

Meeting #20, Hämeenlinna, Finland  
09-12 June 2003

---

**Source:** TSG SA WG2  
**Title:** CRs on 23.141  
**Agenda Item:** 7.2.3

The following Change Requests (CRs) have been approved by TSG SA WG2 and are requested to be approved by TSG SA plenary #20.

Note: the source of all these CRs is now S2, even if the name of the originating company(ies) is still reflected on the cover page of all the attached CRs.

<b>Tdoc #</b>	<b>Title</b>	<b>Spec</b>	<b>CR #</b>	<b>cat</b>	<b>Version in</b>	<b>REL</b>	<b>WI</b>	<b>S2 meeting</b>
<a href="#">S2-031498</a>	Editorial cleanup of 23.141	23.141	51r1	D	6.2.0	6	PRESNC	S2-31
<a href="#">S2-031500</a>	3GPP-WLAN IW supplier for PRESENCE information	23.141	50r2	B	6.2.0	6	PRESNC	S2-31

CR-Form-v7

## CHANGE REQUEST

⌘ **23.141 CR 51** ⌘ rev **1** ⌘ Current version: **6.2.0** ⌘

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

**Proposed change affects:** UICC apps  ME  Radio Access Network  Core Network

<b>Title:</b>	⌘ Editorial cleanup of 23.141		
<b>Source:</b>	⌘ Ericsson		
<b>Work item code:</b>	⌘ PRESNC	<b>Date:</b>	⌘ 08/04/2003
<b>Category:</b>	⌘ <b>D</b>	<b>Release:</b>	⌘ Rel-6
	Use <u>one</u> of the following categories: <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900.		Use <u>one</u> of the following releases: 2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6)

<b>Reason for change:</b>	⌘ Editorial corrections		
<b>Summary of change:</b>	⌘ A number of editorial changes including removal of duplicated text, aligning text regarding Presence attributes and aligning figures with related text.		
<b>Consequences if not approved:</b>	⌘		

<b>Clauses affected:</b>	⌘ 5.1, 6.1.1, 6.1.2, 7, A.2.2.1, A.2.3.3, A.2.4.1						
<b>Other specs affected:</b>	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Other core specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘	
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Test specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘	
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> O&M Specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘	
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
<b>Other comments:</b>	⌘						

### How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

\*\*\*\*\* First CHANGE \*\*\*\*\*

## 5.1 Presence Server

The Presence Server shall reside in the presentity's home network.

The Presence Server shall be able to receive and manage presence information that is published by the Presence User/Network/External agents, and shall be responsible for composing the presence-related information for a certain presentity from the information it receives from multiple sources into a single presence document. The composing process to create the single presence document may involve complex transformations of presence information such as modifying the presence information from one presence source based on information from another presence source. In particular, the Presence server shall be able to receive and manage presence information that is published from multiple Presence User agents of the same presentity. These Presence User agents may be updating the same parts of the presence information. ~~In particular, the Presence server shall be able to receive and manage presence information that is published from multiple Presence User agents of the same presentity. These Presence User agents may be updating the same parts of the presence information.~~

The mechanisms for combining the presence related information shall be defined based on presence attributes, and according to certain policy defined in the Presence Server. The Presence Server shall be capable of receiving and composing the Presence information received in the standardized formats from authorized sources regardless of the source of the information or the ability to interpret the information contained in the presence tuples. The information that the Presence Server is not able to interpret shall be handled in a transparent manner.

The Presence Server shall also allow watchers to request and subscribe to either the full set of presence information of a presentity, or only certain information within. Watcher defines the subset of the presence information, that he is interested in, by the filter that is carried in presence information subscription. The Presence Server shall be able to generate partial notifications to a watcher, which has indicated the capability to process them. These partial notifications contain the presence information those tuples of the presentity that which have been modified since the latest notification sent to the watcher about this presentity, and required additional information to be able to link the partial notification to the information watcher has received earlier. In case the watcher does not indicate the capability to process partial notifications the presence server shall send only full updates.

Before the subscription to presence information is accepted, the Presence Server should attempt to verify the identity of the watcher that subscribes to Presentity's Presence information, except if the watcher has indicated his desire to remain anonymous. The action taken by the Presence Server if the verification fails may include notifying the Presentity.

The Presence Server shall support SIP-based communications for publishing presence information.

The Presence Server shall support SIP-based communications with the Presentity Presence Proxy. The Presence Server is a SIP Application Server as defined by 3GPP TS 23.228 [9], and is located using SIP URLs, standard SIP and existing IMS mechanisms (SIP routing, HSS query, ISC filtering, etc...).

The Presence Server shall provide Subscription Authorization Policy. The Subscription Authorization Policy determines which Watchers are allowed to subscribe to a Presentity's Presence information.

The Subscription Authorization Policy also determines which tuples of the Presentity's Presence information the watcher has access. It shall be possible for the Presentity's Presence User Agent to provide the Subscription Authorization Policy or it may be configured by the operator as part of the service provisioning.

The Presence Server may provide a watcher configurable filtering function that is used to limit the information that is delivered to a watcher. After subscription the authorized watchers get notified of the actual Presence Information based on the Subscription Authorization Policy and the filters set by the watcher in the subscription. If the Presence Server does not support the filters as requested by the watcher, this is indicated to the watcher. In this case the notification shall contain the actual Presence information based on the Subscription Authorization Policy and local policy in the Presence Server. The Presence Server may support one or more of the following types of filters: Filters, which allow watchers to define

- the tuples that the watcher is interested in;  
 Watcher can define a criteria which allows the complete tuple and all the information within the tuple to be

transmitted. E.g. watcher can define the filter to permit notifying all the tuples (and all the information within those tuples) which has "tel:user@domain" as the contact address or "IM" as a communication means.

