3GPP SA3 Meeting #25 **SA3-020569**
Munich, Germany, 8-11 November 2002

Title:	**Presence Security Architecture**
Source:	SA3
To:	SA2
Cc:	SA1

Contact Person:

Name:	Krister Boman
Tel. Number:	+46313446055
E-mail Address:	krister.boman@erv.ericsson.se

Attachments: SA3-020507, SA3-020508

1. Overall Description:

SA3 has started the work defining the presence security architecture and has agreed that Clause 2 in SA3-020507 and Clause 3 in SA3-020508 shall be included in the SA3 TR for presence. These requirements shall be viewed as SA3 working assumptions and SA3 asks SA2 to review these requirements and provide SA3 with feedback.

At SA3#25 the following requirements where discussed in more detail:

1. Presentity and Watcher anonymity cf. SA3-020508
2. Presentity defined passwords i.e. that the Presentity defines a password and distribute this password to selected Watchers by e.g. email, chat or SMS. This password can then be used for authenticating a Watcher in the Presence Server. The rationale behind this requirement is the Trust model between the Presentity and a Watcher as defined in Clause 2.3 SA3-020507

2. Actions:

To SA2 group.

ACTION: Review the attached documents that define the current SA3 working assumptions and provide with feedback to SA3. In particular SA2 is asked to check the requirements around anonymity and Presentity defined passwords.

3. Date of Next SA3 Meetings:

SA3 Meeting #25	19-22 November 2002	Oxford, UK
SA3 Meeting #26	25-28 February 2003	TBD

3GPP TSG SA WG3 Security **S3-020507**

8th – 11th October, 2002

Munich, Germany

Agenda Item:	7.17
Source:	Ericsson
Title:	Presence Security Architecture
Document for:	Discussion/Decision

1. Introduction

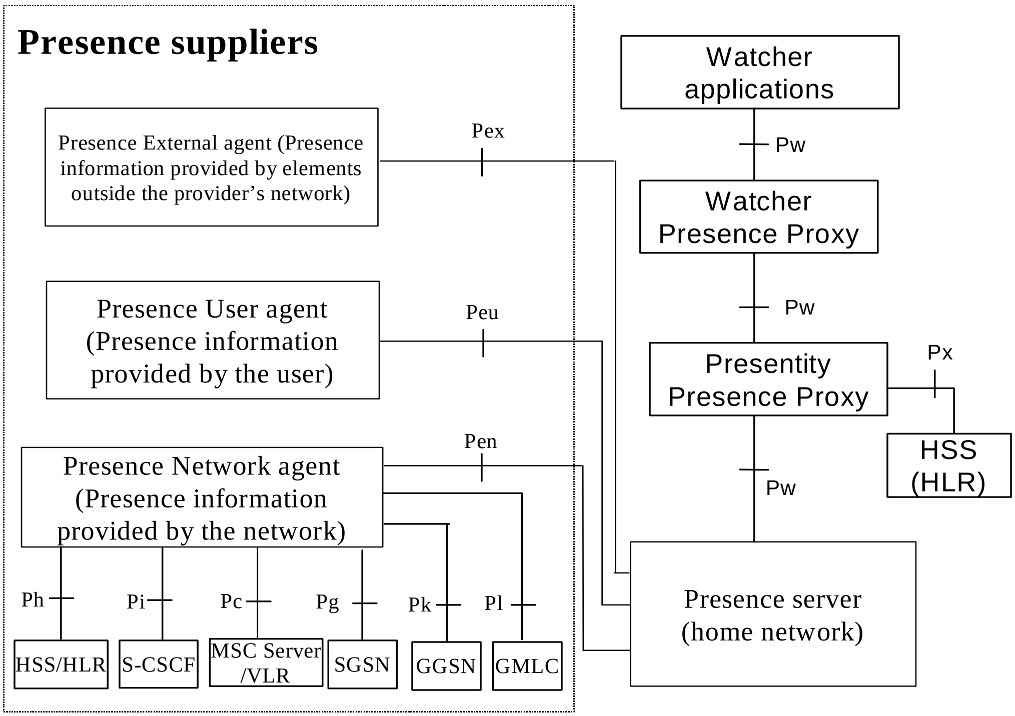
This paper aims to identify some security requirements that apply for the Presence Architecture. In particular this paper does not assume any particular architecture e.g. IMS and it is general in nature.

