3GPP TSG SA WG3 Security — S3#23 **S3-020196**
14 - 17 May 2002
Victoria, Canada

TSG-SA WG 2 meeting #24 **S2-021499**
Madrid, Spain, 22-26th April 2002

Title: LS on Presence Service
Source: SA2
To: SA3, SA5, CN1, CN4
Cc:
Response to:

Contact Person:

Name: **Kirsi Maansaari**
Tel. Number: +358 40 5690136
E-mail Address: kirsi.maansaari@nokia.com

Attachments:

- TR 23.841, version 1.1.0

TSG SA2 kindly informs other groups that SA2 has done a Technical Report on Presence Service. This LS reports the current status of this work and sends the latest version of 23.841 for review. The attached version of the TR is sent for approval to SA#16. The version 1.1.0 is going to be raised for version 2.0.0 before next SA plenary.

SA2 feels that the architecture contained in TR 23.841 has reached sufficient level of maturity for other groups to start working on the Stage-3 and other detailed Stage-2 aspects (security, charging, etc.) of Presence.

Date of Next SA2 Meetings:

Title	Date	Location	Country
SA2 #25	24–28 June 02	TBD	Finland
SA2 #26	19–23 Aug 02	Toronto	Canada

3GPP TR 23.841 V1.1~~0~~.0 (2002-03)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Presence Service;
Architecture and Functional Description
(Release ~~5~~6)

The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.

The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented.
This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification.
Specifications and reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords

Presence

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.

1 Scope

The present document describes the architectural solution and functionalities required for the Presence Service.

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: "3G Vocabulary".

[2] 3GPP TS 22.141: “Presence Service; Stage 1”.

[3] CPIM Presence Information Data Format, Internet Draft in IMPP WG http://www.ietf.org/internet-drafts/draft-ietf-impp-cpim-pidf-01.txt, October 2001

[4] SIP Extensions for Presence, Rosenberg et al., Internet-Draft in SIMPLE WG, http://www.ietf.org/internet-drafts/draft-ietf-simple-presence-03.txt, September 2001

[5] 3GPP TS 33.203: "Access security for IP-based services"

[6] 3GPP TS 32.200: "Charging Principles"

[7] 3GPP TS 32.225: "Charging Data Description for the IMS domain"

[8] 3GPP TS 33.210: "Network Domain Security"

[9] 3GPP TS 23.228: "IM Subsystem Stage-2"

[10] 3GPP TS 23.218: "IP Multimedia (IM) Session Handling; IP Multimedia (IM) call model"

[11] SIP-Specific Event Notification, Internet-Draft in SIP WG, http://www.ietf.org/internet-drafts/draft-ietf-sip-events-01.txt, November 2001

[12] SIP Event Package for Buddy List Presence, Internet-Draft, http://search.ietf.org/internet-drafts/draft-rosenberg-simple-buddylist-package-00.txt, November 2001

[13] 3GPP TS 29.061: "Packet Domain; Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based services and Packet Data Networks (PDN)".

3 Definitions and abbreviations

3.1 Definitions

3.2 Abbreviations

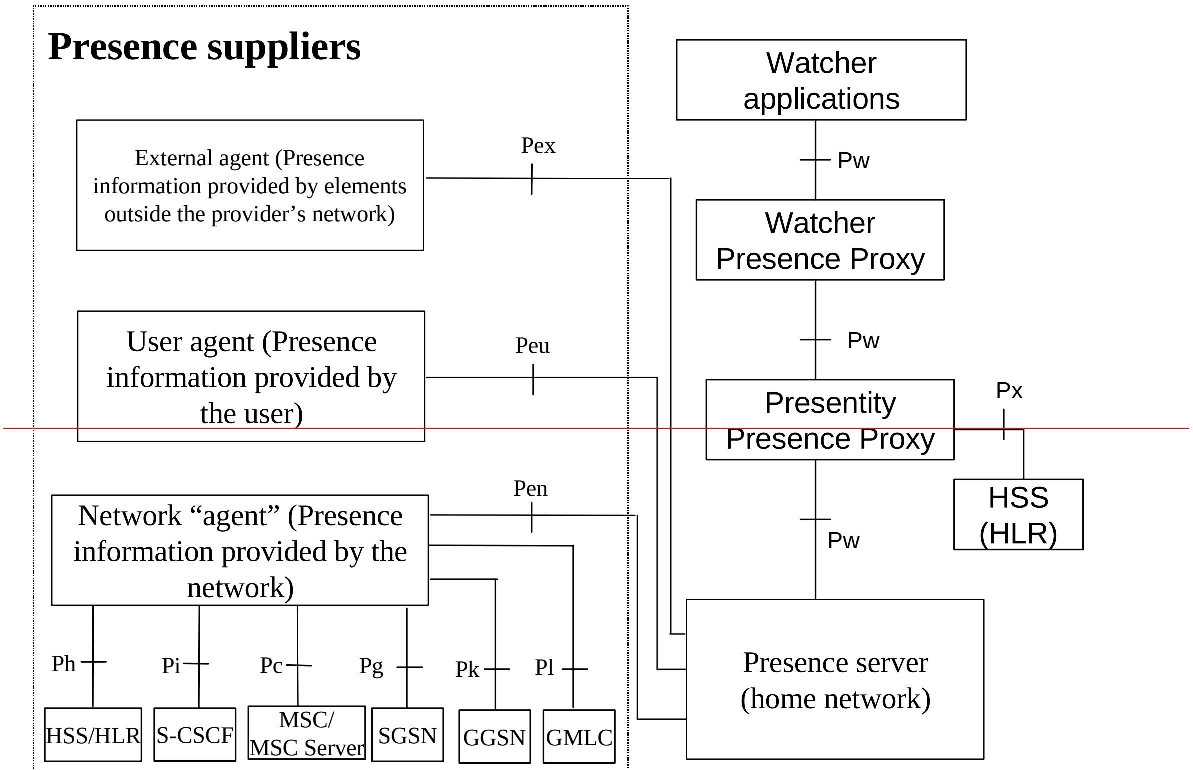
PPP	Presentity Presence Proxy
WPP	Watcher Presence Proxy

4 Reference Architecture

Editors note: This chapter describes the reference architecture, the reference points and interfaces used for Presence Service, and the Presence Service functionality within.

The generic reference architecture for providing presence service is depicted in Figure 1 below.

It shall be noted that domain-specific simplifications of this generic architecture may be applicable. Such simplifications applicable for providing presence service within the IM CN Subsystem are described in Section 5.6.


Presence suppliers
External agent (Presence information provided by elements outside the provider's network)
User agent (Presence information provided by the user)
Network "agent" (Presence information provided by the network)
Pex
Peu
Pen
Ph
Pi
Pc
Pg
Pk
Pl
HSS/HLR
S-CSCF
MSC/ MSC Server
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.

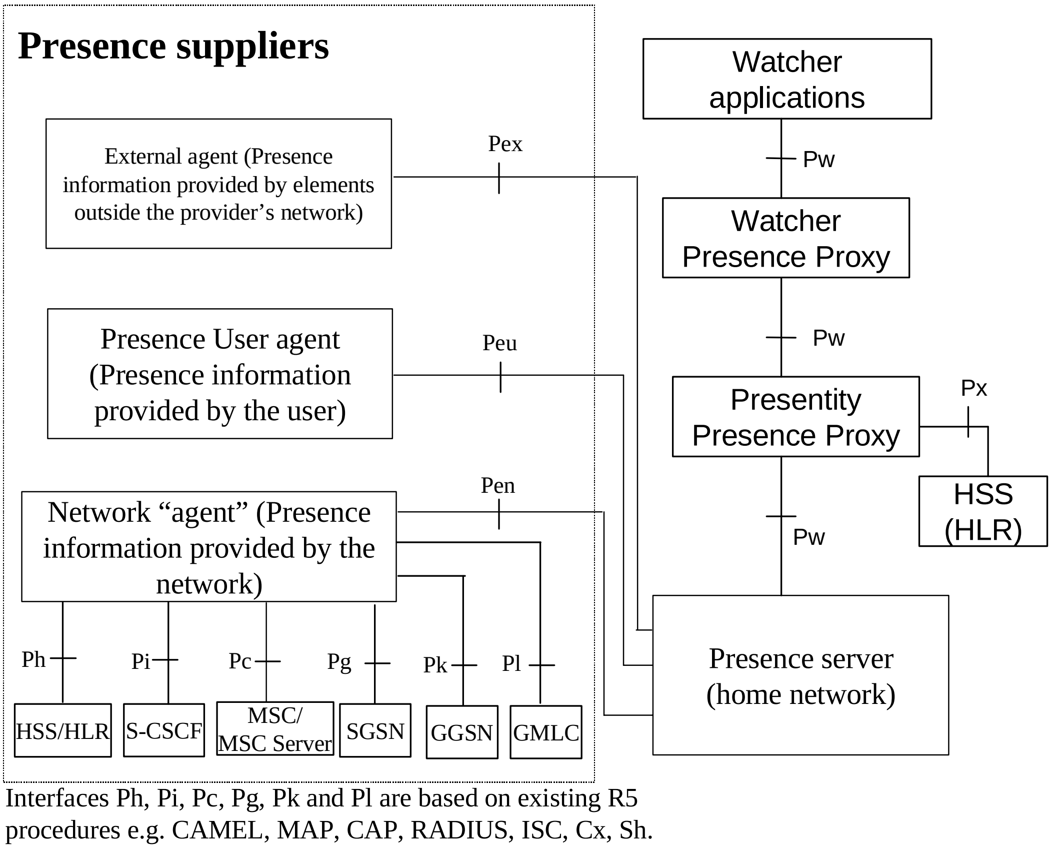

Presence suppliers
External agent (Presence information provided by elements outside the provider's network)
Presence User agent (Presence information provided by the user)
Network "agent" (Presence information provided by the network)
Pex
Peu
Pen
Ph
Pi
Pc
Pg
Pk
Pl
HSS/HLR
S-CSCF
MSC/ MSC Server
SGSN
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

4.1 Reference points

4.1.1 Reference point Presence User Agent – Presence Server (Peu)

This interface shall allow a presentity's presence information to be supplied to the Presence Server. [3] provides guidelines for such an interface. The transport on this interface shall not impose any limitations on the size of the presence information.

