Technical Specification Group Services and System Aspects **TSGS#22(03)0719**

Meeting #22, Hawaii, USA, 15-18 December 2003

Presentation of Specification to TSG

Presentation to:	**TSG SA Meeting #22**
Documents for presentation:	**TR 33.141, Version 1.0.0**
Presented for:	**Information**

Abstract of document:

SA WG3 is specifying the security for Presence Services. It should be noted that in parallel with this work the GAA is also specified. In particular there is a relation to TS 33.222 Access To Network Application Functions using HTTPS. However SA3 has come to an agreement that TS33.141 has higher priority and TS33.222 is more generic and hence not critical for Release 6. To avoid duplicate work in release 6, the HTTPS TS shall reference the Presence TS when appropriate. Also for future releases, the two Technical Specifications could be restructured when needed.

NOTE: During the work on Presence Security a TR was developed (TR 33.941) from which a number of CRs were derived that were implemented in TS33.203 the access security TS for IMS.

Changes since last presentation to SA Meeting:

This TR has not been presented to SA plenary before.

Outstanding Issues:

There are open issues but it is the view of SA3 that all of the open issues are possible to resolve according to the Release 6 timescales.

- The exact references to the Technical Specifications of GAA are FFS
- Some 3GPP related profiling of TLS RFC is still open
- The use of Shared Key TLS is FFS however SA3 aims to based on amongst other things the progress in IETF make a decision at the SA3#32 meeting
- Clauses 6 and 7 are empty however SA3 has agreed on a working assumption to implement TLS and the material in S3-030749 is agreed as a basis for future work.

Contentious Issues:

None.

3GPP TS 33.141 V1.0.0 (2003-12)

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

Copyright Notification

Contents

Foreword ... 4
Introduction ... 4
1 Scope ... 5
2 References ... 5
3 Definitions and abbreviations ... 5
3.1 Definitions ... 5
3.2 Abbreviations ... 6
4 Overview of the security architecture ... 7
5 Security features ... 8
5.1 Secure Access to the Presence Server/Presence List Server ... 8
5.1.1 Authentication of the subscriber and the network ... 8
5.1.2 Confidentiality protection ... 9
5.1.3 Integrity protection ... 9
5.1.4 Authentication Proxy ... 9
6 Security Mechanisms ... 10
6.1 Authentication and key agreement ... 10
6.1.1 Authentication of the user ... 10
6.1.2 Authentication of the Server ... 10
6.1.3 Authentication Failures ... 10
6.2 Confidentiality mechanisms ... 10
6.3 Integrity mechanisms ... 10
7 Security parameters agreement ... 10
7.1 Set-up of Security parameters ... 10
7.2 Error cases ... 10
Annex A (informative): Technical solutions for access to application servers via Authentication Proxy and HTTPS ... 11
Annex B (informative): Change history ... 12

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".

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 sending a SIP SUBSCRIBE over IMS towards the network subscribe to or 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.

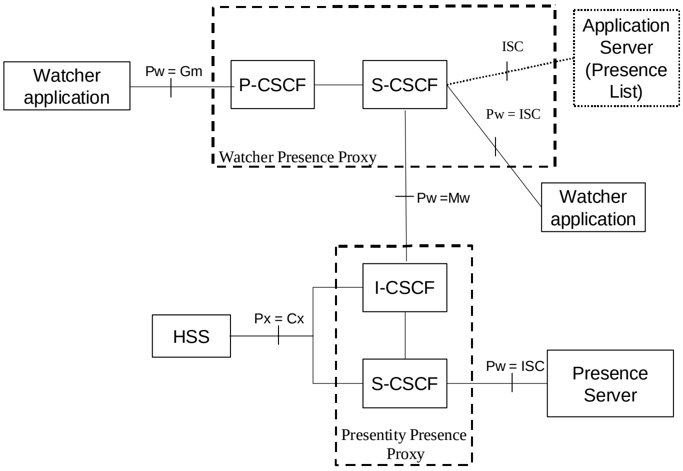

Figure 1: The Location of the Presence Server and the Presence List Server from an IMS point of view

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.

The Ut interface needs the following security features:

1. it shall be possible to provide with mutual authentication between the Server and the Watcher/Presentity;
2. a secure link and security association shall be established between the 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:

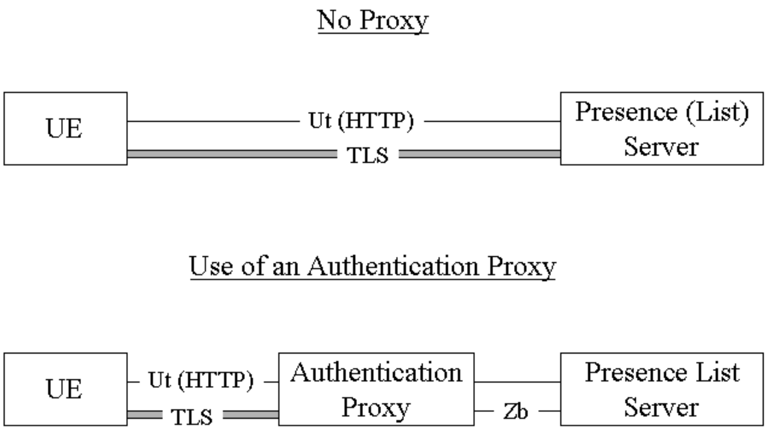

Figure 2: An overview of the Security architecture for the Ut interface including the support of an Authentication Proxy

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

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

[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].

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.

A UE may contact the Presence Server/Presence List 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

The Ut interface shall be confidentiality protected using TLS using effective key size of at least 128 bits. 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/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 shall be able to 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

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

6.1.2 Authentication of the Server

6.1.3 Authentication Failures

6.2 Confidentiality mechanisms

6.3 Integrity mechanisms

7 Security parameters agreement

7.1 Set-up of Security parameters

7.2 Error cases

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."

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

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