- the attributes that the watcher is interested in; and  
Watcher can define a criteria which result notifies to contain values only for defined attributes (attributes are defined by the filter and values for other attributes are not available in the notifications)
- the triggers when a notification should be sent.  
Watcher can define a criteria which specifies when to send a notification. E.g. every time the communication means status attribute changes its value, a notification is sent to the watcher. Another example: filter out and do not send the notifications resulting from the publication of the Presence User agent that is equal to the watcher.

The Presence Server shall collect watcher information to enable presentity to obtain information of the watchers that are or have been requesting, fetching or subscribing presentity's presence information. Service provider shall be able to define the maximum time period over which information is collected and stored. The watcher information list shall include:

- identity of the watcher (unless anonymity was requested);  
In case of anonymous watcher, the identity of the watcher shall not be provided to the presentity. The presentity shall be able to determine that an anonymous watcher has requested, fetched or subscribed presence information of the presentity including related information as specified in this list without revealing the watchers identity.
- time of the request, fetch or subscription;
- length of the subscription; and
- state of the request or subscription.

The Presence Server shall be able to support the presentity obtaining the above watcher information. The Presence Server shall be able to receive watcher information fetches and subscriptions from the presentity. These watcher information fetch and subscribe requests shall be able to contain filters which define

- what watchers the presentity is interested in;  
Possible categories are:
  - all watchers;
  - defined watchers;
  - new, unauthorised watchers; and
  - defined and new, unauthorised watchers.
- what information the presentity is interested in; and  
The information is all or part of the watcher information list as defined above.
- the length of the watcher information history collection period that the presentity is interested in.

In response to watcher information fetches, the presence server shall be able to provide requested watcher information to the presentity. In response to watcher information subscriptions, the presence server shall provide notification to the presentity of the current state of the subscribed watcher information. When there are subsequent changes in the subscribed watcher information, notifications of the changes in watcher information are sent to the presentity.

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

~~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.~~

## 5.2 Presence Agent Elements

\*\*\*\*\* NEXT CHANGE \*\*\*\*\*

### 6.1.1 3GPP Subscriber Presence Attributes and Values

A 3GPP subscriber is described by attributes: *subscriber's status*, ~~*communication means*~~ ~~*network-status*~~, *one or more communication address(es)* (containing *communication means* and *contact address*), *location* (*subscriber provided location* ~~*and/or*~~ *network provided location*), *priority*, *text*. The attributes can be categorised as communication means and contact address specific information or generic information. Generic information attributes shall be: subscriber's status, ~~subscriber provided location~~ and text. Communication means and contact address specific information attributes shall be: ~~*communication means*~~ ~~*network-status*~~, *communication means*, *contact address*, ~~*network provided location*~~, *priority* and *text*.

- Generic information attributes, if these attributes are used as part of any tuple they shall use following values (values in parenthesis) to enable interoperability:
  - Subscriber's status (willing, willing with limitations, not willing, not disclosed),
    - NOTE: Attribute name subscriber's status has been defined in stage 1 and it does not imply any mapping to the IETF defined presence model e.g. IETF RFC 2778 [16], IETF RFC 2779 [17].
  - The subscriber's status attribute is not intended to be used when interworking with IM clients. Subscribers are able to provide more detailed willingness information as well as other information through the generic Text attribute, and the communication means and contact address specific Text attribute.
  - Location (Last known CGI/SAI and/or geographic co-ordinates and/or free format text and timestamp),
  - Text (free format text).
- Communication means and contact address specific information attributes, if these attributes are used as part of any tuple they shall use following values (values in parenthesis) to enable interoperability:
  - communication means status (online, offline),
  - communication means (Service type (e.g. telephony, SMS, email, multimedia messaging service, instant messaging service)),
  - contact address (E.164 (e.g. MSISDN), SIP URL, Email, Instant message address e.g. IM:name@domain name),
  - Priority (Priority order for each of the defined communication means and contact address),
  - Text (free format text).

NOTE: The mapping of these attributes and values to the IETF defined presence model IETF RFC 2778[16], IETF RFC 2779 [17] may result one or several of the following:

- using existing IETF defined attributes and values (or subset of them)
- using existing IETF defined attributes but extending the value set
- Creating new attributes to the tuples.

The mapping of these values for tuples and different fields of the tuple is defined in stage 3. Furthermore, mechanisms to allow extensibility of the presence information in order to ensure interoperability are defined in stage 3.

All these attributes shall be able to contain value NULL to enable polite blocking.

### 6.1.2 Presence Structure to Support Multiple Values for Attributes

Attributes shall be 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. The association of tuples to different watchers and watcher groups shall be based on the subscription authorisation policies s. The presentity controls the value of the attribute by modifying the corresponding tuple. Figure 6.1.2-1 illustrates how different values for different watchers are provided utilising subscription authorisation policies s.

NOTE: The figure 6.1.2-1 is illustrative only and it shall not mandate or limit the server implementation options.