Peu shall provide mechanisms for the Presence User Agent to manage access rules.

In order to provide all the functionalities required on this interface, a combination of multiple protocols may be used.

4.1.2 Reference point Network Agent – Presence Server (Pen)

This interface shall allow a presentity's presence information to be supplied to the Presence Server. [3] provides guidelines for such an interface. The transport on this interface shall not impose any limitations to the size of the presence information.

Pen shall provide mechanisms for the Network Agent to manage access rules.

In order to provide the all the functionalities required on this interface, a combination of multiple protocols may be used.

This interface shall allow the Presence Server to request and cancel the request for presence information and associated updates from the Network Agent.

4.1.3 Reference point External Agent – Presence Server (Pex)

This interface shall allow a presentity's presence information to be supplied to the Presence Server. [3] provides guidelines for such an interface. The transport on this interface shall not impose any limitations on the size of the presence information.

In order to provide all the functionalities required on this interface, a combination of multiple protocols may be used. Presence information obtained from an external network by the External Agent is transferred across the Pex reference point to the Presence Server.

4.1.4 Reference point Watcher applications – Presence Server (Pw)

This interface shall allow a Watcher application to request and obtain presence information. [3] provides guidelines for such an interface.

The transport shall not impose any limitations to the size of the presence information.

In order to provide the all the functionalities required on this interface, a combination of multiple protocols may be used.

This interface shall support both presence subscription and fetching operations.

4.1.5 Reference point HSS/HLR – Network agent (Ph)

This interface shall allow the Network agent to query HSS/HLR about the state and status of a subscriber (associated with a presentity) from the Circuit Switched, GPRS and IMS perspective. This interface may also allow the enabling of receiving updates of presence information.

4.1.6 Reference point S-CSCF – Network agent (Pi)

The S-CSCF may provide IMS-specific presence information (e.g. about ongoing IMS sessions). This interface shall use mechanisms defined for the ISC interface.

4.1.7 Reference point Presentity Presence Proxy – HSS (Px)

This interface shall assist locating the Presence Server of the presentity.

4.1.8 Reference point Network Agent – GMLC (Pl)

This reference point shall be used to retrieve location information related to a subscriber (associated with the presentity). This reference point is based on the Le interface as defined in TS 23.071.

4.1.9 Reference point Network Agent – SGSN (Pg)

This reference point shall allow the SGSN to report mobility management related events to the Network Agent (such as attach/detach/routing area update). This capability exists in Release 5 as a MAP interface, where the mechanisms for reporting mobility management events are already defined.

4.1.10 Reference point Network Agent – MSC/MSC Server (Pc)

This reference point shall allow the MSC/MSC Server to report the mobility management related events to the Network Agent (such as attach/detach/location area update). This capability already exists in Release 99, where the mechanisms for reporting mobility management events are already defined.

4.1.11 Reference point Network Agent – GGSN (Pk)

This reference point shall allow the GGSN to report presence relevant events to the Network Agent (such as PDP context activation/de-activation). This capability already exists in Release 99 as a RADIUS interface. The mechanism for reporting of access requests is already defined [13].

4.2 Support of OSA Presence Service Capability Server in the Presence Architecture

This section describes how an operator could use the OSA API to allow an external application to access the presence service features offered by the Home Network. The application would then be able to register as presentity and/or watcher, to supply presence information, to request presence information, to be notified of subsequent changes, to request watcher information, to manage access rules (c.f. TS 22.127). From the Presence Server point of view, the OSA Presence SCS would then act like a presentity or a watcher.

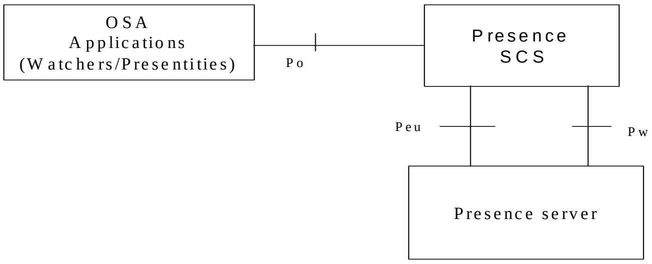


Figure 2. Presence Architecture showing support of OSA

4.2.1 Reference point Po between OSA application Watcher/Presentity and the Presence SCS

This reference point shall allow OSA applications:

1. to register as a watcher, to request a presentity's presence information and to be notified of changes in the presence information. This shall be based on an Application Programming Interface (API) in line with the architectural principles of OSA 23.127 and shall fulfil the agreed requirements defined in 22.127.

2. to register as a presentity, to publish presence information, to retrieve watcher information and to manage related parameters (e.g. access rules). Presence management may include the setting of user preferences, the update of access rules…etc. This shall be based on an Application Programming Interface (API) in line with the architectural principles of OSA 23.127 and shall fulfil the agreed requirements defined in 22.127.

5 Functional Description of Network Elements

Editors note: This chapter describes the Presence Service specific functionalities of existing network elements and possible new network elements.

5.1 Presence Server

The Presence Server resides in the presentity's home network.

The Presence Server shall manage presence information that is uploaded by the Presence User/Network/External agents, and is responsible for combining the presence-related information for a certain presentity from the information it receives from multiple sources into a single presence document.

The mechanisms of combining the presence related information will be defined based on presence attributes, and according to certain policy defined in the Presence Server. The Presence Server is not required to interpret all information, the information that the Presence Server is not able to interpret shall be handled in a transparent manner.

The Presence Server shall also allow users to fetch and subscribe for receiving presence information.

The Presence Server shall support internetwork operability mechanisms to allow for an interoperable Presence Service across multiple operators' networks and domains (e.g. external Internet). Mechanisms for locating the Presence Server shall be developed, especially with respect to these internetwork operability aspects.

The Presence Server shall support SIP-based communications with the Presentity Presence Proxy. In the IMS the Presence Server is seen as a SIP Application Server, and is located using SIP URLs, standard SIP and existing IMS mechanisms (SIP routing, HSS query, ISC filtering, etc…).

The Presence Server shall support authorization and security mechanisms, at least the following levels of authorization are foreseen:

- Providing presence information to any Watcher application that requests it
- Provide presence information to only those Watcher applications in an "allowed" list

The Presence Server may also support authorization and security mechanisms that is based on asking permission from the Presence User agent on a case-by-case basis.

The Presence Server may support rate-limiting or filtering of the presence notifications based on local policy in order to minimize network load.

The Presence Server could be extended to a generic State Agent, supporting subscriptions and notifications regarding other types of events than presence as well. An example for such event is the combined presence of a whole buddy list.

5.2 Watcher and Presentity Presence Proxy

When a Watcher application intends to access some presence information of a presentity, it first needs to find the Presence Server containing this information.

The Watcher Presence Proxy provides the following functionality:

- Address resolution and identification of target networks associated with a presentity;
- Authentication of watchers;
- Interworking between presence protocols for watcher requests;
- Generation of accounting information for watcher requests.

The Presentity Presence Proxy provides the following functionality:

- Determination of the identity of the presence server associated with a particular presentity;
- Generation of accounting information for updates to presence information.

The Presentity and or the Watcher Presence Proxies may also be responsible for providing network configuration hiding. This is for further study.

The more exact functionalities of the Watcher and Presentity Presence proxy depends on the relative location and trust relations of the Watcher application and the Presence Server as detailed in section 5.6.2 and 5.6.4

Communications between the Presentity Presence Proxy and the Watcher Presence Proxy shall be based on SIP as shown in figure 3 below. Other IP-based mechanisms may also be needed to support the delivery of large amount of presence information. Support for non-SIP based Watchers may be provided by the use of an interworking functions located at the Watcher Presence Proxy.

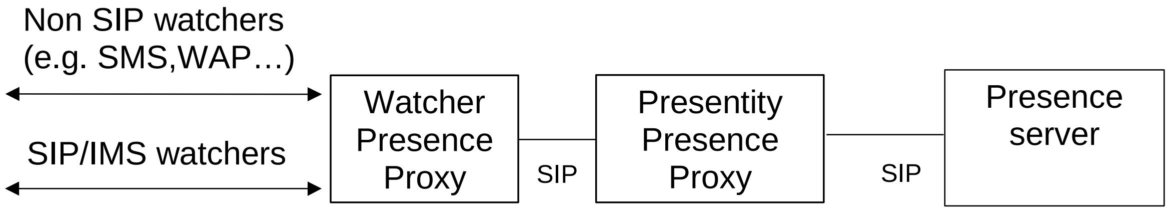


Figure 3. Communications between the Presentity Presence Proxy and the Watcher Presence Proxy for Watchers

5.3 External Agent

The Agent elements in the Presence Architecture are functionally distinct from the Presence Server functional element. The generic function of the Agent elements is to make presence information available to the Presence Server element in standardized formats across standardized interfaces.

The External Agent element provides the following functionality:

- The External Agent supplies Presence information from external networks.
- The External Agent sends the Presence information across the Pex interface according to the format standardized for the Pex interface.
- The External Agent handles the interworking and security issues involved in interfacing to external networks.

