subscriber shall be authenticated before accessing user data in a server. The subscriber shall only be able to manipulate data that is associated with that particular subscriber.

Editors note: Relationship between Transaction Identifier and subscriber identity is ffs. In the case of Presence Ut interface, there are several potential identities that are related to the Transaction Identifier, i.e. IMPI and IMPUs. The subscriber may have several Presence accounts related to same IMPI. Transaction Identifier does not carry enough information on which IMPU the end-user is trying to use.

Authentication between the subscriber and the network shall be performed as specified in clause 6.1.

Subscriber authentication can be made by the operator using proprietary or non-3G standardized methods. In case 3GPP authentication mechanisms are used, the authentication of the subscriber shall be based on the USIM. The authentication of the subscriber and the network shall be based on Generic Authentication Architecture as defined in 3GPP TR 33.919 [15]. Generic Authentication Architecture enables the use of different authentication methods to be used for the authentication of the subcriber by using:

- subscriber certificates (e.g., TLS, cf. [6,8,9]), or
- shared secrets (e.g., TLS with HTTP Digest, cf. [17]).

The server certificate to be used for application server authentication shall be based on WAPCert [12].

NOTE: The interleaving attack shall not be possible.

Editors Note: It is agreed that the shared key TLS draft need to be more mature in IETF before being considered for Presence. It is FFS and a decision is expected at SA3#32, cf. also S3-030721 and S3-030732.

Editors Note: If 3GPP decides that ISIM-only UICCs are allowed then it needs to be studied further if also the ISIM may be used in the Generic Authentication Architecture

A UE may contact the Presence Server/Presence Server for further instructions on authentication procedures.

The consumption of Authentication Vectors should be minimized. The architecture shall ensure that SQN synchronization failures is minimized.

5.1.2 Confidentiality protection

It shall be possible to apply confidentiality protection over the Ut interface using TLS and with effective key size of at least 128 bits. The terminal shall in the negotiation phase include protection alternatives that include at least one alternative with encryption algorithm support. The terminal and the server shall be able to resume a previous session and to perform an abbreviated handshake.

5.1.3 Integrity protection

The Ut interface shall be integrity protected. The terminal and the server shall be able to resume a previous session and to perform an abbreviated handshake.

5.1.4 Authentication Proxy

The Authentication Proxy may reside between the UE and the Presence Server 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.

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

- Authentication Proxy may authenticate the UE using the means of Generic Bootstrapping Architecture.
- Authentication Proxy shall send the authenticated identity of the UE to the application server belonging to the trust domain at the beginning of new HTTP session.
- Authentication Proxy may not reveal the authenticated identity of the UE to the application server not belonging to the trust domain if required.
- 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.
- Activation of transfer of asserted user identity shall be configurable in the Authentication Proxy on a per AS base.
- Implementation of check of asserted user identity in the AS is optional.

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

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
- Terminal Configurability]

6 Security Mechanisms

The UE and the AP/Presence Server shall support the TLS version as specified in RFC 2246 [6] and WAP-219-TLS [13] or higher. Earlier versions are not allowed.

Editors Note: It is FFS if it is possible to base the Presence Security on TLSv1.1 [14], which is currently in draft status in IETF.

Note 1: The management of Root Certificates is out of scope for this Technical Specification

6.1 Authentication and key agreement

6.1.1 Authentication of the Subscriber

From a TLS point of view the UE shall be considered as un-authenticated, cf. RFC 2246 [6].

The authentication of the UE may take place in either the Authentication Proxy or the Server. However the AP or the Server may given the policy of the operator conclude that the AP/Presence Server shall not authenticate the UE using GBA i.e. the UE is considered as authenticated already or the UE is authenticated by other means.

Otherwise if the AP/Presence Server concludes that the authentication shall take place in the AP/Presence Server then the UE may be authenticated as specified in TS 33.220 [11] (where the Ua interface is between the UE and the AP/Presence Server).

It shall be possible for the operator at any time to request a re-authentication of an active UE.

Editors Note: A clean up what item is used for authentication purposes might be needed i.e. User, Subscriber and UE.

6.1.2 Authentication of the AP/Presence Server

The AP/Presence Server is authenticated by the Client as specified in WAP-219-TLS [13], which in turn is based on RFC 2246 [6].

The AP/Presence Server certificate profile shall be based on WAP Certificate and CRL Profile as defined in WAP-211-WAPCert [12].

6.1.3 Authentication Failures

If the UE receives a Server Hello Message from the AP/Presence Server 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/Presence Server upon receiving this message may respond with a failure alert, however if the AP/Presence Server shall authenticate the UE as configured by the policy of the operator the AP/Presence Server 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 initated 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/Presence Server 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/Presence Server shall re-authenticate the UE and not give access to the AP/Presence Server unless the authentication was successful.

6.2 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 AP/Presence Server 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 AP/Presence Server.

Editors Note: It is FFS is 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 [9] that shall be implemented in this TS

6.3 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 for Presence Services:

- 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

7 Security parameters agreement

7.1 Set-up of Security parameters

The TLS Handshake Protocol negotiates a session, which is identified by a Session ID. The Client and the AP/Presence Server 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.

7.2 Error cases

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

- If the received ciphersuites only includes all or some of the Ciphersuites in Clause 6.4
- If the received ciphersuites do not include any integrity protection
- If none of the received ciphersuites include encryption
- If the policy of the operator stipulates that encryption is required and the common set of supported ciphersuites only include key material less than 128 bits for confidentiality protection

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 with an AP, the following two solutions could also be used to identify the host during the TLS handshaking phase:

1. Extension of TLS is specified in RFC 3546 [9]. This RFC supports the UE to indicate a virtual host that it intends to connect in the very initial TLS handshaking message;

2. 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 [17].

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.

Editors Note: The text in this informative annex may need to be revisited if changes in the main body of the text are made and when a final solution have been chosen.

Annex B (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
12-2003	SP-22	SP-030719	-	-	Presentation to TSG SA#22 for Information	0.3.1	1.0.0
02-2004	SA3#32	S3-040169			Text to empty the empty clauses 6 and 7 included. ISIM removed and changed to USIM.	1.0.0	1.1.0
03-2004	SA3#32	-			After email review over SA3 reflector some editorial changes were made. Included also an Editors Note on only ISIM application support on the UICC and its relation to GAA. Inclusion of TD S3-040069 in the informative Annex A as it was agreed to be included in the HTTPS TS.	1.1.0	1.1.1