3GPP TR 33.cde V0.56.0 (2003-0609)

Technical Report

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

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 Report 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 TR defines the security architecture, trust model 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 description (security architectural solution and functionalities) for the Presence Service, which includes the elements necessary to realise the stage 1 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] Common Presence and Instant Messaging (CPIM) Presence Information Data Format, Internet Draft http://www.ietf.org/internet-drafts/draft-ietf-impp-cpim-pidf-05.txt, May 2002

Editor's note: The above document is not yet published as an RFC, where possible the reference should be converted to an RFC prior to approval should this document be converted to a Technical Specification.

[5] Session Initiation Protocol (SIP) Extensions for Presence, Internet-Draft http://www.ietf.org/internet-drafts/draft-ietf-simple-presence-07.txt, May 2002

Editor's note: The above document is not yet published as an RFC, where possible the reference should be converted to an RFC prior to approval should this document be converted to a Technical Specification.

[6] 3GPP TS 33.203: "3G security; Access security for IP-based services".

[7] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[8] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[9] IETF RFC 3265: "Session Initiation Protocol (SIP) Event Notification"

[10] A SIP Event Package for List Presence, Internet-Draft, http://search.ietf.org/internet-drafts/draft-ietf-simple-presencelist-package-00.txt, June 2002

Editor's note: The above document is not yet published as an RFC, where possible the reference should be converted to an RFC prior to approval should this document be converted to a Technical Specification.

[11] IETF RFC 2778: "A Model for Presence and Instant Messaging".

[12] IETF RFC 2779: "Instant Messaging / Presence Protocol Requirements".

[13] IETF RFC 2406 (1998) "IP Encapsulating Security Payload (ESP)".

[14] IETF RFC 2401 (1998) "Security Architecture for the Internet Protocol".

[15] RFC 2451 (1998): "The ESP CBC-Mode Cipher Algorithms".

[16] RFC 3329 (2003): "Security Mechanism Agreement for the Session Initiation Protocol".

[17] Draft-ietf-sip-privacy-general-01: A Privacy Mechanism for the Session Initiation Protocol (SIP), June 6, 2002.

[18] Draft-ietf-sip-asserted-identity-02: Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Network, June 21, 2002.

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

3 Definitions, symbols and abbreviations

Delete from the above heading those words which are not applicable.

Subclause numbering depends on applicability and should be renumbered accordingly.

3.1 Definitions

For the purposes of the present document, the [following] terms and definitions [given in ... and the following] apply.

Definition format

***<defined term>**: <definition>.*

example: text used to clarify abstract rules by applying them literally.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

Symbol format

<symbol> <Explanation>

3.3 Abbreviations

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

Abbreviation format

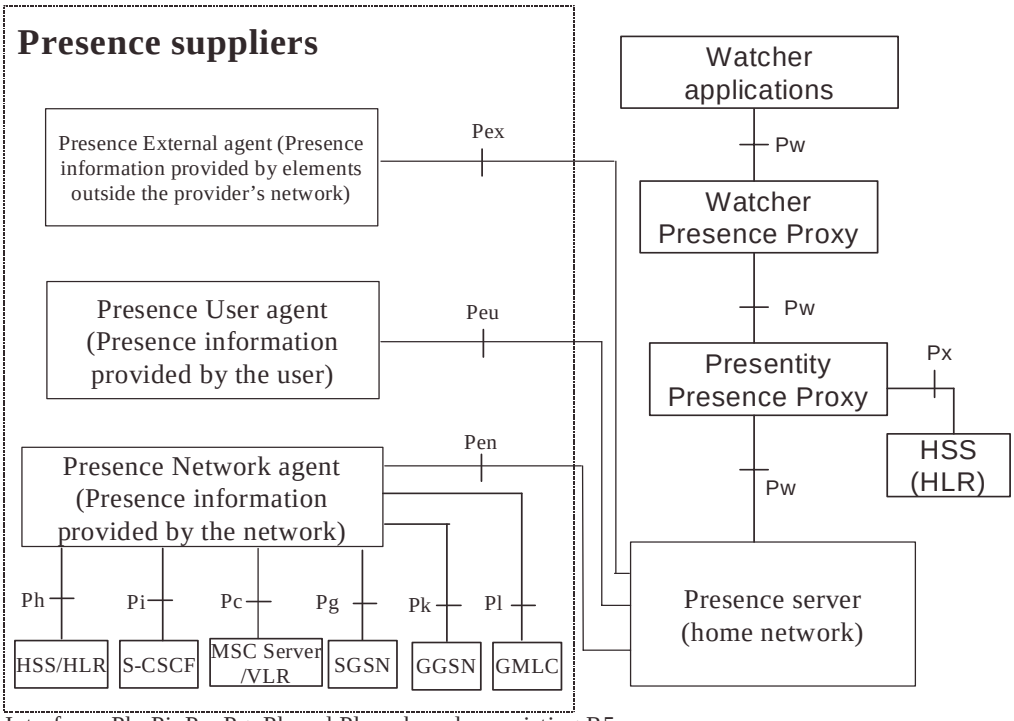
<ACRONYM> <Explanation>

4 Security Requirements for Presence Service

In this section some important requirements that will or may affect the security solutions for presence are identified.