Examples of Presence Information that the External Agent may supply, include:

- Third party services (e.g. calendar applications, corporate systems)
- Internet Presence Services
- Other Presence Services

5.4 Presence User Agent

The Agent elements in the Presence Architecture are functionally distinct from the Presence Server functional element. The generic function of the Agent elements is to make presence information available to the Presence Server element in standardized formats across standardized interfaces.

The Presence User Agent element provides the following functionality:

- The Presence User Agent collects Presence information associated with a Presentity representing a Principal.
- The Presence User Agent assembles the Presence information in the format defined for the Peu interface.
- The Presence User Agent sends the Presence information to the Presence Server element over the Peu interface.
- The Presence User Agent shall be capable of managing the Access Rules.

- The Presence User Agent shall handle any necessary interworking required to support terminals that do not support the Peu reference point.

From a conceptual view, the Presence User Agent (PUA) element resides between the presence server and the user's equipment as illustrated in the reference architecture in figure 1. In reality, a Presence User Agent may be located in the user's terminal or within a network entity.

Where the PUA is located in a terminal, the terminal shall support the Peu interface to the presence server as illustrated in Figure 4 below.

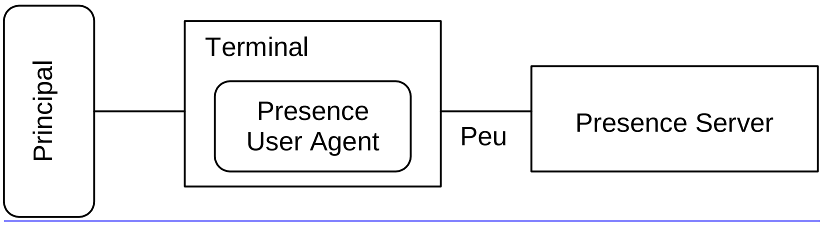


Figure 4. Terminal based Presence User Agent

Where the PUA is located within the network, the particular network entity shall support the Peu interface to the presence server as illustrated in Figure 5. In such a case an additional functionality may be required to resolve the location of the presence server associated with the presentity.

In this case, the interface between the terminal and the Presence User agent is outside of the scope of standardisation of the presence service.

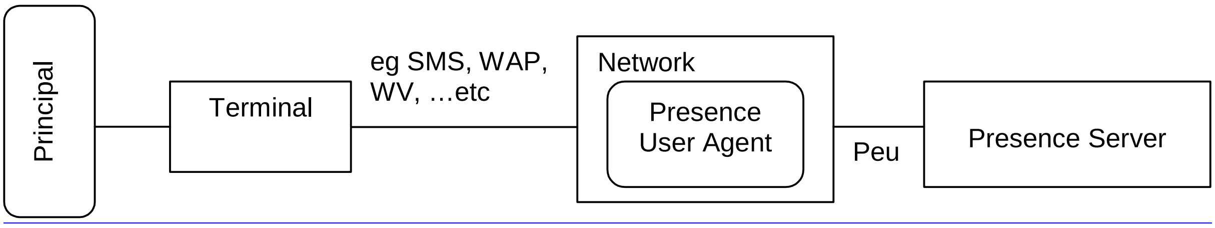


Figure 5. Network based Presence User Agent

5.5 Network Agent

The Agent elements in the Presence Architecture are functionally distinct from the Presence Server functional element. The generic function of the Agent elements is to make presence information available to the Presence Server element in standardized formats across standardized interfaces.

The Network Agent element provides the following functionality:

- The Network Agent receives Presence information from network elements within the Operator's network.
- The Network Agent associates Presence information with the appropriate Subscriber/Presentity combination.
- The Network Agent converts the Presence information into the format standardized for the Pen interface.
- The Network Agent sends the Presence information across the Pen interface.
- The Network Agent may Push Presence information to the Presence Server alternatively some network elements may be queried, signaled, or provisioned to deliver Presence information. For those elements that require querying or signaling, the Presence Server makes a request to the Network Agent directing it to acquire the Presence information. The Network Agent then issues the appropriate commands to the element.

5.5.1 Suppliers of Presence Information

The Network Agent may receive Presence information from one or more of the following 2G/3G network elements over the specified interface:

Network Element supplying Presence Information	Reference Point
HSS/HLR	Ph
S-CSCF	Pi
MSC/MSC Server	Pc
SGSN	Pg
GGSN	Pk
GMLC	Pl

Editors Note: The appropriate mechanism to be used by each element Push or subscribe/notify is FFS.

5.6 Presence Server and Watcher application located in an IMS network

Figure ~~4~~ 6 below presents the mapping of the Watcher and Presentity Presence Proxy functionalities to IMS network elements when located within the IMS along with the Watcher application. This mapping is based on and restricted to reusing the existing IMS architecture mechanisms and can be clearly seen in the detailed information flows show in section 7.1.

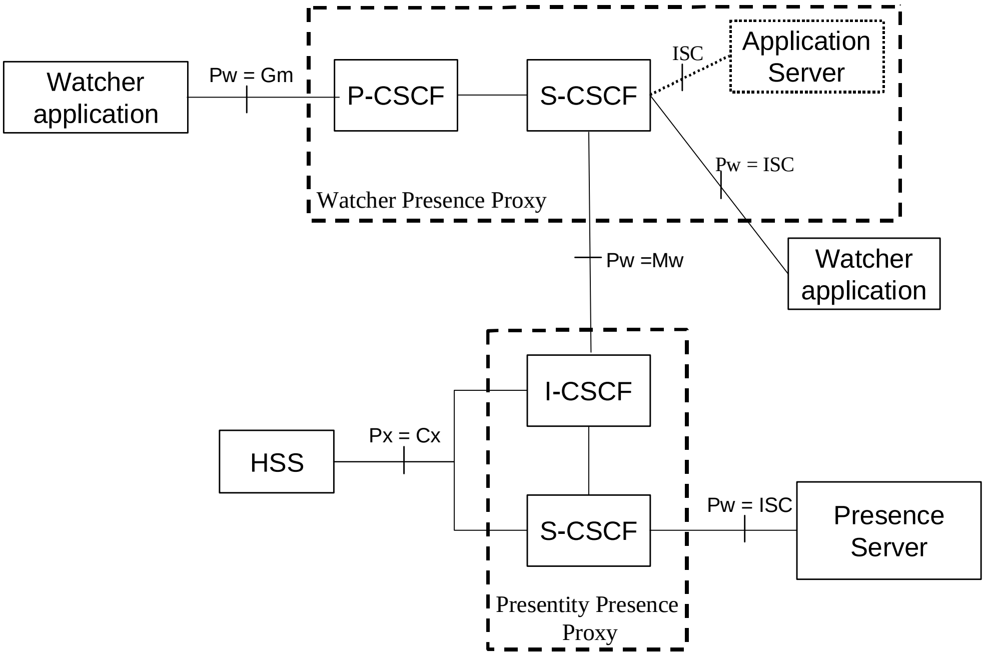


Figure ~~4~~6: Both the Watcher application and the Presence Server located within IMS

Note-i: In order to apply optimizations for wireless environment, such as those proposed in [12], the Watcher Presence Proxy functionality may be augmented by an Application Server. Figure ~~4~~ 6 presents such an Application Server as a dotted box. Such an Application Server would allow a Watcher Application to subscribe to the presence of several presentities with a single SUBSCRIBE transaction. Other solutions for such aggregated SUBSCRIBE mechanisms are also possible, e.g. via an Application Server located in the presentity's IMS network.
This optimizations would help the scalability of the system.

Note-ii: The standard IMS (SIP) routing mechanisms define whether a certain CSCF is indeed included in the path of a SUBSCRIBE or NOTIFY transaction.

As described in [4], the Watcher Application sends a SIP SUBSCRIBE to Event: presence addressed to the presentity's SIP URL to subscribe or fetch presentity's presence information. This SUBSCRIBE transaction will be routed and handled by the IMS infrastructure according to standard IMS routing and ISC procedures defined in [9] and [10]. The presence document will be provided from the Presence Server to the Watcher Application using SIP NOTIFY along the dialogue setup by SUBSCRIBE either within the NOTIFY payload, or via a URL provided in the NOTIFY. The means to fetch the content can be seen as part of the Pw interface.

5.6.1 Watcher application in the IMS

There are two alternatives to locate a Watcher application in an IMS network:

- The Watcher application can be located within a UE registered in the IMS network, it is registered to a S-CSCF via a P-CSCF – according to standard IMS procedures.
- The Watcher application can be located within an AS behind an ISC interface.

5.6.2 Watcher Presence Proxy in the IMS

The functionalities of the Watcher Presence Proxy are then taken care of by the P-CSCF and the S-CSCF:

- The S-CSCF is responsible for authentication according to procedures described in [5].
- The charging and accounting procedures are conducted as per procedures defined by [6], [7].
- The security mechanisms between the Watcher and the Presentity Presence proxy is defined by [8].

5.6.3 Presence Server in the IMS

When the presentity is associated with a UE that has subscribed to an IMS network, according to the home control model its Presence Server shall also be located within the presentity's home IMS network. The Presence Server within the IMS is a SIP Application Server as defined by [9].

Figure 7 below presents the architecture for the S-CSCF and the HSS to provide presence related information to the Presence Server.

Note: The architecture on Figure 7 is an IMS-specific simplification of the generic Presence reference architecture presented in Section 4.