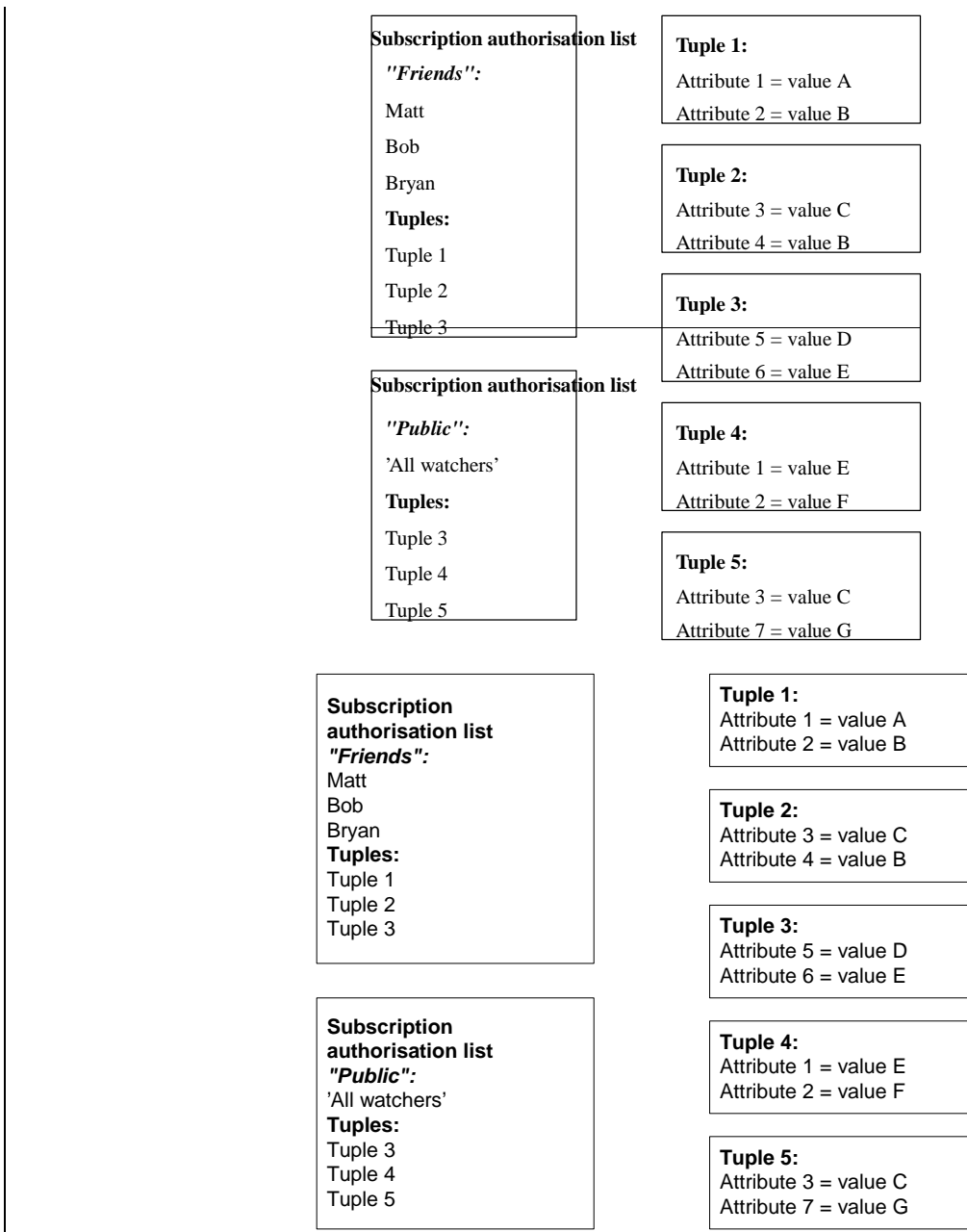


Figure 6.1.2-1: Illustration how subscription authorisation lists are utilised to present different values of the same attribute to different watchers

## 6.2 Presence Information Model

Presence information related to a particular communications means and contact address shall be carried in a presence tuple dedicated to that particular communications means and contact address.

Generic presence information that is not directly applicable to a particular communications means and contact address shall be conveyed in a way that conforms to the IETF presence model e.g. IETF RFC 2778 [16], IETF RFC 2779 [17] (to ensure interoperability) and preferably does not require multiple instances of this information to be sent.

Generic information may be mapped to the tuples specific to each communication means and contact address. In that case the information shall be equal in each tuple. The stage 3 description should use a mechanism which conforms to the IETF presence model.

Application identifiers may be allocated to applications, which are using presence capabilities. The conventions and the allocation mechanism for application identifiers are subject to stage 3 specification. Application identifier(s) are carried as part of the presence information. Application identifier(s) may be added to published presence information on the presentity side. In this case, the presence server shall include this application identifier to the relevant tuple(s) in the presence document together with the published information. On the watcher side the received application identifier may be used e.g. for determining which application should receive and process the related presence information. Details of processing the application identifier(s) on the Presence User Agent and watcher side are out of scope of this specification.

---

## 7 Subscription authorisation policies

Subscription authorisation policies shall define the watchers who can access the presence information of the presentity. In addition to the watcher identities, the subscription authorisation policies shall contain the presence information or reference to the presence information that is allowed to be accessed by the listed watchers. The subscription authorisation lists can be logically arranged to be part of the presence server or a separate entity in the network.