4.1 Roles in Presence Architecture

In this section the different roles that come into play for presence are identified and described.



Interfaces Ph, Pi, Pc, Pg, Pk and Pl are based on existing R5 procedures e.g. CAMEL, MAP, CAP, RADIUS, ISC, Cx, Sh.

Figure 1 Overview of the presence architecture

The architecture as defined in [3] to support presence service contains a number of roles. This architecture is very general in nature and it can be applied on e.g. IMS.

The following roles have been identified which substantiates the development of the security architecture for Presence:

1. Information sources - Suppliers
    a. External Presence Supplier (External Agent)
    b. User Agent Presence Supplier (Presence UA)
    c. Network Presence Suppliers
        i. HSS
        ii. S-CSCF
        iii. MSC/VLR
        iv. SGSN
        v. GGSN
        vi. GMLC
2. Information sinks
    a. Watcher applications in terminals (fetcher or subscriber)
    b. Watcher applications in Application Servers (fetcher or subscriber)
    c. Presence Server
3. Information proxy provider
    a. Watcher presence proxy
    b. Presentity Presence proxy
4. Customer
    a. Principal
    b. Watcher
5. Attacker

A user shall be able manage his or her data on the AS (Presence Servers) e.g.:

- Lists on the presence list server
- Access lists on the presence server
- Buddy lists for chat (IMS messaging)
- IMS Group Management
- Conference settings: creation, data, type, participants, …

The reference point Ut between UE and AS for this manipulation is based on HTTP. The functional architecture for the management of the user's service related information is depicted in the figure below:

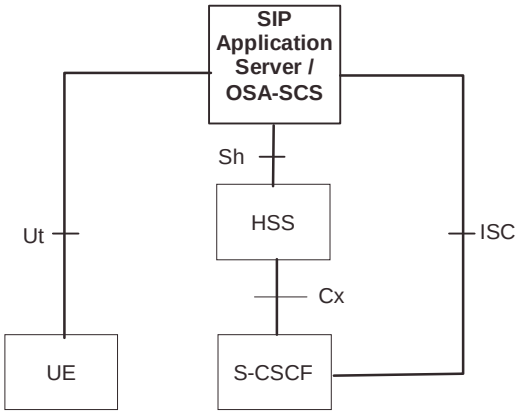


Figure 2 Overview of the functional architecture for the management of user information from the UE

[Editors Note: It is FFS what security architecture to use over the Ut reference point ~~it could e.g. be based on TLS and/or on AKA~~. It is also FFS whether the authentication in IMS can be re-used. ~~The mechanisms that are given priority include AKA (or the AKA architecture) and TLS.~~ An important aspect to consider is the interleaving attack.

The proposals that have been discussed include:

1. *Base it on IMS Registrations, new key management procedures and base the protection on HTTPS*
2. *Use of AKAv2 and Authentication proxy and TLS*
3. *Use of Bootstrapping function for HTTP AKA using TLS]*

The security protocol to be used over the Ut interface shall be based on TLS, cf. [19].

4.1.1 Watcher application

- An application that can request and obtain presence information
- In IMS a watcher application can be located in the UE registered and the UE is registered in the S-CSCF
- In IMS a watcher application cab be located in an AS behind an ISC interface

4.1.2 Watcher presence proxy

- Authenticates the Watcher
- Generates accounting information

4.1.3 Presentity Presence Proxy

- Generates accounting information
- Determines the identity of the presence server

4.1.4 Presence Server

- Transforms presence related information from different sources to on single presence document
- Allows user to subscribe and fetch presence information
- Provides with presence information to any watcher application
- Provides with presence information to allowed watcher applications specified in a list

4.1.5 Presence User Agent

- Sends presence information to the presence server
- Manages Access Rules
- Can be located in the UE
- Can be located in the network e.g. for SMS or WAP scenario

4.1.6 Network Agent

- May receive presence information from HSS, S-CSCF, MSC, SGSN, GGSN and GMLC
- Sends presence information to the Presence Server in the Home Network