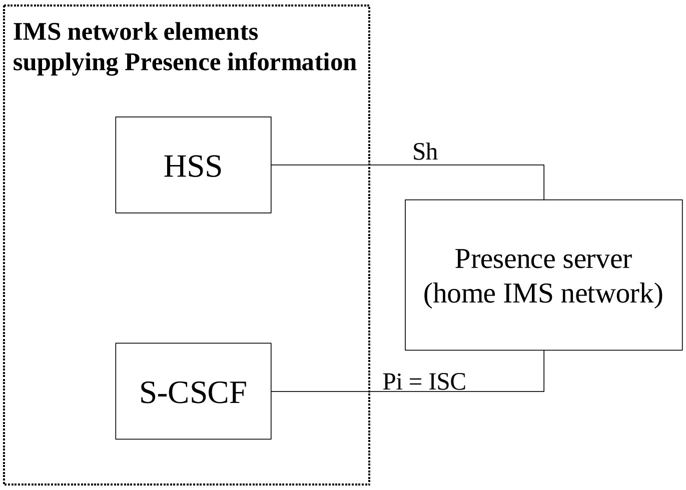

IMS network elements supplying Presence information
HSS
Sh
Presence server (home IMS network)
S-CSCF
Pi = ISC

Figure 7: IMS network elements supplying presence information

The ISC interface is used to convey presence information from the S-CSCF to the Presence Server. More specifically, the functions of the Pi interface are taken care of by the ISC interface. As an example, the S-CSCF can convey a user's IMS-registration status by generating and sending a 3rd party REGISTER request to the Presence server.

The Sh interface is used to convey information from the HSS to the Presence Server.

5.6.4 Presentity Presence Proxy in the IMS

The functionalities of the Presentity Presence Proxy are taken care of the following way:

- The procedures for locating, routing to and accessing the Presence Server of the presentity are defined in [9] and [10]. These procedures also take care of routing and accessing the Presence Server of a presentity that is associated with an unregistered UE.

5.7 Presence Server located in the IMS, Watcher application located in the external Internet

For a Presence Server located within IMS, the functionalities of the Presentity Presence Proxy are as described in Section 5.6.4.

For a Watcher application located in the external Internet, the Watcher Presence Proxy may reside in a network capable of executing security functionalities as per procedures defined in [8].

The interworking with Watcher Applications located in the external Internet not supporting the standard Pw interface is out of the scope of this TR.

5.8 Presence Server located in the external Internet, Watcher application located in the IMS

For a Watcher Application located within IMS, the functionalities of the Watcher Presence Proxy are as described in Section 5.6.2. Depending on the mechanisms and protocols supported by the external Presence Server, the Watcher Presence Proxy may implement additional functionalities, e.g. mapping.

The interworking with Presence Servers located in the external Internet not supporting the standard Pw interface is out of the scope of this TR.

6 Presence attributes

Editors note: This chapter describes the Presence Service attributes.

6.1 Presence Attributes

Presence attributes describe the presentity. As the type of the presentity can vary significantly the definition of generic attributes is practically impossible. In 3GPP, the only attributes that are defined describe the 3GPP subscriber type of presentity. Other attributes can be defined by the service providers and manufacturers as part of the other presence markup as specified in IETF (e.g. RFC 2778, RFC 2779). The values (and process of generating them) and value ranges for all attributes shall be kept relatively simple. It is necessary for the 3GPP subscriber to understand how the values are set/modified as it may have direct impact to whom the access to presence data is given (as defined by the admission rules).

6.1.1 3GPP Subscriber Presence Attributes and Values

3GPP subscriber is described with attributes: *subscriber's status*, *network status, one or more communication address(es)* (containing *communication means* and *contact address*), *subscriber provided location*, *network provided location, priority, text.* All these attributes shall be able to contain value NULL to enable polite blocking.

The following Table1 lists the values for the numbers of attributes, which are currently defined by S1. It may be extended in the future dependent on user and operator 's requirements. The values can be setup and modified by user or operator.

Table 1: Presence service attributes for 3GPP subscriber

Attribute	Values
Subscriber's status[1]	~~Open, (* the definition came from S1 which include all wireless devices*)~~ ~~Closed,~~ ~~Not Disclosed~~ Willing Willing with limitations Not willing Not Disclosed

Network status	**CS domain** {FFS}
	PS domain {FFS}
	IMS domain (2 sets of attributes) {Registered, Not registered}

Communication means	Service type (telephony, SMS, email, multimedia messaging service (SIP), instant messaging service etc.)
Contact address	E.164 (e.g. MSISDN), SIP URL, Email, Instant message address e.g. M:name@domain name
Subscriber provided location	Free Format Text
Network provided location	Last known CGI/SAI and/or geographic co-ordinates and age of location information
Priority	Values (FFS)

Text	Free Format Text

[1] The semantics for the values of the subscriber's status are:

Willing, 3GPP subscriber is willing to communicate

Willing with limitations, 3GPP subscriber may be willing to accept some communication

Not willing, 3GPP subscriber is not willing to communicate

Not disclosed, 3GPP subscriber does not reveal his status

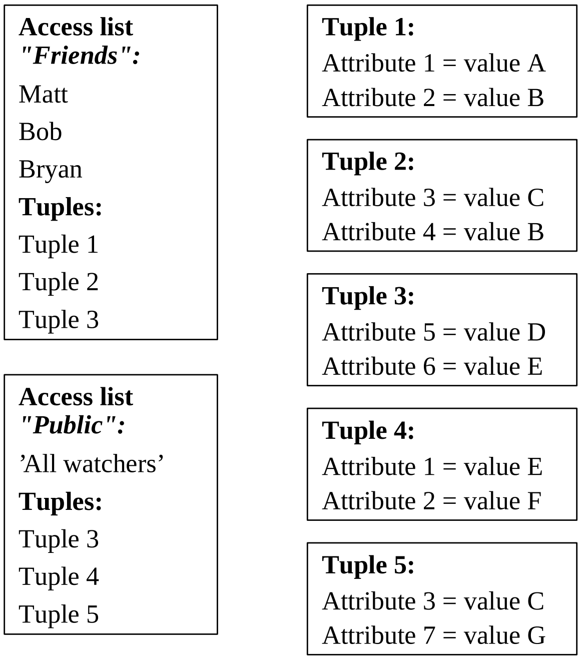
NOTE1: The subscriber's status describes the principal's willingness to communicate. The information is primarily intended to be used for human interpretation.

NOTE2: The user interface of the terminal may or may not present the values as defined in the table, alternatives such as icons, etc. may be used instead. (It is an implementation and service provisioning option how the values are presented).

6.1.2 Presence Structure to Support Multiple Values for Attributes

Attributes are mapped to separate tuples which have unique identifiers. If the presentity wants to show different presence information concerning one attribute to different watchers the presentity shall create more than one tuple that contain the same attribute with different value. Separate tuples are assiociated to different watchers and watcher groups based on the access rules. The presentity controls the value of the attribute by modifying the corresponding tuple. Figure ~~5~~ 8 illustrates how different values for different watchers are provided utilising access rules.

NOTE: The figure ~~5~~ 8 is illustrative only and it shall not mandate or limit the server implementation options.



Access list *"Friends":*
Matt
Bob
Bryan
Tuples:
Tuple 1
Tuple 2
Tuple 3

Access list *"Public":*
'All watchers'
Tuples:
Tuple 3
Tuple 4
Tuple 5

Tuple 1:
Attribute 1 = value A
Attribute 2 = value B

Tuple 2:
Attribute 3 = value C
Attribute 4 = value B

Tuple 3:
Attribute 5 = value D
Attribute 6 = value E

Tuple 4:
Attribute 1 = value E
Attribute 2 = value F

Tuple 5:
Attribute 3 = value C
Attribute 7 = value G

Figure ~~5~~8: Illustration how access lists are utilised to present different values of the same attribute to different watchers

6.2 Presence Information Model

Editors note: This information is currently also in the stage 1 specification and in some phase the information has to be deleted either from the stage 1 or stage 2 specification.

A logical model of a presentity's presence information consists of an arbitrary number of elements, known as presence tuples, as depicted in figure ~~6~~9. Such presentation enables presence to be independent service and not being dependent on other services. Each tuple consists of *status* marker, optional *communication address* (includes *communication means* and *contact address*) and optional other presence markup. Presence information for each presentity is identified by a unique identifier furthermore each tuple is uniquely identified.

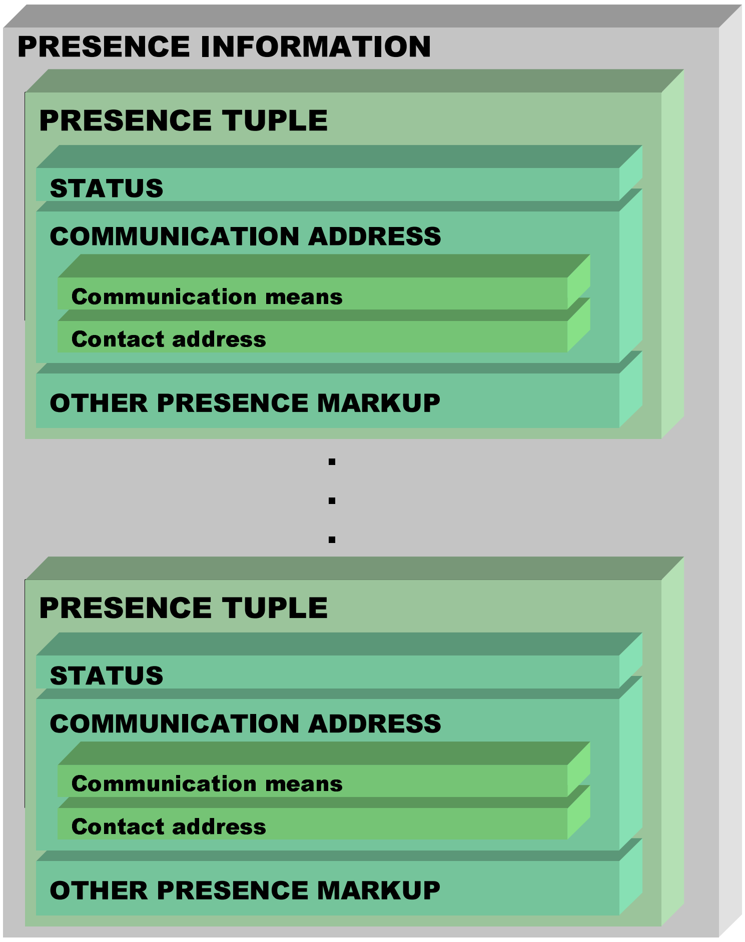


Figure ~~6~~9: Presence information

- status

Table ~~1~~2: Status

Item	Explanation
status	Indicates the current condition of the presentity represented by the presence tuple