In case of presence information fetch or subscription from a watcher that has not been authorised by the subscription authorisation policies, the presence server shall put the fetch or subscription on hold until the watcher has been authorised, added to the subscription authorisation lists or until a preconfigured timer has expired.

Subscription authorisation lists can be divided into three different categories: personal subscription authorisation lists, public subscription authorisation lists and blocking subscription authorisation lists.

Personal and general subscription authorisation lists shall define which watchers can access which information. Personal subscription authorisation lists shall explicitly identify watchers, while general subscription authorisation 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 subscription authorisation lists shall 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 subscription authorisation lists as well as blocking subscription authorisation lists.

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

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

In this particular example, once the hit is found the evaluation is halted and presence information according to access is delivered.

1. Is the watcher on the blocking subscription authorisation list?
2. Is the watcher on the personal subscription authorisation list?
3. Is the watcher on the general subscription authorisation list (created e.g. by service provider containing all watchers)?
4. Send a notification to the presentity of pending subscription authorisation request.



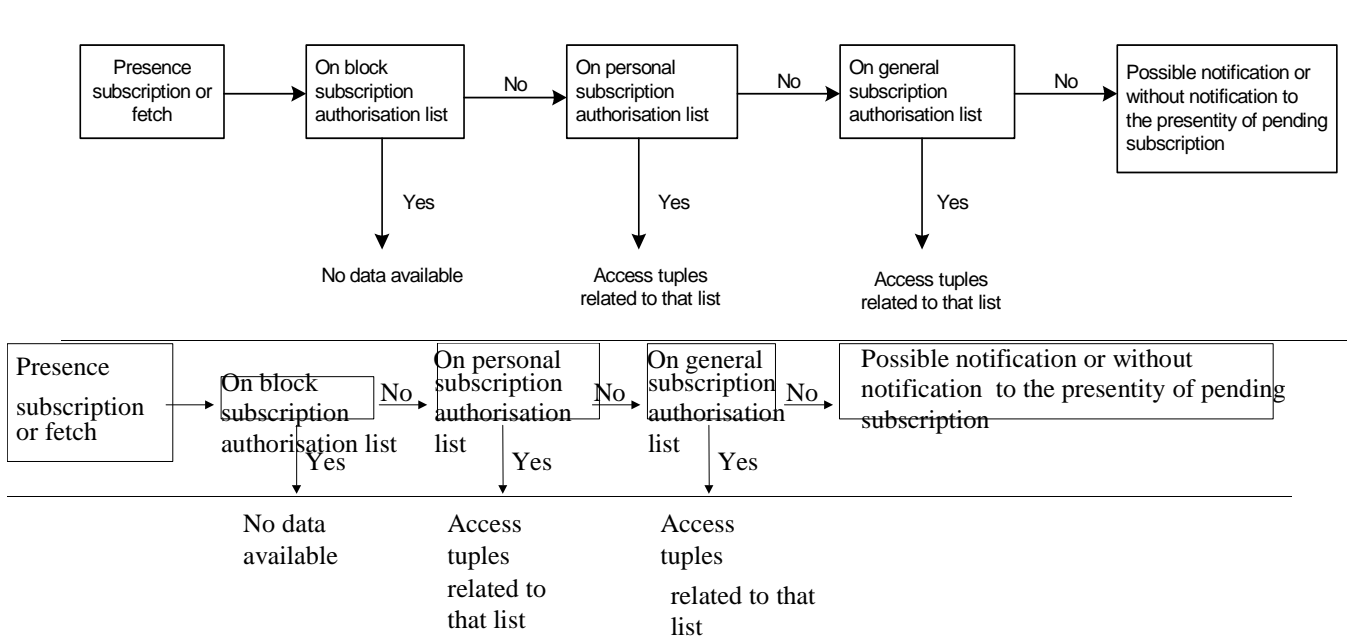


Figure 7-1. Example of subscription authorisation list evaluation order for presence service