4.1.7 External Agent

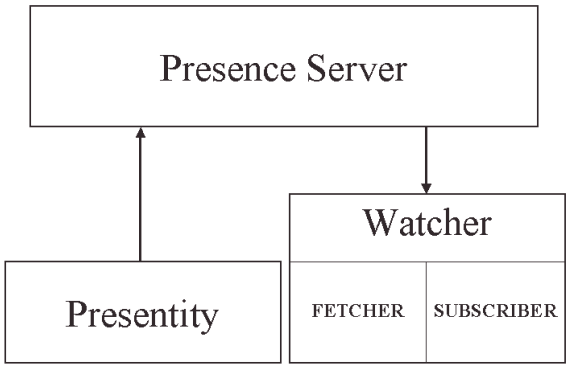
- Supplies presence information from external networks
- Sends presence information to the Presence Server in the Home Network

4.2 Scenarios and assets

The scenarios below are basically taken from [RFC2778]:

- The Presence Server accepts, stores and distributes presence information
- The Watcher receives presence information from the presence server
- The Presentity provides with presence information

Here it has not been given from what sources apart from the Presentity that provide with information to the Presence Server. According to [RFC2778] the Presence Server (or Presence Service) has Watcher information as well. This information is based on what activities the Watcher is undertaking e.g. acting as a fetcher (i.e. poller) or subscriber. The presence server may also distribute watcher information to watchers. Whenever the presence information is changed it is distributed to subscribers, cf. figure below.



In order to identify the threats and security requirements we need to identify the assets in presence.

The information that is the key asset in the presence service is of course the presence information. This information is used by watchers e.g. watcher applications. It seems that in order for the presence server to 'sell' presence information it should be available, reliable and accurate. If the presence server cannot guarantee this it could mean that the reputation of the presence server owner could be damaged. Furthermore since external 3rd parties can also provide with information to the presence server a general business model means that also these players would regard their information as an asset in particular if the information is based on raw data which is gathered and processed. Hence the identified assets are:

- The Presence and Watcher Information – especially the aspects related to user privacy. This asset is assumed to be very valuable for the user.
- The reputation of the owner of the Presence Server
- The Presence Information gathered and supplied by Suppliers

What is interesting is how these assets are exchanged i.e. between what Roles and over what interfaces.

4.3 Trust model

The Presence Server is the central node in the Presence architecture. It will receive and manage information from different sources. The Presence Server shall authorise who can get access to what information. Clearly everyone in the system shall trust the Presence Server.

The network nodes that provide information via the Presence Network Agent either reside in the Visited Network or in the Home Network. It is reasonable to adopt the existing trust model we have in e.g. R'99 where the SGSN is trusted to authenticate a 3G subscriber via the roaming agreement. It seems therefore fair to assume that the information provided by those network elements can be trusted i.e. that both the HN and the VN can ensure that non-authorised entities cannot tamper with the data in the node. Hence the Presence Server trusts the Network Presence Suppliers, the Presentity Presence Proxy and the Watcher Presence Proxy.

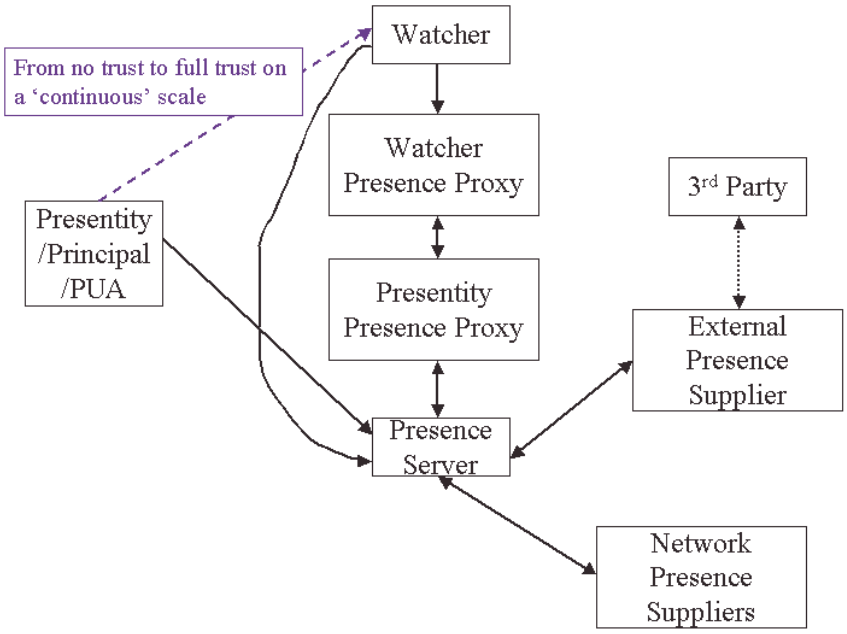
The Presence User Agent supplies the presentity information to the Presence Server and it will also manage the access rules. From the presentity point of view there will be a number of watcher applications that request or subscribe to presence information. Some of these watchers may be known to the Presentity e.g. friends or colleagues whereas others are not known beforehand or are even anonym. Since the presence information will potentially reveal sensitive information about the Presentity e.g. user status and location, not all the watchers are trusted by the presentity. Some watchers are only trusted to the extent that they can get information about user status but not location. Hence the trust of the presentity to a watcher might be total, non-existing or anything in between.