- communication address (optional)

  consists of a communication means and a contact address

Table ~~2~~3: Communication address

Item	Explanation
Communication means	Information indicating a method whereby communication can take place
contact address	Information indicating a specific point of contact via some communication means

- other presence markup (optional)

  any additional presence information

6.2.1 3GPP subscriber attribute mapping to tuples

The presence information format consists of one or several tuples. Each tuple consists of number of attributes that describe the presentity. When the presentity is a 3GPP subscriber; he/she shall have one tuple describing his/her personal status that does not necessarily have any link to any client or device. The 3GPP SUBS tuple contains at minimum the following information and it is mapped to tuple structure as shown in table 4:

Table 4: 3GPP SUBS tuple.

Attribute	Attribute's location in 3GPP SUBS tuple
Subscriber's status	Status
Subscriber provided location	Other presence markup
Text	Other presence markup

NOTE: The details of the attribute mapping are to be worked out in stage 3.

The remaining information describing the status of the 3GPP subscriber shall be arranged to one or several other tuples as described in table 5.

Table 5: Attribute mapping to tuples in case of 3GPP subscriber's client or device related presence information

Attribute	Attribute's location in tuple_n (client)[1]
Client or devices status[1]	Status
Network status	Other presence markup
Communication means	Communication means
Contact address	Contact address
Network provided location	Other presence markup
Priority	Other presence markup
Text	Other presence markup
NOTE 1: Status field is mandatory in each tuple. The field shall be filled with client specific information e.g. in case of instant messaging the value is either *open* or *closed.*	

NOTE: The details of the attribute mapping are to be worked out in stage 3.

7 Access rules

Access rules define the watchers who can ~~contain the identities of the watchers (in case of anonymous watchers can be e.g. anybody) that are allowed to~~ access the presence information of the presentity. In addition to the watcher identities, the access rules contain the presence information or reference to the presence information that is allowed to be accessed by the listed watchers. The access lists can be logically arranged to be part of the presence server or a separate entity in the network. ~~e.g. PPR (Privacy Profile Register).~~

Access lists can be divided into three different categories: personal~~private~~ access lists, public access lists and blocking lists.

Personal and general access lists define which watchers can access which information. Personal access lists explicitly identify watchers, while general access lists relate to groups of watchers whose exact identities are not necessarily known by the presentity e.g. “all watchers” or “all 3GPP watchers”.

Blocking lists define watchers that are not allowed to access any presence information related to the presentity.

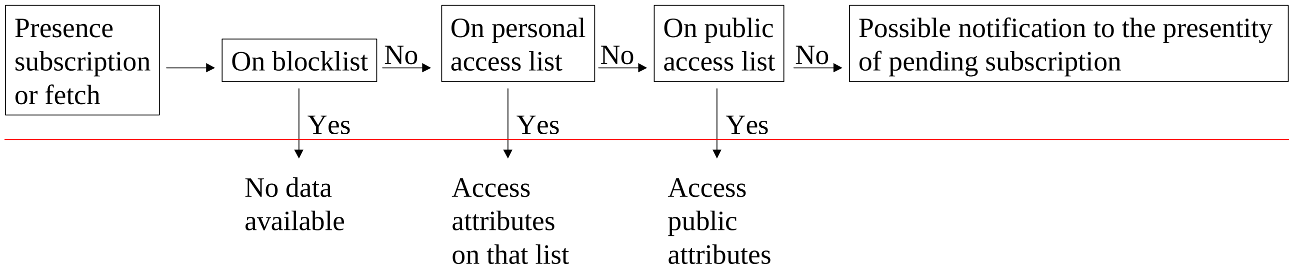
A presentity shall be able to manage several personal and general access lists as well as blocking lists.

The three access list categories shall be evaluated in the following order: blocking lists, personal access lists and general access lists.

The following shows an example where the presentity has defined a single access list for each category.

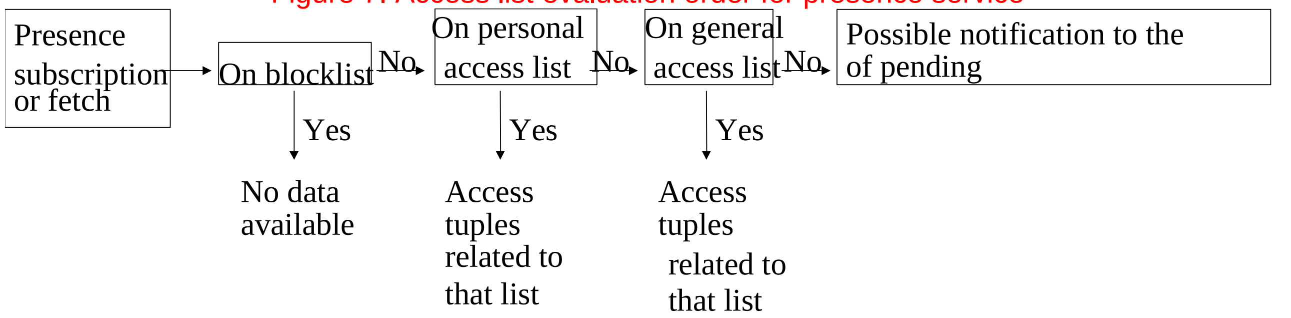
~~To ensure correct operation of presence service the access lists have to be evaluated in a defined order as presented below (described in Figure 7).~~ In this particular example, o~~O~~nce the hit is found the evaluation is halted and presence information according to access is delivered.

1. Is the watcher on the blocking list?
2. Is the watcher on the personal access list ~~(there can be several personal access lists)~~?
3. Is the watcher on the general~~public~~ access list (created e.g. by service provider containing all watchers)?
4. Send a notification to the presentity of pending access request.



Presence subscription or fetch
On blocklist
No
On personal access list
No
On public access list
No
Possible notification to the presentity of pending subscription
Yes
Yes
Yes
No data available
Access attributes on that list
Access public attributes

~~Figure 7. Access list evaluation order for presence service~~



Presence subscription or fetch
On blocklist
No
On personal access list
No
On general access list
No
Possible notification to the of pending
Yes
Yes
Yes
No data available
Access tuples related to that list
Access tuples related to that list

Figure 10. Example of access list evaluation order for presence service

8 Information flows

Figure ~~8~~ 11 illustrates the message flow for user A requesting presence information for user B in a different network.

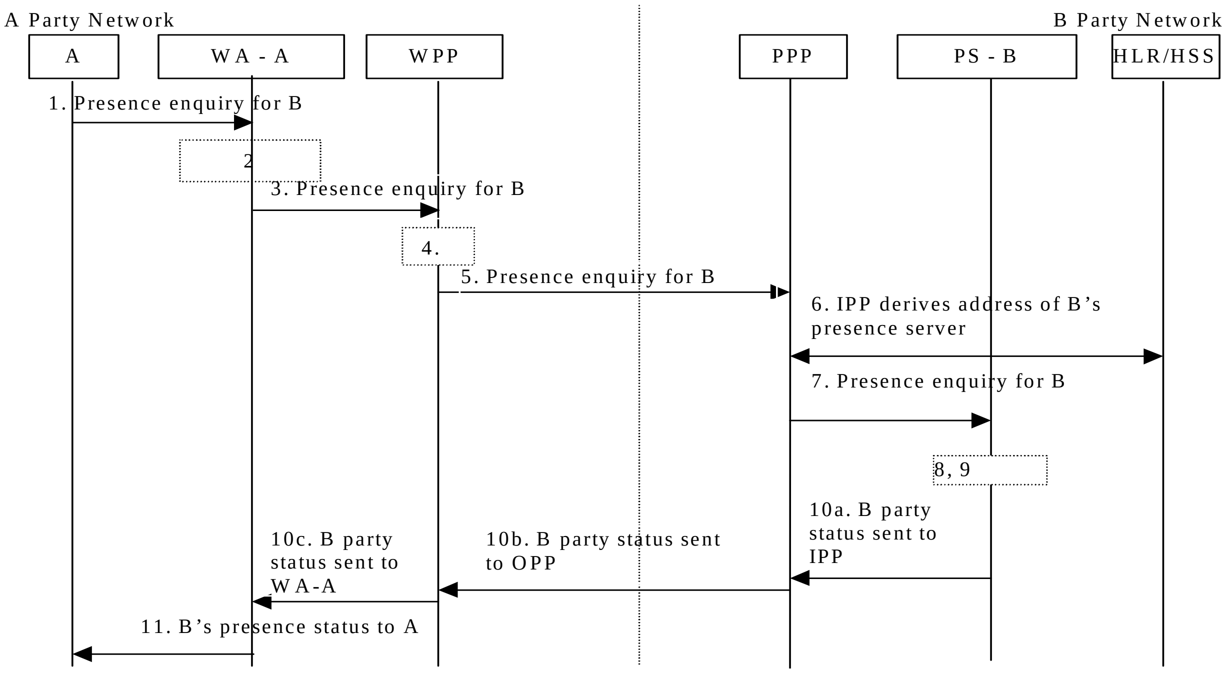

A Party Network
B Party Network
A
WA - A
WPP
PPP
PS - B
HLR/HSS
1. Presence enquiry for B
2
3. Presence enquiry for B
4.
5. Presence enquiry for B
6. IPP derives address of B's presence server
7. Presence enquiry for B
8, 9
10a. B party status sent to IPP
10b. B party status sent to OPP
10c. B party status sent to WA-A
11. B's presence status to A