## 8 Charging requirement

\*\*\*\*\* NEXT CHANGE \*\*\*\*\*

### A.2.2 Flows demonstrating how watchers subscribe to presence event notification

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

A.2.2.1 IMS Watcher and IMS Presentity in the same or different IM-CN

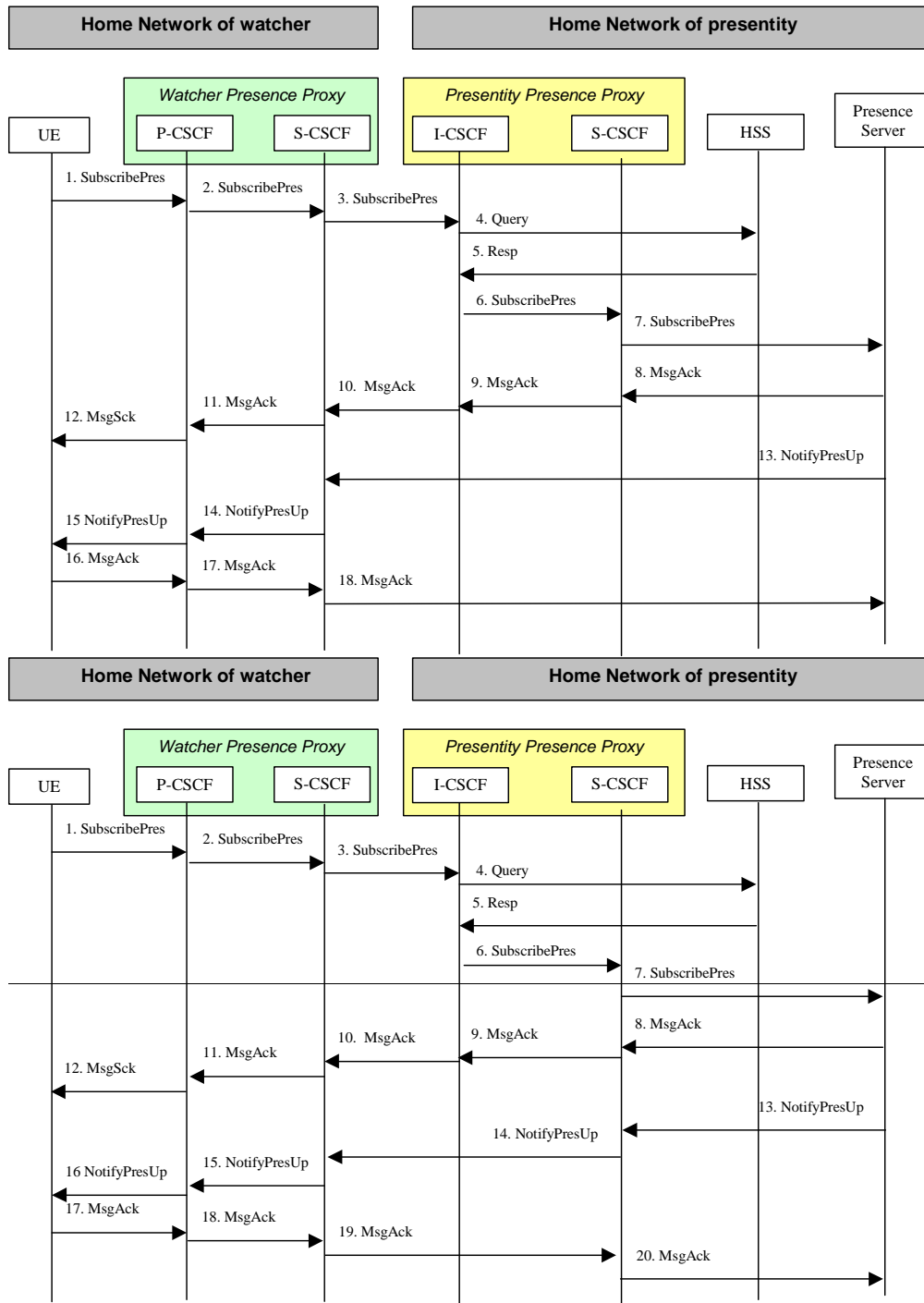


Figure A.2.2.1-1. IMS Watcher registering for event notification

Figure A.2.2.1-1 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.

Note-i: The path of the SUBSCRIBE dialog may optionally include additional I-CSCF(THIGs) in networks where network topology hiding is applied.

Note-ii: The flow shows the case that the S-CSCF of the Presentity does not remain in the path of the dialog.

The details of the flows as follows:

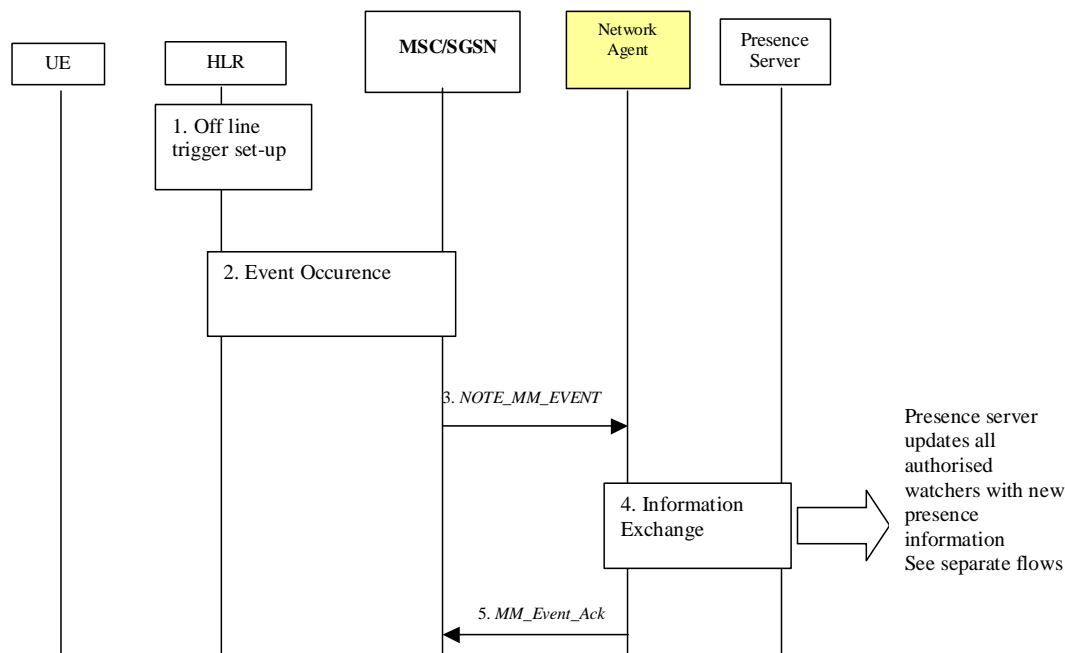
1. A watcher agent in a UE wishes to watch a presentity's presence information, or certain parts of the presentity's presence information (defined by the filters included in *SubscribePres*). To initiate a subscription, the UE sends a *SubscribePres* message request containing the presence related events 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). The *SubscribePres* may also include an indication of the watcher's capability to handle partial notifications.
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 presentity 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 a *NotifyPresUp* message with the current full state of the presentity's tuples that the watcher has subscribed and been authorised to. The *NotifyPresUp* is sent along the path of the SUBSCRIBE dialog to the S-CSCF allocated to the Watcher. Further notifications sent by the Presence server may either contain the complete set of presence information, or only those tuples that have changed since the last notification if the watcher has indicated the capability to process partial notifications.
14. The S-CSCF forwards the *NotifyPresUp* to the P-CSCF.
15. The P-CSCF forwards the *NotifyPresUp* to the watcher application in the UE
16. The UE acknowledges the receipt of the *NotifyPresUp* message with a *MsgAck* sending this to the P-CSCF.
17. The P-CSCF forwards the *MsgAck* message to the S-CSCF.
18. The S-CSCF allocated to the presentity forwards the *MsgAck* to the Presence Server.

