

3GPP2 X.S0027-002-0 v1.0

Version 1.0

Version Date: February 2008



**3RD GENERATION  
PARTNERSHIP  
PROJECT 2  
"3GPP2"**

## *Presence Security*

---

### *COPYRIGHT NOTICE*

*3GPP2 and its Organizational Partners claim copyright in this document and individual Organizational Partners may copyright and issue documents or standards publications in individual Organizational Partner's name based on this document. Requests for reproduction of this document should be directed to the 3GPP2 Secretariat at [secretariat@3gpp2.org](mailto:secretariat@3gpp2.org). Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. See [www.3gpp2.org](http://www.3gpp2.org) for more information.*

This page intentionally left blank.

## PRESENCE SECURITY

**CONTENTS**

8	REVISION HISTORY .....	iv
10	1 Scope .....	1
12	2 References .....	2
13	2.1 Normative References .....	2
14	2.2 Informative References .....	2
17	3 Definitions, Symbols and Abbreviations .....	3
18	3.1 Definitions .....	3
19	3.2 Symbols and Abbreviations .....	3
22	4 Overview of the security architecture .....	5
24	5 Security Features .....	7
25	5.1 Secure Access to the Presence Server over the Ut reference point .....	7
26	5.1.1 Authentication of the subscriber and the presence server .....	7
27	5.1.2 Confidentiality protection .....	7
28	5.1.3 Integrity protection .....	7
31	6 Security Mechanisms .....	8
32	6.1 Authentication .....	8
33	6.1.1 Authentication of the subscriber .....	8
34	6.1.2 Authentication of the Presence Server .....	8
35	6.1.3 Management of public user identities .....	8
36	6.1.4 Authentication Failures .....	8
37	6.2 Confidentiality protection .....	8
38	6.3 Integrity mechanisms .....	9
42	7 Security parameters agreement .....	10
43	7.1 Set-up of Security parameters .....	10
44	7.2 Error cases .....	10

## LIST OF FIGURES

---

<i>Figure 1</i>	The Location of the Presence Server and the Presence List Server from an IMS point of view	6
<i>Figure 2</i>	An overview of the Security architecture for the Ut interface .....	6

# FOREWORD

---

This Technical Specification has been produced by the 3rd Generation Partnership Project 2 (3GPP2) based on material contained in 3GPP specification TS 33.141-620.

This document contains portions of material copied from 3GPP document number(s) TS 33.141. The copyright on the 3GPP document is owned by the Organizational Partners of 3GPP (ARIB - Association of Radio Industries and Businesses, Japan; CCSA – China Communications Standards Association, China; ETSI – European Telecommunications Standards Institute; Committee T1, USA; TTA - Telecommunications Technology Association, Korea; and TTC – Telecommunication Technology Committee, Japan), which have granted license for reproduction and for use by 3GPP2 and its Organizational Partners.

## REVISION HISTORY

---

Revision	Content Changes	Date
1.0	Publication version	February 2008

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59

# 1 Scope

---

The present document describes the Stage 2 security requirements, security architecture, security features and security mechanisms for the Presence Service, which includes the elements necessary to realize the requirements in [20] and [3]. As far as SIP-based procedures are concerned, this specification refers to [4]. The main content of this specification is the security for the Ut reference point, which is HTTP-based, as applied in presence services.

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

## 2 References

---

### 2.1 Normative References

---

- [1] Void.
- [2] Void.
- [3] 3GPP2 X.S0027-001 v1.0: "Presence Service; Architecture and Functional Description".
- [4] 3GPP2 S.S0086-B v1.0: "3GPP2 IMS Security Framework".
- [5] 3GPP2 X.S0013-002-A v1.0: "IP multimedia subsystem; Stage 2".
- [6] IETF RFC 2246 (1999): "The TLS Protocol Version 1".
- [7] Void .
- [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] Void.
- [11] 3GPP2 S.S0109 v1.0: "Generic Bootstrapping Architecture"
- [12] Void.
- [13] Void.
- [14] IETF RFC 2246 (January, 1999): "The TLS Protocol Version 1.0".
- [15] Void
- [16] Void.
- [17] IETF RFC 2818 (2000): "HTTP over TLS".
- [18] IETF RFC 3310 (2002): "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)".
- [19] 3GPP2 S.S0114 v1.0: "Security Mechanisms using GBA".

### 2.2 Informative References

---

- [20] 3GPP2 S.R0062-0 v1.0: "Presence for Wireless Systems".

## 3 Definitions, Symbols and Abbreviations

---

### 3.1 Definitions

---

For the purposes of the present document the following definitions apply:

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

**Data integrity:** The property that data has not been altered in an unauthorized 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 authorized party.

### 3.2 Symbols and Abbreviations

---

For the purposes of the present document the following definitions apply:

AKA Authentication and key agreement

AS Application Server

BSF Bootstrapping Server Functionality

CSCF Call Session Control Function

ESP Encapsulating Security Payload

GBA Generic Bootstrapping Architecture

HTTP Hypertext Transfer Protocol

HTTPS HTTP over TLS

HSS Home Subscriber Server

IM IP Multimedia

IMPI IM Private Identity

IMPU IM Public Identity

IMS IP Multimedia Core Network Subsystem

IP Internet Protocol

ISIM IM Services Identity Module

MAC Message Authentication Code

ME Mobile Equipment

NAF Network Application Function

NDS	Network Domain Security
SA	Security Association
SDP	Session Description Protocol
SIP	Session Initiation Protocol
TLS	Transport Layer Security
UA	User Agent
UE	User Equipment

## 4 Overview of the security architecture

---

This technical specification defines the security architecture and defines the security features and security mechanisms for the presence services.