Figure ~~8~~11: Presence enquiry message flow

1. The A party sends a presence enquiry to Watcher Application A (WA-A). The A party identifies B by B's address (e.g. MSISDN or URI). The enquiry can be of various types, e.g.:

   a) "tell me the current state of B"

   b) "tell me all state changes of user B for the next x hours"

   c) "tell me when B next changes state"

   d) "stop telling me about B"

2. Watcher Application A 'authenticates' A and checks their credit status (details of authentication and credit status are outside scope of this message flow)
3. Watcher Application A sends a "Presence enquiry for B" message to Watcher Presence Proxy (WPP).
4. The Watcher Presence Proxy derives B's network name from B's address (details of how this is derived is outside the scope of this message flow).
5. The Watcher Presence Proxy sends a "Presence enquiry for B" message to B's network's Presentity Presence Proxy (PPP).

   Note: Authentication may be necessary between A and B party networks in line with techniques used in other instances of inter operator message flow; precise details are outside the scope of this message flow.

6. The Presentity Presence Proxy derives the address of B's Presence Server
7. B's network PPP sends "Presence enquiry for B" message to B's Presence Server.

8. B’s Presence Server processes the presence enquiry request (e.g. check A is one of B’s buddy’s and B still wants A to watch him/her).
9. B’s Presence Server raises charge record for A against A’s network (precise details are for further study)
10. B’s Presence Server sends B’s status back to Watcher Application A in Originating PLMN (may be returned via PPP and WPP).
11. Watcher application returns B’s presence to use A.

NOTE 1: Steps 10 and 11 are repeated as necessary if B party has been requested to provide regular presence updates.

NOTE 2: In the event that the presence enquiry message is “stop telling me about B” steps 8-11 are just an acknowledgement for watcher application A.

8.1 Detailed information flows

8.1.1 Overview of flows used

The messages used in this section are representative and are not meant to indicate any particular protocol as this is outside the scope of this document. In this section the following messages have been used:

SubscribePres: This is a request by a watcher to obtain presence information about a presentity. The message may be used to either request the current presence information or to subscribe to updates of presence information for a particular time period. This flow may also be used to un-subscribe to periodic updates. The request needs to convey the presence related events that that the watcher is be interested in. A presence server may accept or deny such a request.

MsgAck: This is a generic message acknowledgement for the message flows. It may be used to indicate a positive or negative acknowledgement. In the latter case, the message may convey an indication for the rejection.

Query: This message is used by a Presentity presence proxy to request the HSS/HLR to provide the necessary information to locate a presence server that is associated with a presentity.

Resp: This message is the reply by the HSS/HLR to provide the required information to the Query message above.

NotifyPresUp: This message is used to notify a watcher of updates to a presentitiy’s presence information. The watcher would have either requested the current presence information or had previously subscribed to periodic updates. The message may contain the presence information or a pointer to the information.

PresUpdateMsg: This message is used by a Presence user agent to provide updates of a presentity’s presence information to a presence server. This message needs to be able to convey the presence information associated with a presentity. The message may contain the presence information or a pointer to the information. (Note: there are similarities with the *NotifyPreseUp* message listed above since they both convey presence information. However for simplicity, different message names are used).

8.1.2 Flows demonstrating how watchers subscribe to presence event notification

The section covers the flows that show how watchers can request presence information about a presentity.

8.1.2.1 IMS Watcher and IMS Presentity in the same or different IM-CN

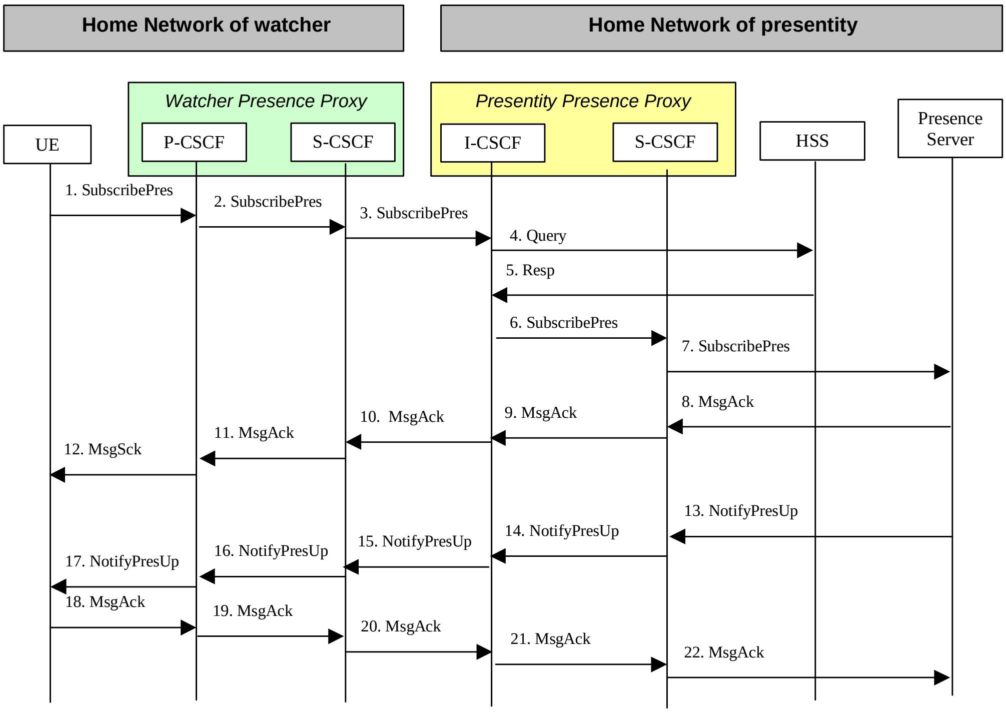


Figure ~~9~~12. IMS Watcher registering for event notification

Figure ~~9~~ 12 shows an IMS watcher subscribing to presence event notification about an IMS based presentity. The presentity may either be in the same IM-CN subsystem as the watcher or may be in a different IM-CN subsystem. The flows for both these cases are the same. The details of the flows as follows:

1. A watcher agent in a UE wishes to watch a presentity. To initiate a subscription, the UE sends a *SubscribePres* message request containing the presence related events that it wishes to be notified of, together with an indication of the length of time this periodic subscription should last. The UE sends the *SubscribePres* information flow to the proxy (subscriber identity, home networks domain name).

2. The P-CSCF remembers (from the registration process) the next hop CSCF for this UE. In this case the *SubscribePres* is forwarded to the S-CSCF in the home network. In this case, the P-CSCF and the S-CSCF act as a Watcher Presence Proxy.

3. The S-CSCF is unable to resolve the presence server address of the presentity that the UE is requesting to watch, and as a result forwards the *SubscribePres* message to the an I-CSCF offering part of the Presentity Presence Proxy functionality. The S-CSCF shall examine the home domain of the presentity associated with the request and if the request is for a presentitiy outside the operator's domain, it determines the external I-CSCF. If the request is for a presentity in the same domain, the S-CSCF forwards the request to the local I-CSCF.

4. The I-CSCF examines the presentity identity and the home domain identity and employs the services of a name-address resolution mechanism to determine the HSS address to contact. The I-CSCF shall query the HSS to obtain the address of the S-CSCF associated with the Presentity. It shall query the HSS via a Query message.

5. The Query Resp message from the HSS provides the name of the S-CSCF associated with the presentity.

6. The I-CSCF, using name of the Presence Server shall determine the address of the S-CSCF through a name-address resolution mechanism. The *SubscribePres* message is forwarded to the S-CSCF.

7. The S-CSCF using any necessary filtering criteria forwards the *SubscribePres* message to the appropriate Presence Server.
8. At this stage the presence server performs the necessary authorisation checks on the originator to ensure it is allowed to watch the presentity. Once all privacy conditions are met, the presence server issues a *MsgAck* to the S-CSCF . (In the case where the privacy/authorisation checks fail, then a negative acknowledgement is sent to the watcher).
9. The S-CSCF forwards the to the I-CSCF.
10. The I-CSCF forwards the *MsgAck* to the originating S-CSCF.
11. The S-CSCF forwards the *MsgAck* message to the P-CSCF.
12. The P-CSCF forwards the *MsgAck* to the watcher agent in the UE.
13. As soon as the Presence Server sends a *MsgAck* to accept the subscription, it sends the watcher agent a *NotifyPresUp* message with the current state of the presentity to the S-CSCF.
14. The S-CSCF forwards the *MsgAck* to the I-CSCF.
15. The I-CSCF forwards the *NotifyPresUp* to the originating S-CSCF.
16. The S-CSCF forwards the *NotifyPresUp* message to the P-CSCF.
17. The P-CSCF forwards the *NotifyPresUp* to the watcher agent in the UE.
18. The UE acknowledges the receipt of the *NotifyPresUp* message with a *MsgAck* sending this to the P-CSCF.
19. The P-CSCF forwards the *MsgAck* message to the S-CSCF.
20. The S-CSCF forwards the *MsgAck* to the I-CSCF.
21. The I-CSCF forwards the *MsgAck* message to the S-CSCF.
22. The S-SCSF forwards the *MsgAck* to the Presence Server.

