ETSI TS 133 141 V9.0.0 (2010-02)

Technical Specification

Universal Mobile Telecommunications System (UMTS);
LTE;
Presence service;
Security
(3GPP TS 33.141 version 9.0.0 Release 9)

Reference

RTS/TSGS-0333141v900

Keywords

LTE, SECURITY, UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

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 gives an overview of 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 a 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, 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. However, the presence service is based on Public Identities, and consequently it is possible to have several terminals related to the same presentity. A watcher is also a uniquely identifiable entity but with the aim to fetch or request information about a presentity. There are access rules that set the rules for how presence information gets available to watchers.

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

1 Scope

The present document is the Stage 2 specification for the security requirements, security architecture, security features and security mechanisms for the Presence Service, which includes the elements necessary to realise the requirements in TS 22.141 [2] and TS 23.141 [3]. As far as SIP-based procedures are concerned, this specification refers to TS 33.203 [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

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; Architecture and functional description".

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

[5] Void

[6] Void

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

[8] Void

[9] Void

[10] 3GPP TS 33.210: "3G Security; Network Domain Security; IP network layer security".

[11] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[12] Void

[13] Void.

[14] Void

[15] 3GPP TR 33.919: "Generic Authentication Architecture (GAA); System description".

[16] Void

[17] Void

[18] Void

[19] 3GPP TS 33.222: " Generic Authentication Architecture (GAA); Access to network application functions using secure hypertext transfer protocol (HTTPS)".

[20] Void.

[21] 3GPP2 S.S0109-A v1.0: "Generic bootstrapping architecture"

[22] 3GPP2 S.S0114-A v1.0: "Security mechanisms using GBA"

[23] 3GPP TS 29.329: "Sh interface based on the Diameter protocol; Protocol details"

[24] 3GPP TS 24.109: "Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details

[25] 3GPP TS 23.003: "Numbering, addressing and identification".

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.

3.2 Abbreviations

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

AKA	Authentication and key agreement
AP	Authentication Proxy
APN	Access Point Name
AS	Application Server
BSF	Bootstrapping Server Function
CSCF	Call Session Control Function
ESP	Encapsulating Security Payload
GBA	Generic Bootstrapping Architecture
GGSN	Gateway GPRS Support Node
GIBA	GPRS-IMS-Bundled Authentication
HTTP	HyperText Transfer Protocol
HTTPS	HTTP over TLS
IM	IP Multimedia
IMPI	IM Private Identity
IMPU	IM Public Identity
IMS	IP Multimedia Core Network Subsystem
IP	Internet Protocol
IPsec	IP Security
ISIM	IM Services Identity Module
NAF	Network Application Function
NDS/IP	Network Domain Security for IP based Protocols
P-CSCF	Proxy Call Session Control Function
PDP	Packet Data Protocol
SEG	Security Gateway
SIP	Session Initiation Protocol
TLS	Transport Layer Security

4 Security architecture

4.1 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, see TS 22.141 [2]. The access security for IMS is specified in 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 may send 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 as specified in TS 33.210 [10] with the access security provided in 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 a subscription authorization policy that is used to determine which watchers are allowed to subscribe to certain presence information. Prior to accepting the subscription requests from watchers, the presence server attempts to verify the identities of the watchers. 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.

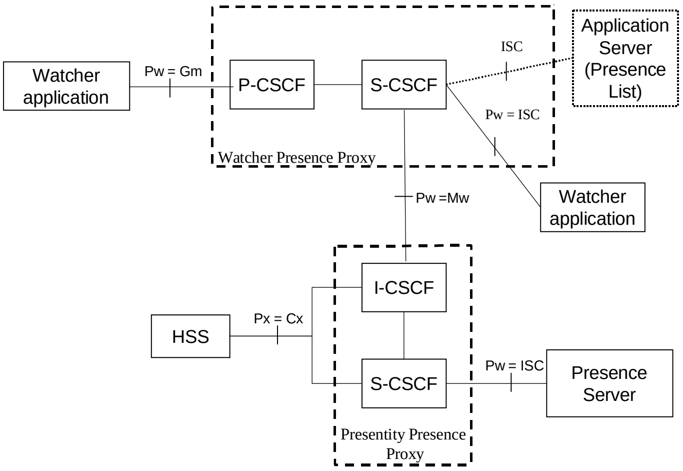

Figure 1: The Location of the Presence Server and the Presence List Server from an IMS point of view

