3GPP TS 33.cde V0.1.0 (2003-09)

Technical Report

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

GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS

Remove GSM logo from the cover page for pure 3rd Generation documents.

Select keywords from list provided in specs database.

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

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 [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: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.141: "Presence service; Stage 1".

[3] 3GPP TS 23.141: "Presence service; Stage 2".

[4] 3GPP TS 33.203: "3G security; Access security for IP-based services".

[5] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[6] IETF RFC 2246 (1999) “The TLS Protocol Version 1”

[7] 3GPP TS 23.002: "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: Network domain 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.

3.3 Abbreviations

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

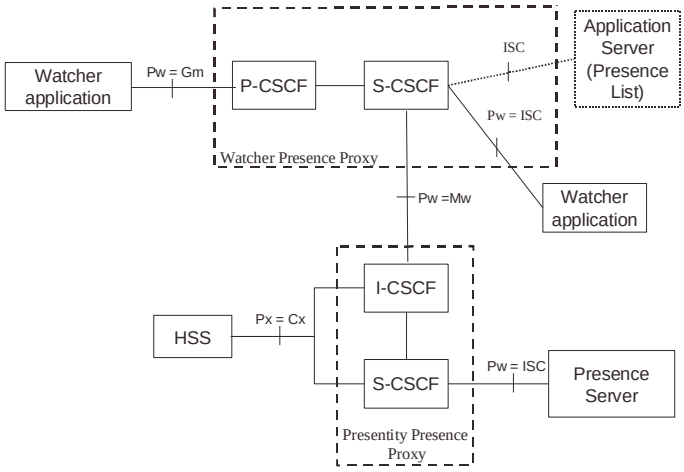
4 Overview of the security architecture

An IMS operator using the CSCFs as Watcher Presence proxies and Presentity Presence proxies may offer the Presence services on top the IMS network, cf. [2]. The access security for IMS is specified in [4] ensuring that SIP signalling is integrity protected and 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.

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 [10] with the access security provided in [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 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 below.



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

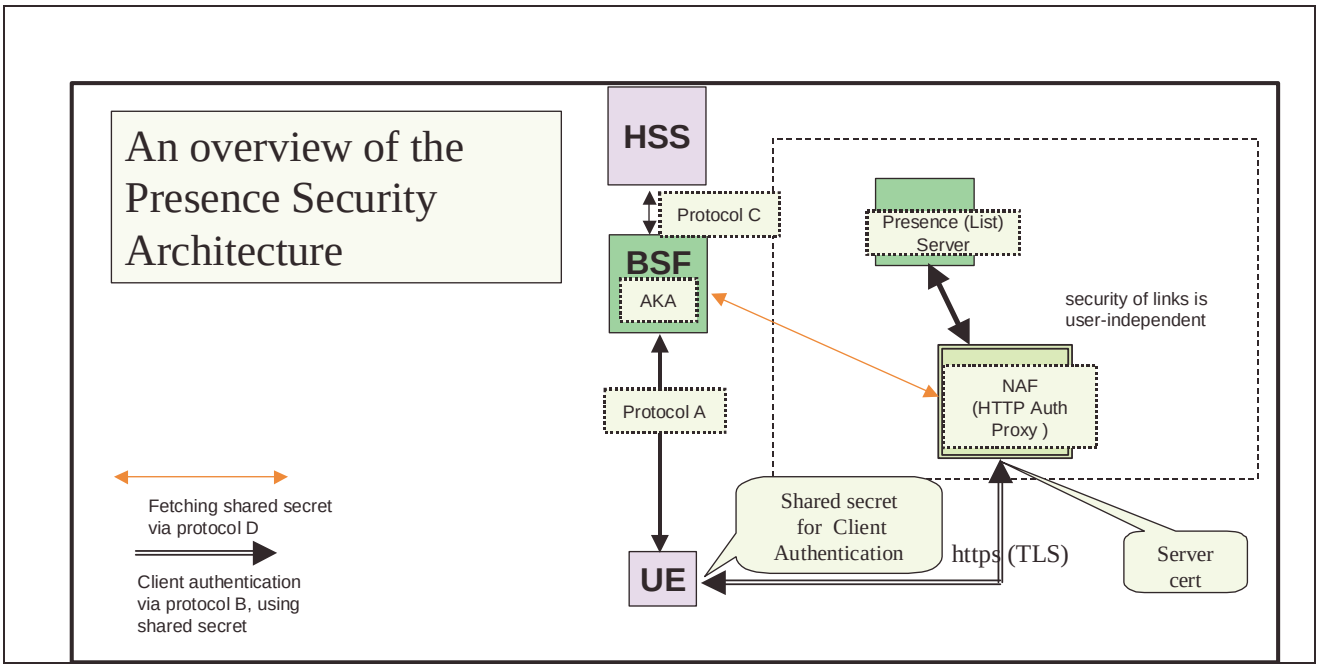
The Ut interface need to be protected as defined below:

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 is depicted in the figure below:



5 Security features

5.1 Secure Access to the Presence Server/Presence List Server

5.1.1 Authentication of the subscriber and the network

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

The authentication of the subscriber shall be based on the ISIM as defined in [4]. The authentication of the subscriber shall be HTTP based. The authentication of the subscriber shall not be based on asymmetric mechanisms.

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]

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.

6 Security Mechanisms

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

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

Annexes are only to be used where appropriate:

Annex <A>:
<Annex title>

Annexes are labeled A, B, C, etc. and are "informative"(3G TRs are informative documents by nature).

Annex <X>: Change history

It is usual to include an annex (usually the final annex of the document) for reports under TSG change control which details the change history of the report using a table as follows:

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2003-10	*SA3#30*	*SA3-020xxx*			*First Draft TS*		*0.1.0*