8.1.3 Flows demonstrating how presentities update Presence Information ~~Presentities updating presence information to Presence Server~~

~~<Further study required pending clarification and resolution of open issues>~~

8.1.3.1 Updating presence information by terminals without support of the Peu reference point

For the case of terminals that do not support the Peu reference point presence information can be provided alternative mechanisms such as SMS, WAP …etc. The Presence User Agent provides the necessary interworking with the presence server. As previously indicated, the PUA may be located with network entities such as a WAP WML/HTTP server or SMS-C, however this is an implementation issue and outside of the scope of technical report. This particular example is illustrative and shows the case where a user updates presence information through a WAP browser, where the Presence User Agent is located inside the WAP WML/HTTP server and is illustrated in figure 13 below. It is acknowledged that other possibilities exist.

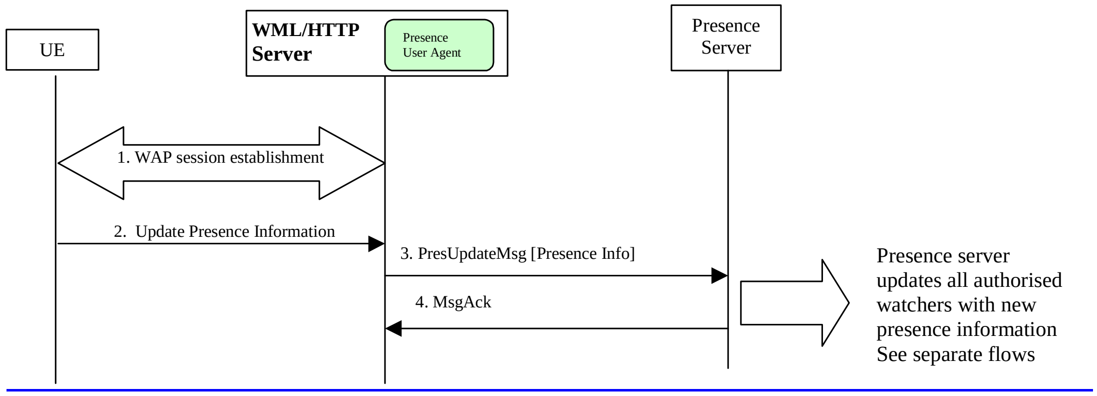

UE
WML/HTTP Server
Presence User Agent
Presence Server
1. WAP session establishment
2. Update Presence Information
3. PresUpdateMsg [Presence Info]
4. MsgAck
Presence server updates all authorised watchers with new presence information See separate flows

Figure 13: Updating presence information via WAP WML/HTTP server

1. The user opens a WAP session by requesting a WAP URL that is dedicated to updates of presence information.

2. Using a WAP browser, the user modifies aspects of ‘user presence information.

3. The WML/HTML server, which in this example hosts the Presence User Agent (although the PUA may be a separate entity, in which case the interface to the PUA will be proprietary), sends a PresUpdateMsg to the Presence Server. Additional functionality may be required to locate the presence server associated by the presentity. In this particular example, it is assumed that the PUA is configured with the appropriate address of the presence server.

4. The Presence Server acknowledges the PresUpdateMag with a MsgAck to the WAP WML/HTTP server.

8.1.3.2 Notification process of the Presence Server within IMS

The following flow describes how the presence server is notified of an event by the network elements.

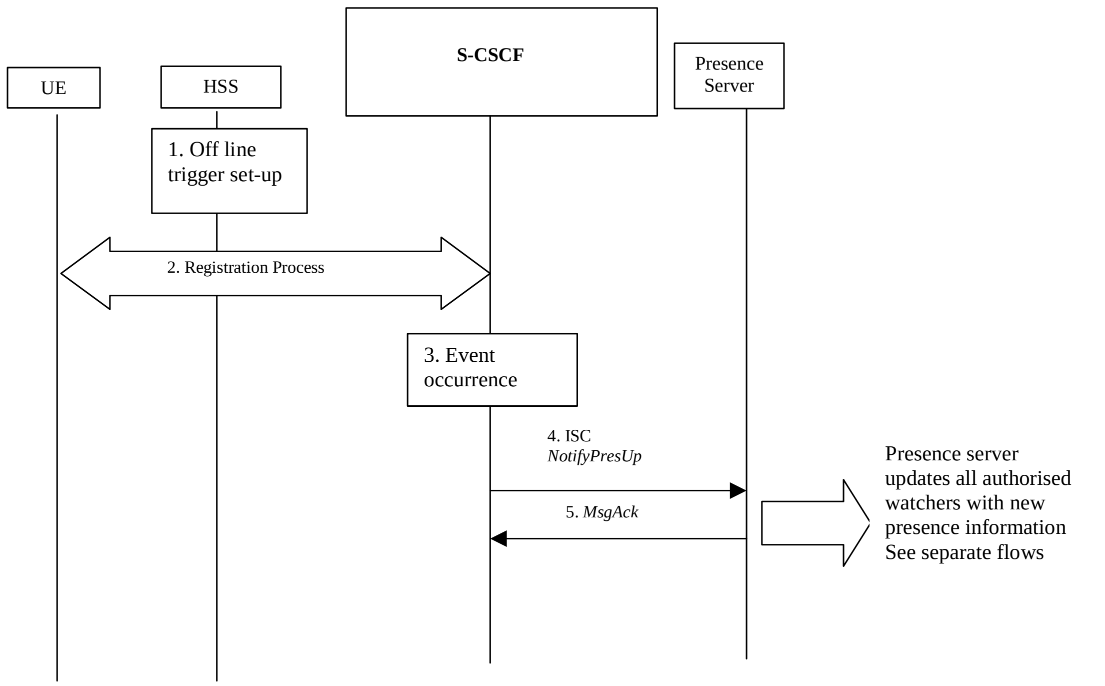


Figure 14 Notification procedure for the Presence Server.

1. For the S-CSCF to report events of a presentity, the filtering criteria associated with the user need to be set. This takes place off-line and is outside the scope of this TR as to how it is achieved.

2. UE registration takes place with the S-CSCF as detailed in TS 23.228 [9]. As part of this process, the filtering criteria are downloaded to the S-CSCF from the HSS. In addition to the presence server address, the filtering criteria contain the event notifications to be reported to the presence server (eg. registration, de-registration).

3. When an event occurs that in the S-CSCF, the *NotifyPresUp* message is generated.

4. The S-CSCF sends *NotifyPresUp* message to the Presence Server via the ISC interface.

5. Prior to notifying all authorised watchers, it acknowledges the receipt of the *NotifyPresUp* message with a *MsgAck* to the S-CSCF.

8.1.3.3 CS/PS Notification process of the Presence Server

The following flow describes how the presence server is notified of an event by the network elements for a CS/PS subscriber.

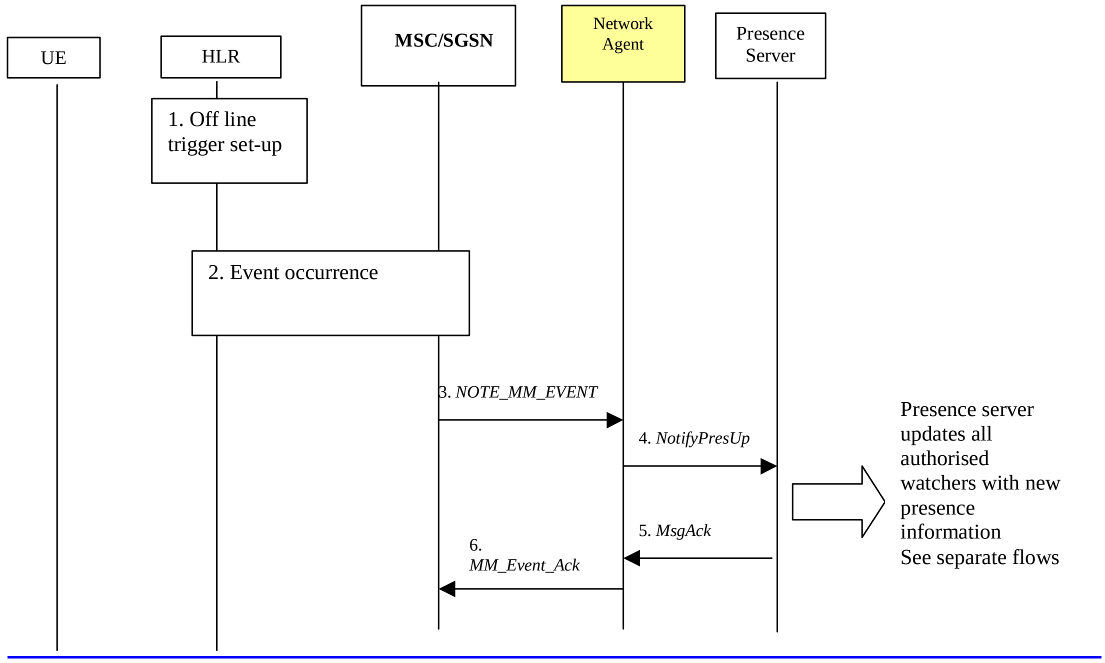


Figure 15 CS/PS Notification procedure for the Presence Server.

1. For network event to be reported on behalf of a CS/PS subscriber, the necessary triggers are armed in the MSC/SGSN. This takes place off-line and is outside the scope of this TR as to how it is achieved.

2. At the occurrence of an event between the HLR and the MSC/SGSN, (e.g UE detach) a notification message is generated.

3. A MAP notification message (NOTE_MM_EVENT) is sent to the Network Agent via Pc/Pg interface on the occurrence of an event, details of this are outside the scope of this flow. There may be some address resolution needed by the network agent to locate the presence server but details of this is also outside the scope of this flow..