SA3 is asked to discuss and endorse the proposed requirements as working assumptions and collect them where appropriate in the TR i.e. [S3-020340].

2. An overview of Threats

2.1 Roles

The architecture as defined in [TS23141] to support presence service contains a number of roles, cf Figure below.



Presence suppliers
Watcher applications
Presence External agent (Presence information provided by elements outside the provider's network)
Pex
Pw
Watcher Presence Proxy
Presence User agent (Presence information provided by the user)
Peu
Pw
Presentity Presence Proxy
Px
HSS (HLR)
Pen
Presence Network agent (Presence information provided by the network)
Pw
Presence server (home network)
Ph
Pi
Pc
Pg
Pk
Pl
HSS/HLR
S-CSCF
MSC Server /VLR
SGSN
GGSN
GMLC

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

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:

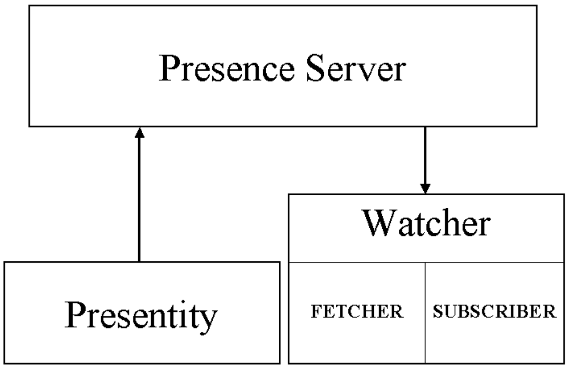
1. Information sources - Suppliers
    a. External Presence Supplier (External Agent)
    b. User Agent Presence Supplier (Presence UA)
    c. Network Presence Suppliers
        i. HSS
        ii. S-CSCF
        iii. MSC/VLR
        iv. SGSN
        v. GGSN
        vi. GMLC
2. Information sinks
    a.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

2.2 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.

2.3 Trust relationships

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.

It is envisioned that the presence information will be in the interests of the legal authorities and that operators need to ensure that there are mechanisms in place making it possible to collect this information e.g. in a Legal Interception Watcher. If such an application is applied the Presentity can do nothing more than to have trust on that application.

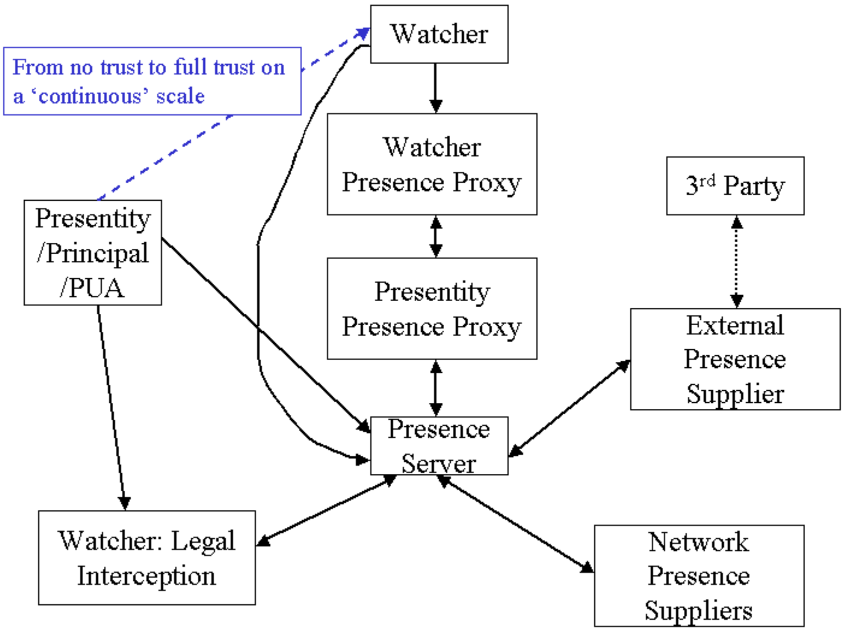
A Watcher Presence Proxy will proxy information between the Watcher and the Presence Server in both directions. The proxy will generate billing and charging information and has a relationship with the Watcher e.g. in terms of a subscription. A Watcher shall trust a Watcher Presence Proxy although the 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 Principal trusts the Legal Interception application

- The Watcher trusts the Watcher Presence Proxy
- The Watcher trusts the Presence Server
- The Watcher Presence Proxy trusts the Presentity Presence Proxy


From no trust to full trust on a 'continuous' scale
Watcher
Watcher Presence Proxy
3rd Party
Presentity /Principal /PUA
Presentity Presence Proxy
External Presence Supplier
Presence Server
Watcher: Legal Interception
Network Presence Suppliers

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.