A Watcher Presence Proxy will proxy information between the Watcher and the Presence Server in both directions. The proxy will generate billing and charging information and has a relationship with the Watcher e.g. in terms of a subscription. A Watcher shall trust a Watcher Presence Proxy although the proxy might very well be distributed in the Visited Network and the Home Network.

The Watcher Presence Proxy shall proxy the information towards the Presence Server via a Presentity Presence Proxy. Clearly these two nodes need to trust each other.

The following trust relationships between the roles that are participating in Presence are then proposed based on the above (as captured in the figure below):

- The Presence Server trusts the Network Presence Suppliers
- The Presence Server trusts the Presentity Presence Proxy
- The Presence Server trusts the Watcher Presence Proxy
- All Roles (modulo the Attacker) trust the Presence Server
- The Principal may have no trust, low trust, medium trust (scale not to be defined!) or trust in Watchers
- The Watcher trusts the Watcher Presence Proxy
- The Watcher trusts the Presence Server
- The Watcher Presence Proxy trusts the Presentity Presence Proxy



It is assumed that a 3rd party is not necessarily situated in a 3G network and therefore no trust establishment has been stated here. Presumably any operator setting up a relationship with a 3rd party needs to ensure that necessary considerations around trust and security measures are considered.

4.4 Threats

[Editors Note: In this section different potential threats that need to be mitigated should be stated.]

An attacker eavesdrops, modifies, masquerades, replays or performs Denial of Service Attacks over the different P-Interfaces.

- It is estimated that with low probability that the attacker can succeed with any of these attacks over the Ph, Pi, Pc, Pg, Pg, Pl, Pk, and Px Interfaces .
- It is estimated that the attacker with higher probability can succeed with any of these attacks over the Peu, Pen, Pex and the Pw Interface if no security measures are used.

These attacks modulo Denial of Service attacks would have the following impacts if they succeed:

- Eavesdropping would have an impact on the Privacy asset
- If an attacker modifies the Presence information then it would impact on the Reputation of the Presence Server owner since the information would no longer be accurate nor reliable.
- If an attacker replays Presence information it would also impact on the Reputation of the Presence Server owner since the information would no longer be accurate nor reliable.
- If the Attacker succeeds to masquerade as being a valid Presentity the Privacy of that Presentity is impacted as well as the Reputation of the Presence Server owner
- If the Attacker succeeds to masquerade as being a valid and trusted Watcher the Privacy asset is impacted

It is estimated that with high probability the Attacker can interfere with the interface between the 3rd party and the Presence External Agent if no security measures are installed

- Eavesdropping would have an impact on the Privacy asset

If an attacker modifies the Presence information then it would impact the Reputation of the Presence Server owner since the information would no longer be accurate nor reliable

4.5 Requirements

4.5.1 General

The use and access to the presence service shall be supported in a secure manner. It shall only be possible for the presence information to be supplied and/or updated by the presentity or the home environment.

The presence service shall support measures to detect and prevent attempts to maliciously use or abuse the services. It shall be possible to authenticate presentities and/or watchers at any time.

It shall be possible to authenticate a principal before allowing registration to the presence service.

It shall be possible to authenticate a watcher requesting access to the presence service. Existing security mechanisms as well as mechanisms specific to presence service may be used.

It shall be possible to authorise a watcher's watcher-subscription request to a presentity's presence information.

It shall be possible to protect the following items from attacks (e.g., eavesdropping, tampering, and replay attacks):

- Presence information and notifications
- Requests for presence information, e.g., requests for subscription and requests for presence information retrieval.

[Editors Note: These requirements above are copied from [3] and require a review and updates]

There is a need to protect the Peu and the Pw interfaces with security measures offering confidentiality, integrity as well as replay protection. The need for similar security in Pen and Pex interfaces in for further study. Furthermore since using a 'continuous' scale the Presentity shall be able to set access rules in a general way such that it can decide what information shall be available to what Watcher. This shall include that the Presentity shall be able to control the authenticity of a watcher i.e. that the information is controlled via e.g. a password based mechanism. Such a password mechanism is optional. The Presentity if it desires shall also be notified and even to authorise end-to-end Watchers. The Presentity shall also have the possibility to check what watchers have received what presence information from a Presence Server.

These high-level requirements are collected in the following list:

1) The Peu interface shall be integrity protected, confidentiality protected and offer replay protection.
2) The Pw interface shall be integrity protected, confidentiality protected and offer replay protection. Anonymity services shall be provided.
3) The Presentity shall be able to set the access rules in a general manner in the Presence Server for all Watchers
4) The Presentity should be able to require that a Watcher shall be authenticated in the Presence Server

5) The Presentity should be able to authorise a Watcher request end-to-end

6) The Presentity should be able to have access to a log

In addition to the previous requirements, the Pen and Pex interfaces may require integrity and replay protection.