4. The Network Agent sends *NotifyPresUp* message to the Presence Server via the Pen interface.

5. Prior to notifying all authorised watchers, it acknowledges the receipt of the *NotifyPresUp* message with a *MsgAck* to the Network Agent.

Network Agent sends an MM_Event_Ack to the SGSN

8.1.4 Presence Server notifying watcher of updates to presence information

8.1.4.1 IMS based Watcher and presentity in the same or different IM-CN subsystem

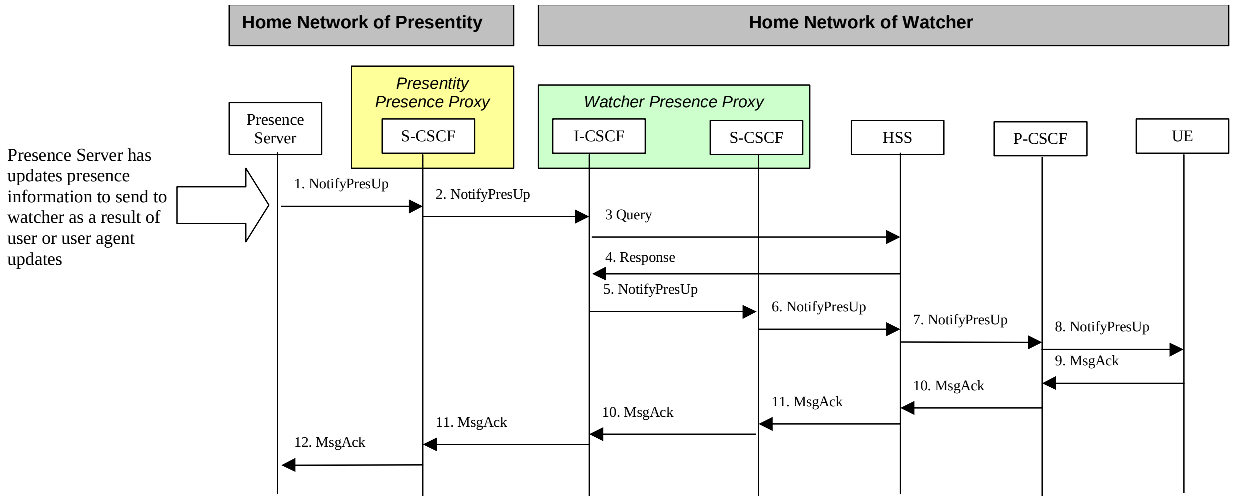


Figure ~~10~~16. Presence Server updating IMS watcher

Figure ~~10~~ 16 shows how an IMS based watcher is notified of updates to a presentity's presence information. The flows are applicable to the case where the Watcher and Presentity are in the same or in different IM-CN subsystems. Details of the flows are as follows:

1. The Presence Server determines which authorised watchers are entitled to receive the updates of the presence information for this presentity. For each appropriate watcher, the presence server sends a *NotifyPresUp* message that contains the updates to the presence information. For the case of an external watcher, this *NotifyPresUp* is sent to the S-CSCF, acting as a Watcher Presence Proxy.

2. ~~.~~The S-CSCF shall examine the home domain of the watcher that needs to get the presence updates and if the request is for a watcher outside the operator's domain, it determines the external I-CSCF. If the request is for a watcher in the same domain, the S-CSCF forwards the request to the local I-CSCF.

3. The I-CSCF shall examine the watcher's identity and the home domain identity and employ the services of a name-address resolution mechanism to determine the HSS address to contact. The I-CSCF shall send a *Query* message to the HSS to obtain the address of the S-CSCF for the watcher.

4. The *Resp* provides the name of the S-CSCF for the watcher.

5. The I-CSCF, using the name of the S-CSCF shall determine the address of the S-CSCF through a name-address resolution mechanism. The *NotifyPresUp* message is forwarded to the S-CSCF of the watcher.

6. The S-CSCF forwards the *NotifyPresUp* message to the P-CSCF.

7. The P-CSCF forwards the *NotifyPresUp* message to the UE.

8. The UE acknowledges the *NotifyPresUp* message with a *MsgAck* to the P-CSCF.

9. The P-CSCF forwards the *MsgAck* message to the S-CSCF.

10. The S-CSCF forwards the *MsgAck* message to the I-CSCF.

11. The I-CSCF forwards the message to the S-CSCF in the home network of the presentity.

12. The S-CSCF forwards the *MsgAck* message to the Presence Server.

8.1.5 Presence User Agent subscribing to watcher list and receiving notification of a new watcher subscription

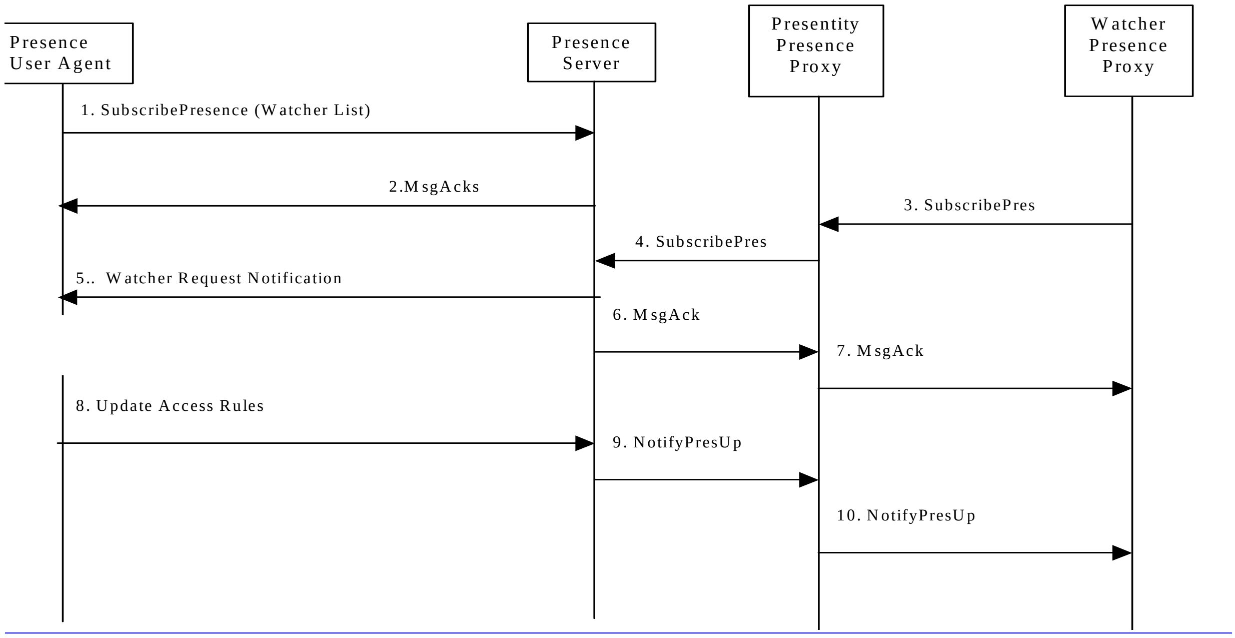


Figure 17. Presence User Agent subscribing to watcher list and receiving notification of a new watcher subscription

Figure 17 shows a Presence User Agent subscribing to watcher list and receiving notification of a new watcher subscription that is not contained in the current access rules. The details of the flows are as follows:

1) The Presence User Agent initiates a subscription to the Presence Server requesting notification of any new watcher subscriptions.

2) The presence server issues a *MsgAck* to the Presence User Agent.

3) A watcher wishes to watch the Presentity. To initiate a subscription, the watcher sends a *SubscribePres* message request containing the presence related events that it wishes to be notified of, together with an indication of the length of time this periodic subscription should last to the Watcher Presence Proxy. The Watcher Presence Proxy sends the *SubscribePres* information flow to the Presentity Presence Proxy.

4) The *SubscribePres* is forwarded by the Presentity Presence Proxy to the Presence Server.

5) The Presence Server checks the access rules and determines that this is a new watcher subscription not contained in the current access rules and so sends a notification to inform the Presence User Agent of the request from the new watcher.

6) The presence server issues a *MsgAck* to inform the watcher that the Presence Server has received the watcher's request for Presence information. The *MsgAck* is sent to the Presentity Presence Proxy.

7) The *MsgAck* is forwarded by the Presentity Presence Proxy to the watcher via the Watcher Presence Proxy.

Steps 8 – 10 depend on the actions of the Principal. The Principal can ignore the notification sent in step 5 or can respond with an Update of the Access Rules to Accept, Accept with conditions or Deny the request.

8) The Presence User Agent sends an *UpdateAccessRules* to the Presence Server. (If the Presence User Agent decides to accept, block or accept with conditions the Presence Information requested by the watcher an appropriate *SubscriptionAccepted, SubscriptionBlocked* or *SubscriptionAcceptedWithConditions* is sent within the *UpdateAccessRules* to the Presence Server).

9) If the UpdateAccessRules accepts the subscription then the Presence Server sends a *NotifyPresUp* message with the current state of the Presence User Agent to the Presentity Presence Proxy. If the *UpdateAccessRules* indicates that the subscription is blocked then steps 9 and 10 are not performed.

10) The Presentity Presence Proxy forwards the *NotifyPresUp* message to the watcher via the Watcher Presence Proxy.

Annex A

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**
2002-03	15				Presented for information at SA#15, same technical content as v.0.5.0	0.5.0	1.0.0
2002-04					Changes done in the SA2#24 Presence Sessions	1.0.0	1.1.0