4.2 The Ut reference point

A Presence User Agent shall be able to manage the data on the Presence Server and the Presence List Server over the Ut reference point, see TS 23.002 [7], which is based on HTTP. This reference point is not covered in TS 33.203 [4] and it is mainly this reference point 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 TS 23.141 [3].

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

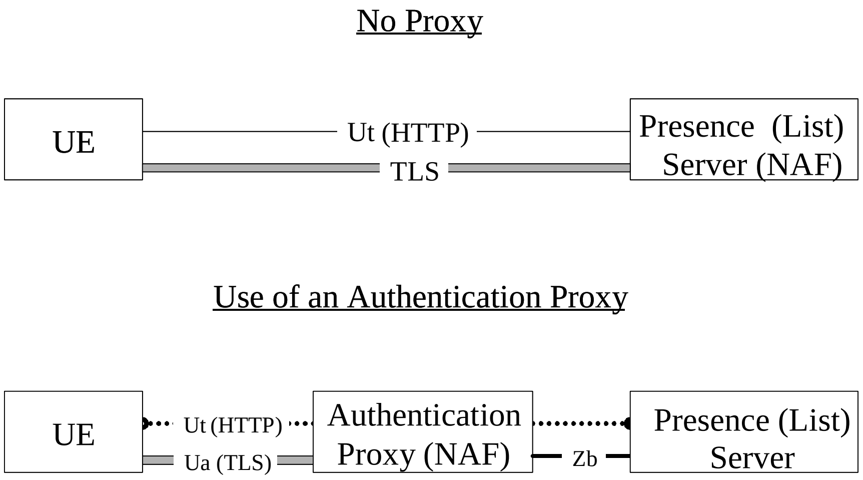
No Proxy
UE
Ut (HTTP)
TLS
Presence (List) Server (NAF)
Use of an Authentication Proxy
UE
Ut (HTTP)
Ua (TLS)
Authentication Proxy (NAF)
Zb
Presence (List) Server

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

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 subscriber. A subscriber shall authenticate the presence server.

Authentication between the subscriber and the presence server 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 reference point shall be integrity protected.

5.1.4 Authentication Proxy

The Authentication Proxy may reside between the UE and the Presence Server as depicted in figure 2. Its use is specified in TS 33.222 [19].

The following requirements apply for the use of an Authentication Proxy in addition to those in TS 33.222 [19]:

- Authentication Proxy may authenticate the UE using the means of Generic Bootstrapping Architecture, or it may use other means of authentication;
- if the AP uses the GBA for authentication of the UE, then the procedures shall conform to TS 33.222 [19].

Confidentiality and integrity protection may be provided for the interface between the AP and the AS, using the Zb interface of NDS/IP as specified in TS 33.222 [19].

6 Security Mechanisms for the Ut reference point

The UE and the AP/Presence Server shall support the TLS version and profile as specified in clause 5.3 of TS 33.222 [19].

6.1 Authentication and key agreement

6.1.1 Authentication of the subscriber

The authentication of the UE may take place in either the Authentication Proxy, see TS 33.222 [19], or 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/AP for further instructions on authentication procedures, see initiation of bootstrapping in clause 4.5.1 of TS 33.220 [11].

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

- subscriber certificates; or
- shared secrets.