### A.2.3 Flows demonstrating how presentities update Presence Information

\*\*\*\*\* NEXT CHANGE \*\*\*\*\*

### A.2.3.3 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 A.2.3.3-1: 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 TSR 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 informs the Presence Server. The Presence Server notifies all authorised watchers and sends an acknowledgement to the Network Agent.
5. Network Agent sends an MM\_Event\_Ack to the MSC/SGSN.

\*\*\*\*\* NEXT CHANGE \*\*\*\*\*

### A.2.4 Presence Server notifying watcher of updates to presence information

#### A.2.4.1 IMS based Watcher and presentity in the same or different IM-CN subsystem

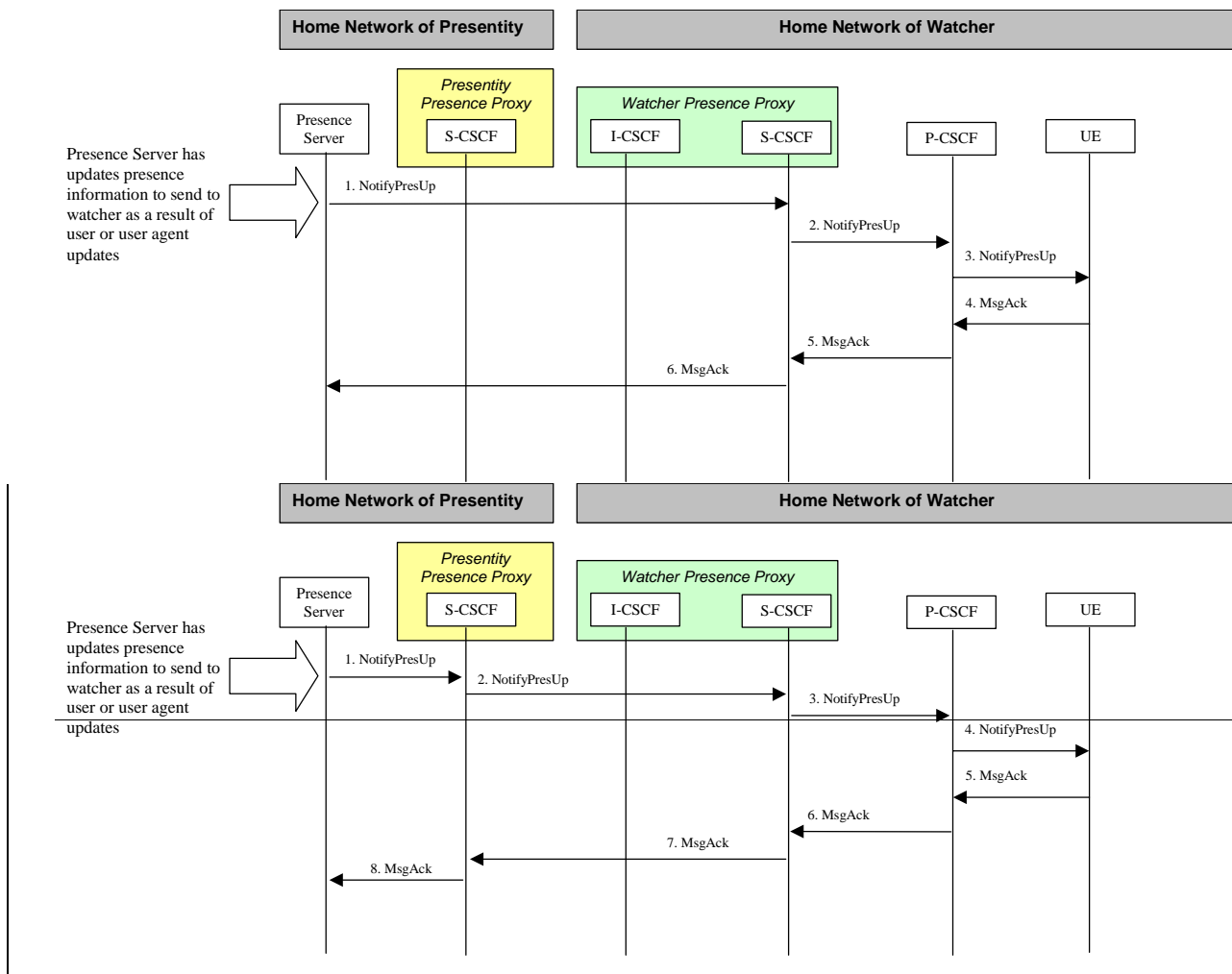


Figure A.2.4.1-1: Presence Server updating IMS watcher

Figure A.2.4.1-1 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.