2.4 Threats

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

2.5 Requirements

Clearly 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. However the Presentity needs to allow that a legal interception Watcher is authorised to collect information about the Presentity such that the Presentity is not even aware of it. 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. 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 except the legal interception application

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.

3 Conclusions

In this document the general architecture as defined in Clause 2.1 has been analysed from security perspective. In particular the different roles in presence has been highlighted and what interfaces an attacker most likely can approach. This architecture is to be applied on e.g. IMS but SA3 is encouraged to endorse the requirements as defined in Clause 2.5 as working assumptions for Presence.

References

[S3-020340] 3GPP SA3 “First Draft TR: Presence security Architecture”, SA3#24 July Helsinki

[TS23141] 3GPP; TSG Services and System Aspects; Presence Service; Architecture and Functional Description, TS 23.141 v 020, June 2002

[RFC2778] IETF RFC 2778, Model for Presence and Instant Messaging, February 200

3GPP TSG SA WG3 Security **S3-020508**

8th – 11th October, 2002

Munich, Germany

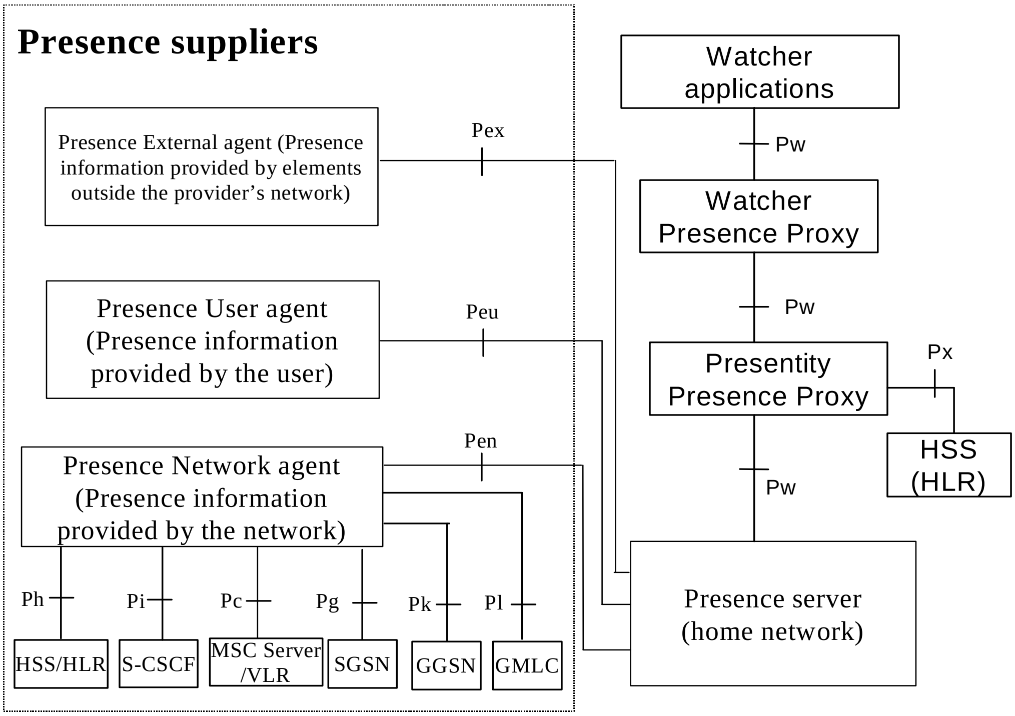
Agenda Item:	7.17
Source:	Ericsson
Title:	Working Assumptions and Open Issues in Presence Security
Document for:	Discussion/Decision

1. Introduction

This paper compares the Presence Reference Architecture to existing UMTS security mechanisms. The goal of the paper is to identity working assumptions and open issues for SA3.