For both cases, the authentication of the subscriber shall conform to the use of the Generic Authentication Architecture, TR 33.919 [15], for access to network application functions using HTTPS, as specified in TS 33.222 [19].

6.1.2 Authentication of the AP/Presence Server

Authentication of the AP/Presence Server shall be performed according to clause 5.3.1.3 of TS 33.222 [19].

6.1.3 Management of public user identities

The presence server, acting as a NAF in the sense of TS 33.220 [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 4.5.3 of TS 33.220 [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 (or AP) shall then verify that the preferred identity inserted in the HTTP request by the UE is one of the IMPUs, associated with the HTTP request, according to clause 6.5.2.4 of TS 33.222 [19].

If the presence server sits behind an AP and the verification of the preferred identity, which was inserted by the UE in the HTTP request, was successful, then the AP shall verify the value of the preferred identity of the user in the HTTP request before forwarding it to the presence server. How the asserted user identity is carried in each HTTP request is specified in the relevant stage 3 specification.

If there is no preferred identity inserted in the HTTP request, the AP shall insert a default IMPU from the user profile in the HTTP request, before forwarding it to the Presence server. If the validation of the UE inserted preferred identity fails in the AP the HTTP request shall be dropped.

6.1.4 Authentication failures

The handling of authentication failures shall be according to clause 5.3.1.4 of TS 33.222 [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 protection

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.

7 Security parameters agreement

7.1 Set-up of Security parameters

Security parameters shall be set-up according to clause 5.3.15 of TS 33.222 [19].

7.2 Error cases

Error cases shall be handled as specified in clause 5.3.1.6 of TS 33.222 [19]. In addition, the AP/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.

Annex A:
Void

Annex B (informative): Void

Annex C (normative): Requirements specific to 3GPP2 Access

C.1 General

This Annex describes how the normative text in the main body of this specification differs for 3GPP2 Access.

C.2 Authentication of the subscriber

The text in clause 6.1.1 is replaced by the following text.

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

Subscriber authentication may be performed by the operator using proprietary or non-3G standardized methods. GBA defined in [21] may also be used. The UE may contact the Presence Server for further instructions on authentication procedures, see initiation of bootstrapping in 3GPP2 S.S0109 [21].

In case GBA is used for authentication, the authentication of the subscriber shall be based on the Generic Bootstrapping Architecture as defined in [21]. 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 with GBA shall conform to Generic Bootstrapping Architecture, [21], for access to network application functions using HTTPS, using TLS with pre-shared keys as specified in [22].

C.3 Authentication of the Presence Server

The text in clause 6.1.2 is replaced by the following text.

Authentication of the Presence Server shall be performed using TLS with pre-shared keys as specified in [22].

C.4 Management of public user identities

The text in clause 6.1.3 is replaced by the following text.

The presence server, acting as a NAF in the sense of GBA, 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 [21]. 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.

C.5 Authentication failures

The text in clause 6.1.4 is replaced by the following text.

The handling of authentication failures when using TLS with pre-shared keys shall be according to [22].

C.6 Set-up of Security parameters

The text in clause 7.1 is replaced by the following text.

Security parameters shall be set-up using TLS with pre-shared keys as specified in [22].

C.7 Error cases

The text in clause 7.2 is replaced by the following text.

Error cases when using TLS with pre-shared keys shall be handled as specified in [22]. 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.

Annex D (normative): GPRS-IMS-Bundled Authentication for Ut interface security

The GIBA solution [4] may be re-used to protect HTTP services based on the secure IP address binding information stored in the HSS as an alternative to the mechanism specified in the main body of this specification. To achieve this, the Sh interface [23] shall be re-used by the Application Server (AS) to fetch secure IP address binding information from the HSS.

This approach requires the HTTP services to use the same APN as the GIBA service, and that all active PDP contexts, for a single UE, associated with that APN use the same IP address (or the prefix in the case of IPv6 stateless autoconfiguration) at any given time. This approach also requires the GGSN to be in the home network. The mechanism assumes that the GGSN does not allow a UE to successfully transmit an IP packet with a source IP address (or prefix) that is different to the one assigned during PDP context activation.