Presence services enable the dissemination of presence information of a user to other users or services. A presence entity or presentity comprises the user, user's devices, services and service 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 is made 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 have access to presence information.

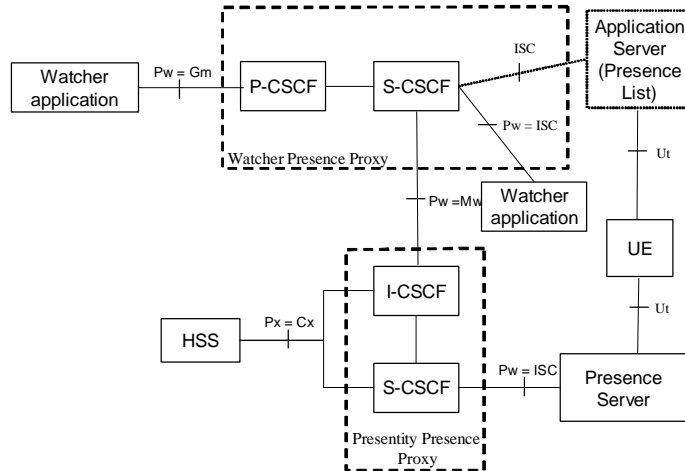
A presentity is an uniquely identifiable entity with the capability to provide the presence information and it has only one principal associated with it. Hence a principal is distinct from all other principals and can be e.g. a human, organization, program or even a collection thereof. One example of 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.

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, see [20]. The access security for IMS is specified in [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 set up by SUBSCRIBE. This traffic is protected in a hop-by-hop fashion as specified 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 a subscription authorization policy that is used to determine which watchers are allowed to subscribe to certain presence information. Also, prior to accepting the subscription request from a watcher, the presence server shall verify the identity of that watcher. 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 enables 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, see Figure 1.

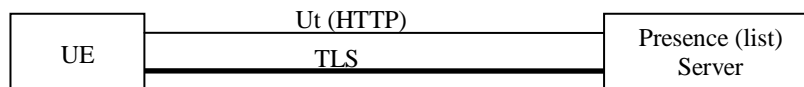


**Figure 1 The Location of the Presence Server and the Presence List Server from an IMS point of view**

A Presence User Agent shall be able to manage the data on the AS over the Ut interface, see [3], 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.

NOTE: 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 Presence Server and the Presence List Server see [3].

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**

## 5 Security Features

---

### 5.1 Secure Access to the Presence Server over the Ut reference point

---

#### 5.1.1 Authentication of the subscriber and the presence server

---

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 user.

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

#### 5.1.2 Confidentiality protection

---

It shall be possible to apply confidentiality protection over the Ut reference point.

#### 5.1.3 Integrity protection

---

The Ut interface shall be integrity protected.

## **6 Security Mechanisms**

---

The UE and the AP/Presence Server shall support the TLS version and profile as specified in clause 5 of [19].

### **6.1 Authentication**

---

#### **6.1.1 Authentication of the subscriber**

---

The authentication of the UE shall take place in the Presence server.

Subscriber authentication can be also performed by the operator using proprietary or non-3G standardized methods. A UE may contact the Presence Server for further instructions on authentication procedures, see initiation of bootstrapping in clause 4.5.1 of [11].

In case 3GPP2 authentication mechanisms are used, the authentication of the subscriber shall be based on the Generic Bootstrapping Architecture as defined in [11]. Generic Bootstrapping Architecture enables the use of different authentication methods to be used for the authentication of the subscriber by using shared secrets.

The authentication of the subscriber shall conform to the use of the Generic Bootstrapping Architecture, [11], for access to network application functions using HTTPS, as specified in [19].

#### **6.1.2 Authentication of the Presence Server**

---

Authentication of the Presence Server shall be performed according to clause 5 of [19].

#### **6.1.3 Management of public user identities**

---

The presence server, acting as a NAF in the sense of [11], may obtain identities related to the subscriber over the Zn reference point, as part of the GBA user security setting for presence, according to the policies of the BSF, see clause 4 and 5 of [11]. These identities may include the IMPI and several IMPUs. The UE shall send its preferred public user identity in each HTTP request. The Presence server shall then verify that the preferred identity inserted in the HTTP request by the UE is one of the IMPUs provided by the BSF.

#### **6.1.4 Authentication Failures**

---

The handling of authentication failures shall be according to clause 5 of [19].

### **6.2 Confidentiality protection**

---

If confidentiality protection is provided over the Ut interface, then it shall be provided using TLS and with effective encryption 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.

## 6.3 Integrity mechanisms

---

Integrity protection over the Ut reference point shall be provided using TLS and with 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.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59

## **7 Security parameters agreement**

---

### **7.1 Set-up of Security parameters**

---

Security parameters shall be set-up according to clause 5 of [19].

### **7.2 Error cases**

---

Error cases shall be handled as specified in clause 5 of [19]. In addition, the Presence Server shall consider the following cases as a fatal error:

- if none of the received ciphersuites include encryption and the policy of the operator stipulates that encryption is required;
- if the policy of the operator stipulates that encryption is required and the common set of supported ciphersuites only include key material less than the number of bits required by the operator for confidentiality protection.