2. Presence Architecture and Security Requirements

Figure 1 describes reference architecture for presence services. The architecture is very general and can be realized over various technical systems, e.g. IMS, WAP or SMS. This paper discusses each protocol interface in different contexts, and identifies working assumptions and open issues for SA3.


Presence suppliers
Presence External agent (Presence information provided by elements outside the provider's network)
Presence User agent (Presence information provided by the user)
Presence Network agent (Presence information provided by the network)
Pex
Peu
Pen
Ph
Pi
Pc
Pg
Pk
Pl
HSS/HLR
S-CSCF
MSC Server /VLR
SGSN
GGSN
GMLC
Watcher applications
Pw
Watcher Presence Proxy
Pw
Presentity Presence Proxy
Px
HSS (HLR)
Pw
Presence server (home network)

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: Reference architecture to support a presence service [TS23141]

2.1 Presence External Agent - Presence Server (Pex)

Presence External Agent (PEA) provides presence information outside the provider’s network. Since PEA and Presence Server (PS) both situate in the home network, the Pex interface is generally ‘secure’.

The following issues are open and for future study:

- Security between PEA and external information source: Presence External Agent must be able to trust on the real source of the presence information. This security is currently outside the Presence Architecture but it has significant influence on the trustworthiness of the system.
- False presence information inside the network: It is not realistic to assume that communication between the presence suppliers (i.e. Pex, Peu and Pen) and the PS is secured end-to-end. However, there is a threat for internal attacks. In theory, anybody (inside some network) could feed false presence information to the Presence Server, and Presence Server would forward this information to the watchers without real security checking.

2.2 Presence User Agent - Presence Server (Peu)

A presentity may provide presence information using a Presence User Agent (PUA). Presentity may also use PUA to manage access rules, and activate/deactivate the presence service.

PUA may situate in UE (e.g. IMS based PUA) or in the network (e.g. WAP or SMS based PUA).

2.2.1 IMS based Presence User Agent

In IMS, the Presence User Agent will be situated in the UE. PUA will send presence information using some SIP method (e.g. UPDATE) and utilizing the existing IMS architecture. The following security services can be re-used from IMS:

- Authentication, integrity protection and replay protection: The Presence Server and UE can trust that IMS covers these security services.
- Anonymity: The presentity may not want to reveal its real identity. For this purpose, the presentity may register an anonyme identity (IMPU).

The following issues are open and for future study:

- Confidentiality: Encryption provided by the access network (e.g. UMTS) may not be enough for end-user privacy. The use of IPsec encryption between the UE and P-CSCF may be required.
- False presence information inside the network: It is not realistic to assume that communication between the presence suppliers (i.e. Pex, Peu and Pen) and the PS is secured end-to-end. However, there is a threat for internal attacks. In theory, anybody (inside some network) could feed false presence information to the Presence Server, and Presence Server would forward this information to the watchers without real security checking.
- Degree of anonymity: It is not clear what is the degree of anonymity that can be achieved by using ‘anonyme’ IMPUs. For example, some information in SIP message may reveal that some IMPUs are actually related to the same UE.
- Protocols: It is not clear yet which protocols will be used in Peu interface. Peu may include protocols for web access (e.g. HTTP for access list manipulation and registrations), and consequently there may be a need for additional security.

2.2.2 Non-IMS based Presence User Agent

The following issues are open and for future study:

- Non-IMS accesses: Ability of WAP/SMS/WV etc to fulfil the security requirements should be studied.

2.3 Presence Network Agent - Presence Server (Pen)

Presence Network Agent (PNA) will provide presence information from various network elements in the home network. Since PNA and Presence Server (PS) both situate in the home network, the Pen interface is generally ‘secure’.

The following issues are open and for future study:

- False presence information inside the network: It is not realistic to assume that communication between the presence suppliers (i.e. Pex, Peu and Pen) and the PS is secured end-to-end. However, there is a threat for internal attacks. In theory, anybody (inside some network) could feed false presence information to the Presence Server, and Presence Server would forward this information to the watchers without real security checking.

2.3.1 HSS/HLR – Presence Network Agent (Ph)

No additional security requirements.