4.5.2 IMS related

The following working assumptions related to Presence have been defined:

1) Peu: Existing IMS security architecture fulfils the security requirements related to integrity protection, replay protection and anonymity.

2) Ph: No additional security requirements.

3) Pi: No additional security requirements.

4) Pc: No additional security requirements.

5) Pg: No additional security requirements.

6) Pk: No additional security requirements.

7) Pl: No additional security requirements.

8) Pw: Existing IMS security architecture fulfils the security requirements related to authentication, integrity protection and replay protection.

9) Peu & Pw: IMS needs to be enhanced by IPsec encryption between UE and P-CSCF in order to fulfil the confidentiality requirement. The confidentiality protection mechanism is mandatory to implement in UE and P-CSCF. P-CSCF shall decide whether the IPsec encryption or the underlying network layer encryption is used based on the local network security policy

10) Pw: IMS is enhanced by a security mechanism for the Watcher to request anonymity.

The following interfaces are left FFS:

1) Pex: Security between PEA and external information source should be further studied.

2) Pex, Peu & Pen: Threats and potential solutions for false presence information inside the network should be further studied.

3) Peu & Pw: The degree of anonymity provided by ‘anonymous IMPU’ should be further studied.

4) Peu & Pw: Ability of non-IMS accesses (e.g. WAP/SMS/WV) to fulfil the security requirements should be further studied.

5 Presence Security architecture

The Presence Security architecture is based on the IMS Security Architecture as specified in TS33.203 [6].

The functional architecture is depicted in Figure 2 and this clause specifies the protection methods for the Ut interface.

[

The proposals that have been discussed include:

1. *Base it on IMS Registrations, new key management procedures and base the protection on HTTPS*

2. *Use of AKAv2 and Authentication proxy and TLS*

3. *Use of Bootstrapping function for HTTP AKA using TLS]*

6 Security features

6.1 IMS related security features

6.1.1 Confidentiality protection

Possibility for IMS specific confidentiality protection shall be provided to SIP signalling messages between the UE and the P-CSCF. Mobile Operators shall take care that the deployed confidentiality protection solution and roaming agreements fulfils the confidentiality requirements presented in the local privacy legislation when IMS is used for Presence. The following mechanisms are provided at SIP layer:

1. The UE shall always offer encryption algorithms for P-CSCF to be used for the session, as specified in chapter 8.
2. The P-CSCF shall decide whether the IMS specific encryption mechanism is used. If used, the UE and the P-CSCF shall agree on security associations, which include the encryption key that shall be used for the confidentiality protection. The mechanism is based on IMS AKA and specified in clause 6.1 of [6].

Confidentiality between CSCFs, and between CSCFs and the HSS shall rely on mechanisms specified by Network Domain Security in [7].

6.1.2 Subscriber anonymity

6.1.2.1 Initiator of a SIP dialog

The network shall hide the identity of the initiator of a SIP dialog (the SIP URI) in the following cases:

a. The initiator has requested from the network that her identity is hidden from the receiver of the request.

b. The initiator has agreed with the home network that the home network takes care of the identity blocking for certain messages on behalf of the initiator.

Anonymity of the SIP URI shall be provided if the subscriber requests it. The network shall not deliver the message to the receiver if the initiator has set the anonymity request as ‘critical’, and the network is not able to provide the requested anonymity. The same anonymity rules shall apply to all messages within a SIP dialog.

Anonymity shall be provided by the last-hop P-CSCF. If the IMS originated messages are sent outside the IMS trust domain (e.g. to the open Internet), the edge proxy (e.g. I-CSCF) shall provide the anonymity.

Anonymity may be requested with multimedia sessions, or with any other services that will use IMS, such as Presence or Instant Messaging.

6.1.2.2 Receiver of a SIP dialog initiation request

The receiver of a SIP dialog initiation request is able to have some degree of anonymity if she registers a pseudonym as IMPU. In this case, the subscriber shall be responsible for not revealing the relationship between the pseudonym IMPU and her real identity to unauthorized parties. If she reveals her real identity, there is no anonymity.

6.1.3 Subscription authentication

The Presence Server shall authenticate the subscription requests originated from Watchers if required in the Subscription Authorization Policy. The Subscription Authorization Policy shall indicate the method and credentials used in authentication. This password needs to be manually distributed by the Principal of the Presentity (or the subscriber) to the Watcher(s). This can be done by several mechanisms but is left out from this specification. The

password should be random and difficult to guess for an attacker however the actual password derivation is under the responsibility of the subscriber (or principal).