Since the security of this approach relies on the security of the PS bearer, a dependency is created between the HTTP service and the PS bearer, which does not exist with the mechanism specified in the main body of this specification. This means that the solution described in this section does not provide as high a degree of access network independency as the solution in the main body of this specification. In particular, the solution does not currently support scenarios where HTTP services are offered over WLAN.

The following steps describe the procedure:

1) The UE sends the HTTP GET request to the AS. The "X-3GPP-Intended-Identity" header, as defined in TS 24.109 [24], shall be used by the UE to indicate the user identity. The user is identified by the IMPU that is derived from the IMSI of the subscription according to the rules in TS 23.003 [25].

2) The AS decides to authenticate the UE based on the secure IP address binding information from the HSS. This decision might be based on the fact that GBA is not available. The AS checks whether secure IP address binding information is available at the AS; if yes, it proceeds with step 7, if not then it proceeds with step 3.

3) The AS queries the HSS using User-Data-Request (UDR) over the Sh interface, and the IMPU is used for User-Identity.

4) The HSS responds with User-Data-Answer (UDA) including the secure binding information. If a securely bound IP address is not available in the HSS, then any incoming HTTP requests at the AS shall be rejected.

5) The AS stores the secure binding information.

6) The AS uses the subscriber/notify feature on the Sh interface to ensure that it is informed about any changes in the secure IP address binding information in the HSS. If the AS is notified by the HSS about such a change, it updates the secure IP address binding information stored in the AS accordingly.

7) The AS shall check that the IP address (or prefix) from the UE in HTTP requests matches the IP address (or prefix) provided by the HSS, otherwise the HTTP request shall be rejected.

The mechanism does not preclude that the HTTP service may run inside a server-authenticated TLS tunnel established between the UE and the AS. However, support of TLS in the UE and in the AS is not mandated in this document.

Editor"s note: The correct stage 3 reference needs to be added in the paragraph below once the stage 3 details have been specified.

The details for the interface between the AS and HSS are described in [tba].

Annex E (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
05-2004	SP-24	SP-040367	-	-	Revision marks removed and editorial updated for Presentation for Approval	1.2.1	2.0.0
06-2004	SP-24	-	-	-	Approved at TSG SA #24. Published version 6.0.0	2.0.0	6.0.0
09-2004	SP-25	SP-040617	001	-	ISIM used in GBA	6.0.0	6.1.0
09-2004	SP-25	SP-040617	002	-	Further modifications to TLS profile related text in 33.141	6.0.0	6.1.0
09-2004	SP-25	SP-040617	003	-	Editorial cleanup of TS 33.141	6.0.0	6.1.0
09-2004	SP-25	SP-040617	004	-	Clarification on Ut interface	6.0.0	6.1.0
2005-09	SP-29	SP-050561	0005	-	Addition of reference to early IMS security TR	6.1.0	6.2.0
2005-12	SP-30	SP-050654	-	-	Raised to Rel-7 to allow reference by TISPAN	6.2.0	7.0.0
2006-06	SP-32	SP-060388	0006	-	Editorial Changes	7.0.0	7.1.0
2008-06	SP-40	SP-080428	0007	4	Changes to support common IMS between 3GPP and 3GPP2	7.1.0	8.0.0
2008-09	SP-41	SP-080485	0009	2	New normative Annex on GPRS-IMS-Bundled Authentication for Ut interface security	8.0.0	8.1.0
2008-09	SP-41	SP-080485	0008	1	Removing annex B of TS 33.141	8.0.0	8.1.0
2009-12	-	-	-	-	Update to Rel-9 version (MCC)	8.1.0	9.0.0

History

Document history		
V9.0.0	February 2010	Publication