Note-i: The path of the SUBSCRIBE dialog (i.e. also the NOTIFY transaction) may optionally include additional I-CSCF(THIGs) in networks where network topology hiding is applied.

Note-ii: The flow shows the case that the S-CSCF of the Presentity does not remain in the path of the dialog.

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 full or partial updates to the presence information. This *NotifyPresUp* is sent along the path of the SUBSCRIBE dialog to the S-CSCF of the Watcher.
2. The S-CSCF forwards the *NotifyPresUp* message to the P-CSCF of the watcher.
3. The P-CSCF forwards the *NotifyPresUp* message to the UE.
4. The UE acknowledges the *NotifyPresUp* message with a *MsgAck* to the P-CSCF.
5. The P-CSCF forwards the *MsgAck* message to the S-CSCF.
6. The S-CSCF of the Watcher forwards the *MsgAck* to the Presence Server.

3GPP TSG-SA WG2 Meeting #30  
Seoul, Korea, 7<sup>th</sup> – 11<sup>th</sup> April, 2003

Tdoc # **S2-031348031500**

CR-Form-v7

## CHANGE REQUEST

⌘ **23.141 CR 50** ⌘ rev **1** ⌘ Current version: **6.2.0** ⌘  
**2**

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

**Proposed change affects:** UICC apps ⌘  ME  Radio Access Network  Core Network

<b>Title:</b>	⌘ 3GPP-WLAN IW supplier for PRESENCE information		
<b>Source:</b>	⌘ Huawei, China Mobile, AWS, Lucent, Orange		
<b>Work item code:</b>	⌘ PRESNC	<b>Date:</b>	⌘ 14/03/2003
<b>Category:</b>	⌘ <b>B</b>	<b>Release:</b>	⌘ Rel-6
Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:	
F (correction)		2 (GSM Phase 2)	
A (corresponds to a correction in an earlier release)		R96 (Release 1996)	
B (addition of feature),		R97 (Release 1997)	
C (functional modification of feature)		R98 (Release 1998)	
D (editorial modification)		R99 (Release 1999)	
Detailed explanations of the above categories can be found in 3GPP TR 21.900.		Rel-4 (Release 4)	
		Rel-5 (Release 5)	
		Rel-6 (Release 6)	

<b>Reason for change:</b>	⌘ As an important component of 3GPP network, 3GPP WLAN network should be considered a Presence information supplier. For example, when a user connects to the 3GPP WLAN network, the related Presence information should be supplied to Presence server such as its connection/disconnection, communication means, address, and so on.
<b>Summary of change:</b>	⌘ A new_reference point should be added between the 3GPP AAA Server and the Presence Network Agent
<b>Consequences if not approved:</b>	⌘ The integrity and quality of the Presence Service may be deficient/degraded without Presence information from 3GPP-WLAN IW network.

<b>Clauses affected:</b>	⌘ Annex										
<b>Other specs affected:</b>	<table border="1"> <tr> <td>Y</td> <td>N</td> </tr> <tr> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> </table>	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications	⌘
Y	N										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
		Test specifications									
		O&M Specifications									
<b>Other comments:</b>	⌘										