6.2 Secure access to HTTP Application Server

[Editors Note: This is a placeholder forHTTP requirements]

6.2.1 Authentication

[Editors Note: This is a placeholder for HTTP authentication requirements]

6.2.2 Integrity protection

[Editors Note: This is a placeholder for HTTP integrity protection requirements]

6.2.3 Confidentiality protection

[Editors Note: This is a placeholder for HTTP confidentiality protection requirements]

6.3 non-IMS related security features

[Editors Note: This is a placeholder for non-IMS requirements]

7 Secure access

8 Security mechanisms

8.1 IMS related security mechanisms

8.1.1 Confidentiality mechanisms

If the local policy in P-CSCF requires the use of IMS specific confidentiality protection mechanism between UE and P-CSCF, IPsec ESP as specified in reference [13] shall provide confidentiality protection of SIP signalling between the UE and the P-CSCF, protecting all SIP signalling messages at the IP level. IPSec ESP general concepts on Security Policy management, Security Associations and IP traffic processing as described in reference [14] shall also be considered. ESP confidentiality shall be applied in transport mode between UE and P-CSCF.

The method to set up ESP security associations (SAs) during the SIP registration procedure is specified in clause 7 of [6]. As a result of the registration procedure, a pair of unidirectional SAs between the UE and the P-CSCF shall be established. The pair consists of an SA for traffic from the UE to the P-CSCF (inbound SA at the P-CSCF) and an SA for traffic from the P-CSCF to the UE (outbound SA at the P-CSCF).

The encryption key CK_{ESP} is the same for the two simultaneously established SAs. The encryption key CK_{ESP} is obtained from the key CK_{IM} established as a result of the AKA procedure, specified in clause 6.1 of [6], using a suitable key expansion function. This key expansion function depends on the ESP encryption algorithm and is specified in Annex I.

The encryption key expansion on the user side is done in the UE. The encryption key expansion on the network side is done in the P-CSCF.

The anti-replay service shall be enabled in the UE and the P-CSCF on all established SAs.

8.1.2 Security association set-up procedure

The security association set-up procedure is necessary in order to decide what security services to apply and when the security services start. In the IMS authentication of users is performed during registration as specified in clause 6.1 of [6]. Subsequent signaling communications in this session will be integrity and confidentiality protected based on the keys derived during the authentication process.

8.1.2.1 New security association parameters

- **Enryption algorithm**

  The enryption algorithm is DES-EDE3-CBC [15].

[Editors note: The encryption algorithm AES should be added as soon as it appears as an RFC in IETF.]

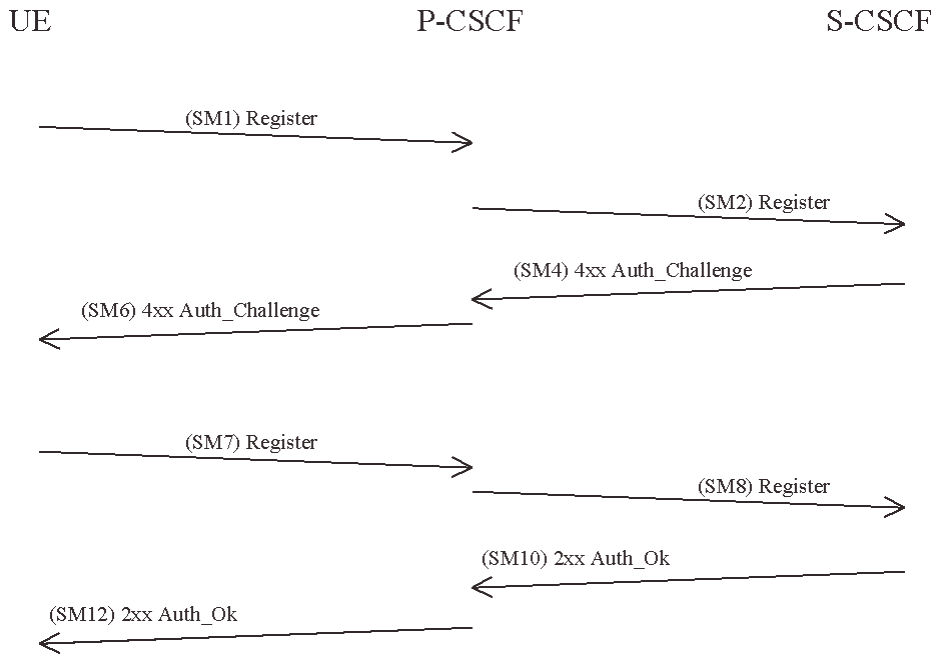
NOTE: This, in particular, excludes the use of the NULL enryption algorithm.

[Editors note: The key expansion function is FFS.]