2.3.2 S-CSCF – Presence Network Agent (Pi)

No additional security requirements.

2.3.3 Presence Network Agent – MSC Server/VLR (Pc)

No additional security requirements.

2.3.4 Presence Network Agent – SGSN (Pg)

No additional security requirements.

2.3.5 Presence Network Agent – GGSN (Pk)

No additional security requirements.

2.3.6 Presence Network Agent – GMLC (Pl)

No additional security requirements.

2.4 Watcher applications – Presence Server (Pw)

The Watcher application (WA) is used to fetch or subscribe presence, presence list and/or watcher information. In practice, there are at least two different instances of Pw interface. Firstly, a subscriber can acts as a Watcher. Secondly, a subscriber can act as a Presentity subscribed to the watcher information. The both cases are discussed here even though the second case may belong to Peu interface (open issue in SA2).

2.4.1 IMS based Watcher applications

In the first case, the IMS Watcher subscribes to the Presence Server situated in the home network of the Presentity. The IMS Watcher and this home network may not have any security relationships.

In the second case, the IMS Presentity subscribes to the watcher information in the Presence Server. This functionality is needed in order to informing the Presentity on watcher information and new Watchers. If a Watcher is not included in the access lists, the Presentity needs to update the access rules in order to allow the subscription. The Presence Server situates in the home network of the Presentity, and consequently, they have an existing security relationship.

The following security services can be re-used from IMS:

- Authentication:

  - The Presence Server can trust that the Watcher Presence Proxy has authenticated the identities of the IMS Presentities and Watchers.
  - The Presentities and the Watchers can trust that the their own Watcher Presence Proxy has a trust relationship with the Presence Servers.
- Integrity and replay protection: The messages between the Presentity/Wacher and the Presence Server are integrity and replay protected between the UE and P-CSCF. The path between the P-CSCF and the Presence Server is trusted.

The following new security services should be considered:

- Anonymity: The Watcher may not want to reveal its real identity. For this purpose, the Watcher may register an anonyme identity (IMPU).

The following issues are open and for future study:

- Confidentiality: Encryption provided by the access network (e.g. UMTS) may not be enough for end-user privacy. The use of IPsec encryption between the UE and P-CSCF may be required.
- Authentication: The Presence Server may need additional mechanism for authenticating the Watchers. For example, the Presentity may provide passwords for Watcher authentication.
- Authentication: The Presentity may need additional mechanism for authenticating the Watchers. For example, the Watcher may provide a token or electronic signature for authentication.
- Degree of anonymity: It is not clear what is the degree of anonymity that can be achieved by using 'anonyme' IMPUs. For example, some information in SIP message may reveal that some IMPUs are actually related to the same UE.
- Anonymity: The Watcher may not want to reveal its real identity. The Watcher may want to request that its identity (IMPU) is hidden from the Presentity.

2.4.2 Non-IMS based Watcher applications

The following issues are open and for future study:

- Non-IMS accesses: Ability of WAP/SMS/WV etc to fulfil the security requirements should be studied.

2.5 Presentity Presence Proxy – HSS (Px)

This interface assists locating the Presence Server of the presentity. There are no additional security requirements related to Px interface.

3. Conclusions

It is suggested that SA3 adopts the following working assumptions related to Presence:

1) Peu: Existing IMS security architecture fulfils the security requirements related to authentication, 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.

It is suggested that SA3 further studies the following open issues related to Presence:

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: IMS may need to be enhanced by IPsec encryption between UE and P-CSCF in order to fulfil the confidentiality requirement.

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

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

6) Pw: The Presence Server may need additional mechanism for authenticating the Watchers. For example, the Presentity may provide passwords for Watcher authentication.

7) Pw: The Presentity may need additional mechanism for authenticating the Watchers. For example, the Watcher may provide a token or electronic signature for authentication.

8) Pw: IMS may need to be enhanced by a security mechanism for the Watcher to request anonymity.

It is suggested that LSs related to the following issues are sent to other 3GPP working groups:

1) Peu: It is not clear yet which protocols will be used in Peu interface. Peu may include protocols for web access (e.g. HTTP for access list manipulation and registrations), and consequently there may be a need for additional security.

4. References

[TS23141] 3GPP, Presence Service; Architecture and Functional Description, Release 6.