### How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

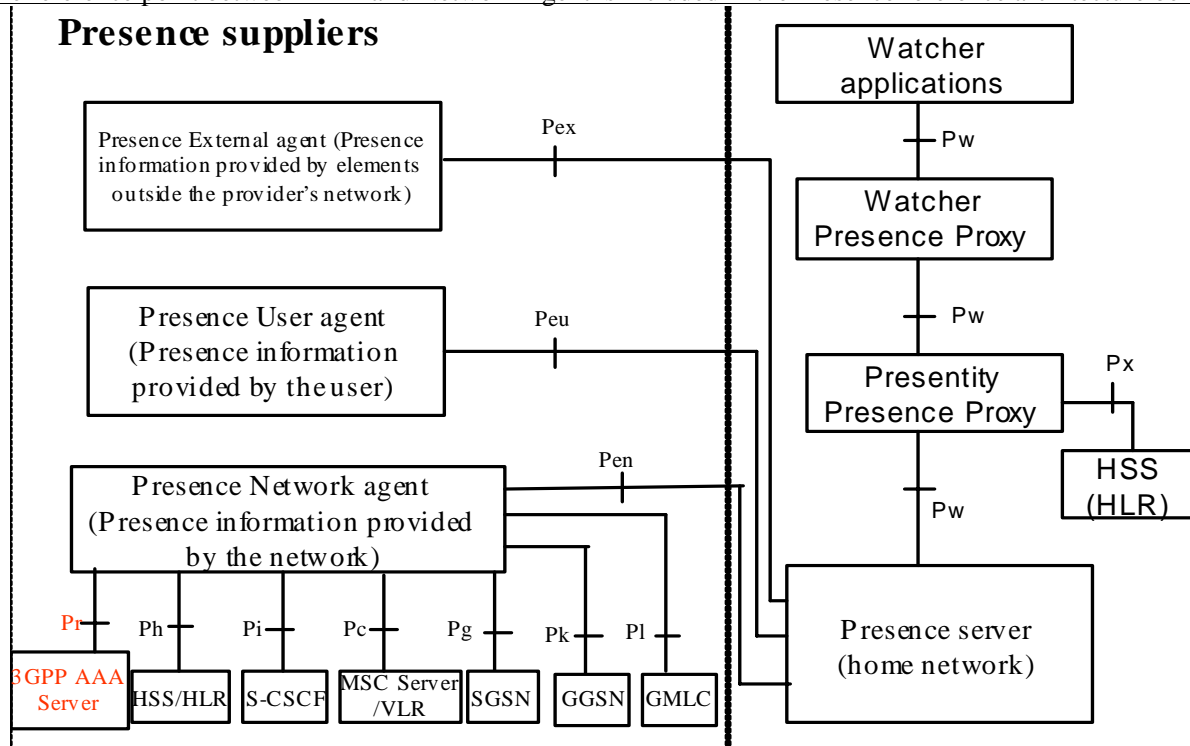
Start of modified section

## Annex B (Informative) 3GPP-WLAN IW architecture as a supplier for Presence information

This Annex describes initial concepts for retrieving Presence information from the 3GPP-WLAN interworking architecture. These concepts are expected to be further developed, and parts from this Annex are expected to be moved to the normative part of this Technical Specification.

### B.1 Reference architecture Model with 3GPP-WLAN supplier

The reference point between AAA and Network Agent is included in the Presence reference architecture below.



Interfaces Ph, Pi, Pc, Pg, Pk and Pl are based on existing R5 procedures e.g. CAMEL, MAP, CAP, RADIUS, ISC, Cx, Sh. The Pr interface is based on existing R6 procedures of the 3GPP-WLAN interworking architecture.

Figure B.1-1: Reference architecture to support a presence service

## B.2 Reference point Presence Network Agent – 3GPP AAA Server (Pr)

This reference point shall allow the 3GPP AAA Server to report IP-connectivity related events to the Presence Network Agent (such as connection/disconnection to the WLAN interworking service). The Pr reference point shall be based on mechanisms of existing interfaces of the 3GPP-WLAN interworking architecture defined in 3GPP TS 23.234.

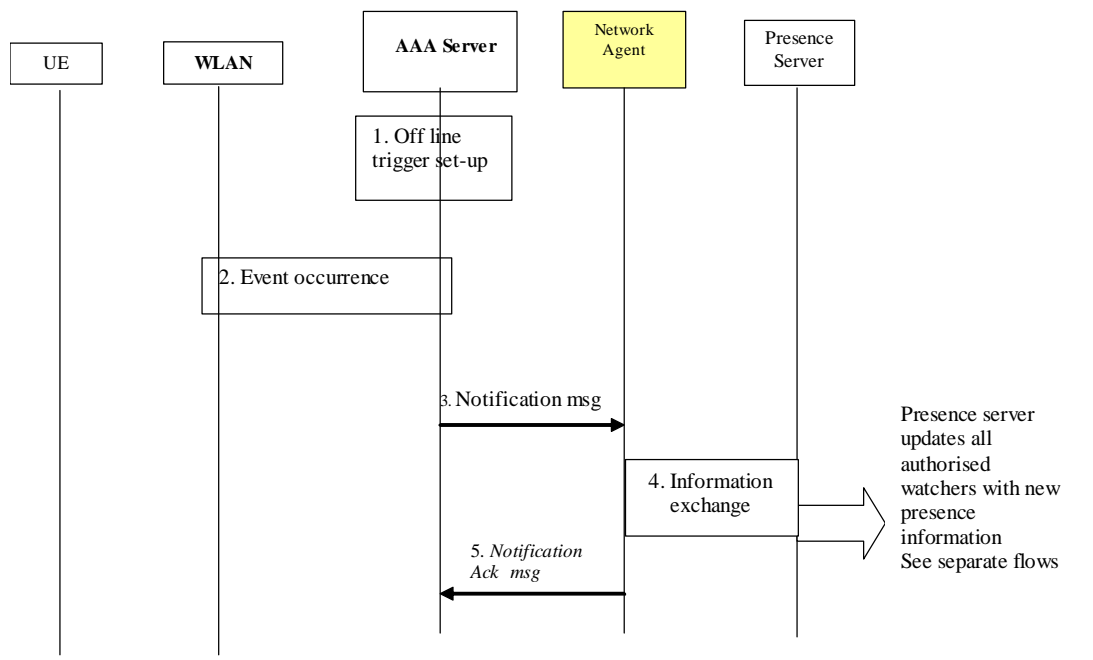
## B.3 Suppliers of Presence Information in 3GPP-WLAN IW

The Presence Network Agent may receive Presence information from one or more of the following network elements over the specified reference point:

Network Element supplying Presence Information	Reference Point
3GPP AAA Server	Pr

## B.4 3GPP-WLAN Notification process of the Presence Server

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



**Figure B.4-1: WLAN Notification procedure for the Presence Server.**

1. For network event to be reported on behalf of a WLAN subscriber, the necessary triggers are armed in the AAA SERVER. 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 WLAN and the AAA SERVER, (e.g UE connection or disconnection) a notification message is generated.
3. A notification message is sent to the Network Agent via Pr 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 are also outside the scope of this flow.
4. The Network Agent notify the Presence Server by exchanging messages via the Pen interface.
5. Network Agent sends an acknowledge message to the AAA Server.



---

Annex ~~B~~-C (informative):  
Change history

.....

End of modified section