8.1.2.2 Set-up of security associations (successful case)

The set-up of security associations is based on [16]. Annex H of [6] shows how to use [16] for the set-up of security associations.

In this section the normal case is specified i.e. when no failures occurs. Note that for simplicity some of the nodes and messages have been omitted. Hence there are gaps in the numbering of messages, as the I-CSCF is omitted.



The UE sends a Register message towards the S-CSCF to register the location of the UE and to set-up the security mode, cf. clause 6.1 of [6]. In order to start the security mode set-up procedure, the UE shall include a *Security-setup-*line in this message.

The *Security-setup-line* in SM1 contains the SPI numbers and the protected port selected by the UE. It also contains a list of identifiers for the integrity and encryption algorithms, which the UE supports.

SM1:
REGISTER(Security-setup = *SPI_U, Port_U, UE integrity and encryption algorithms list)*

Upon receipt of SM1, the P-CSCF temporarily stores the parameters received in the *Security-setup-line* together with the UE's IP address from the source IP address of the IP packet header, the IMPI and IMPU. Upon receipt of SM4, the P-CSCF adds the keys IK_{IM} and CK_{IM} received from the S-CSCF to the temporarily stored parameters.

Release 6 P-CSCF must propose SA alternatives both for Release 5 and Release 6 UE's. The P-CSCF selects the SPI for the inbound SA. The same SPI number shall be used for Release 5 and Release 6 options. The P-CSCF shall define the SPIs such that they are unique and different from any SPIs as received in the *Security-setup-line* from the UE.

NOTE: This rule is needed since the UE and the P-CSCF use the same keys for inbound and outbound traffic.

In order to determine the integrity and encryption algorithms the P-CSCF proceeds as follows: the P-CSCF has a list of integrity and enryption algorithm combinations it supports, ordered by priority. Release 6 algorithms must have higher priority than Release 5 algorithms. The P-CSCF selects the first algorithm combination on its own list which is also supported by the UE.

The P-CSCF then establishes corresponding pair of SAs in the local security association database.

The *Security-setup*-line in SM6 contains the SPI assigned by the P-CSCF and the fixed number of the protected port at the P-CSCF. It also contains a list of identifiers for the integrity and encryption algorithms which the P-CSCF supports.

NOTE: P-CSCF may be configured to trust on the encryption provided by the underlying access network. In this case, the P-CSCF acts according to Release 5 specificatons, and does not include encryption algorithms to the *Security-setup*-line in SM6.

SM6:
4xx Auth_Challenge(Security-setup = *SPI_P, Port_P*, *P-CSCF integrity and encryption algorithms list)*

Upon receipt of SM6, the UE determines the integrity and encryption algorithm as follows: the UE selects the first integrity and encryption algorithm combination on the list received from the P-CSCF in SM6 which is also supported by the UE.

NOTE: Release 5 UE will not support any encryption algorithms, and will choose the first Release 5 integrity algorithm on the list received from the P-CSCF in SM6.

The UE then proceeds to establish another pair of SAs in the local SAD.

The UE shall integrity and confidentiality protect SM7 and all following SIP messages. Furthermore the integrity and encryption algorithms list received in SM6 shall be included:

SM7:
REGISTER(Security-setup = *SPI_P, Port_P*, *P-CSCF integrity and encryption algorithms list)*

After receiving SM7 from the UE, the P-CSCF shall check whether the integrity and encryption algorithms list received in SM7 is identical with the list sent in SM6. If this is not the case the registration procedure is aborted. The P-CSCF shall include in SM8 information to the S-CSCF that the received message from the UE was integrity and confidentiality protected. The P-CSCF shall add this information to all subsequent REGISTER messages received from the UE that have successfully passed the integrity and confidentiality check in the P-CSCF.

SM8:
REGISTER(Integrity-Protection = *Successful, Confidentiality-Protection =Successful,* IMPI*)*

The P-CSCF finally sends SM12 to the UE. SM12 does not contain information specific to security mode setup (i.e. a Security-setup line), but with sending SM12 not indicating an error the P-CSCF confirms that security mode setup has been successful. After receiving SM12 not indicating an error, the UE can assume the successful completion of the security-mode setup.

8.1.3 Subscriber anonymity mechanisms

8.1.3.1 Anonymity of SIP dialog initiator

The anonymity mechanism is optional for implementation in UA. The UA may provide anonymity for the subscriber following the privacy mechanisms described in [17, and 18]. This includes populating the SIP headers with values that reflect the privacy requirements of the subscriber, as well as requesting further privacy from the network.

The UA may use the following priv-value types of the Privacy header in [17, and 18]:

c. 'none'

d. 'id'

e. 'critical'

f. 'user'

[Editors note:priv-value types 'header' and 'session' are FFS.]

