

8th – 11th October, 2002

Munich, Germany

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

## 1. Introduction

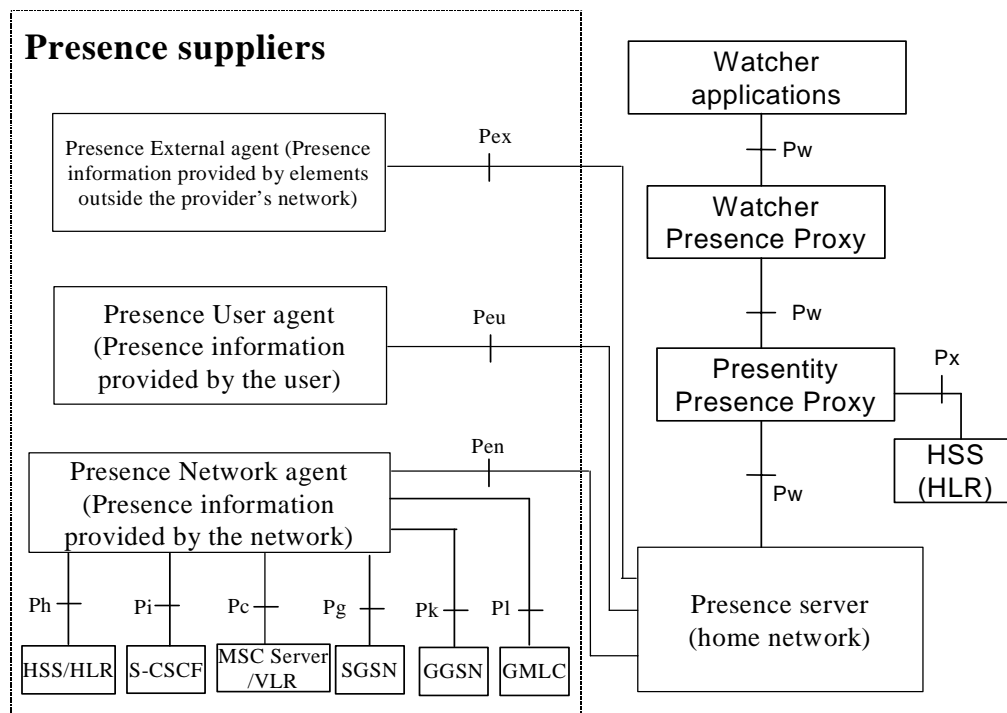
This paper aims to identify some security requirements that apply for the Presence Architecture. In particular this paper does not assume any particular architecture e.g. IMS and it is general in nature.

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.



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:

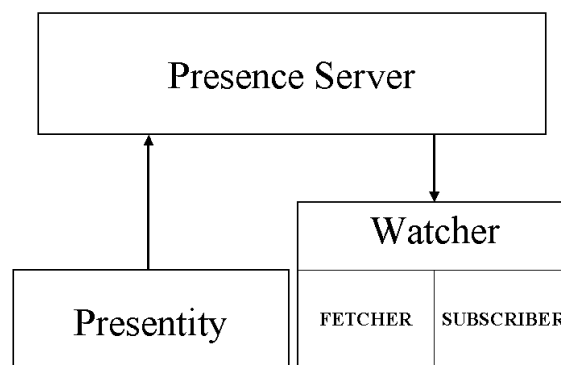
1. Information sources - Suppliers
  - a. External Presence Supplier (External Agent)
  - b. User Agent Presence Supplier (Presence UA)
  - c. Network Presence Suppliers
    - i. HSS
    - ii. S-CSCF
    - iii. MSC/VLR
    - iv. SGSN
    - v. GGSN
    - vi. GMLC
2. Information sinks
  - a. Watcher applications 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 3<sup>rd</sup> 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.

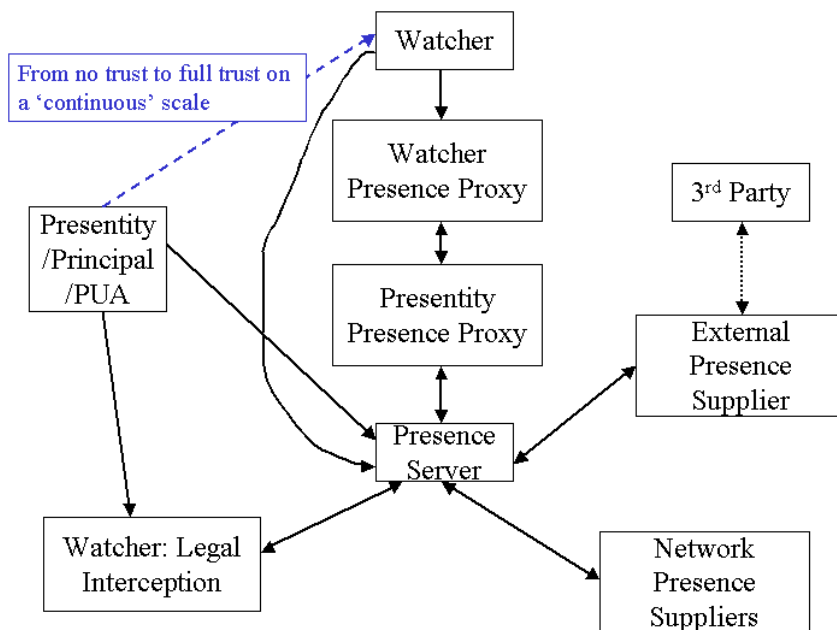
A Watcher Presence Proxy will proxy information between the Watcher and the Presence Server in both directions. The proxy will generate billing and charging information and has a relationship with the Watcher e.g. in terms of a subscription. A Watcher shall trust a Watcher Presence Proxy although the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



It is assumed that a 3<sup>rd</sup> 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 3<sup>rd</sup> 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, 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 3<sup>rd</sup> 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 is 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