The home network (e.g. S-CSCF or an Application Server) may provide the anonymity on behalf of the UA using the following priv-value type [17]:

g. 'user'

P-CSCF and the edge proxy (e.g. I-CSCF) must implement the following priv-value types of the Privacy header in [17, and 18]:

h. 'none'

i. 'id'

j. 'critical'

k. 'user'

[Editors note:priv-value types 'header' and 'session' are FFS.]

P-CSCF and the edge proxy shall monitor the privacy requests in all terminating SIP requests, and provide the requested privacy (e.g. hide the identity of the subscriber). P-CSCF and the edge proxy shall not provide privacy for originating SIP requests.

8.1.3.2 Pseudonym IMPU

Subscriber may use pseudonym IMPU to obtain some degree of anonymity. From system point of view, the pseudonym IMPU is like any other IMPU. All existing rules related IMPUs shall apply.

Note: Unprotected SIP REGISTER messages include identity information that may be intercepted by unauthorized parties when sent over the air-interface. These messages may be used to combine the IMPU and IMPI information, and consequently this information may reveal the parallel IMPUs related to the pseudonym IMPU.

[Editors note: There may be a need for additional rules related to the registration of pseudonym IMPUs.]

8.1.4 Subscription authentication mechanism

[Editors Note: The use of HTTP Digest AKA is FFS:

- *HTTP Digest AKA: If the watcher belongs to the same home network than the presentity, HTTP Digest AKA could be used for authentication. In this case, the related session keys IK and CK would also be available for end-to-end integrity and confidentiality protection if needed. Note that it is also possible to change the IMS/Presence security architecture in the way that all subscriptions are always routed via the Presence Server, and that the communication between the IMS sub-domains is done only between the Presence Servers.*

]

Subscription Authorization Policy may require that the Presence Server must authenticate the Watchers during the subscription phase. The Subscription Authorization Policy shall define which authentication method and credentials are used in the authentication. The following mechanisms shall be supported:

b. HTTP Digest

NOTE: Distribution of HTTP Digest passwords is outside the scope of this specification. There are many known solutions, e.g. the presentity (or principal/subscriber) can take responsibility of the key distribution, or the watchers may need to register to Presence Servers via HTTP.

8.2 HTTP related security mechanisms

[Editors Note: This is a placeholder for HTTP security mechanisms]

8.2.1 Authentication mechanisms

[Editors Note: This is a placeholder for HTTP authentication mechanisms]

[Editors Note: The re-use of USIM for authentication is not perceived as secure if the AKA session keys (IK/CK) are not somehow tied to the security solution. For example, the use of RFC 3310 (HTTP Digest authentication with AKA) with the algorithm version "AKAv1" shall not be used if the related session keys (IK and/or CK) are not also used in the solution.]

[Editors Note: At least the following authentication solutions should be further studied:

a. Presence is limited to the re-use of ISIM with HTTP Digest AKA v1.

b. A new version of HTTP Digest AKA algorithm is developed. In this case, the re-use of USIM with HTTP Digest AKA v1 is secure.

c. HTTP authentication with HTTP Digest passwords is appropriate.

d. Solutions with client certificates (e.g. with TLS, OMA/WAP) are appropriate.

e. Some password based Single-Sign-On solutions could be applied.

f. Integration of HTTP security to IMS registration should be further studied. This may imply some kind of Single-Sign-On solution.]

8.2.2 Integrity protection mechanisms

[Editors Note: This is a placeholder for HTTP integrity protection mechanisms]

8.2.3 Confidentiality protection mechanisms

[Editors Note: This is a placeholder for HTTP confidentiality protection mechanisms]

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**
2002-07	*SA3#24*	*SA3-020340*			*First Draft TR: Presence security Architecture*		*0.1.0*
2002-10	*SA3#25*	*SA3-020507* *SA3-020508*			*Included relevant information as decided at SA3#24*	*0.1.0*	*0.2.0*
2002-12	SA3#26	*SA3-020621* SA3-020622			Included relevant information as decided per SA3#26. Removed all text on Lawful intercept since the LI group will take care of those requirements.	0.2.0	0.3.0
2003-04	SA3#27	SA3-030022			This was an LS from SA2 stating that HTTP shall be used for user manipulation in the AS	0.3.0	0.4.0
2003-04	SA3#27	SA3-030070			The requirements were not agreed but it was agreed to include the requirements on confidentiality as an editors note	0.3.0	0.4.0
2003-04	SA3#27	SA3-030068			A CR on end-to-end authentication was agreed to be included. However end-to-end was removed.	0.3.0	0.4.0
2003-05	SA3#28	SA3-030246			Included watcher authentication and some text on manual keying	0.4.0	0.5.0
2003-05	SA3#28	SA3-030248			Confidentiality requirements included	0.4.0	0.5.0
2003-09	SA3#29				Inclusion of password mechanism is optional and a reference to TLS for the Ut interface.		