ETSI TS 122 141 V19.0.0 (2025-10)

TECHNICAL SPECIFICATION

Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
LTE;
Presence service;
Stage 1
(3GPP TS 22.141 version 19.0.0 Release 19)

Reference
RTS/TSGS-0122141vj00

Keywords
GSM, LTE, UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found at 3GPP to ETSI numbering cross-referencing.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

This specification defines the requirements for the support of the presence service. The presence service results in presence information of a user and information on a user's devices, services and services components being managed by the network. Together, user, these devices, services and services components are termed presentity (presence entity). This TS makes extensive use of internet terminology to ensure alignment with the presence service description and behaviour in internet recommendations.

The presence service provides access to presence information to be made available to other users or services. Exploitation of this service, see figure 1, will enable the creation of enhanced rich multimedia services along the lines of those currently present in the internet world.

Presence is an attribute related to, but quite different from mobility information, and is a service that can be exploited to create additional services. The types of services that could be supported by the presence service may include:

- New communications services

  The presence service will enable new multimedia services to exploit this key enabler to support other advanced multimedia services and communications. These new services may infer the context, availability and willingness of a user to accept or participate in particular types of communications by accessing the presence information for the user's devices and services. Examples of such new multimedia services that could potentially exploit the presence service include "chat", instant messaging, multimedia messaging, e-mail, , handling of individual media in a multimedia session etc.

- Information services

  The presence service may also be exploited to enable the creation of services in which abstract entities are providing the services to the mobile community. The presence service may be used to support such abstract services as cinema ticket information, the score at a football match, motorway traffic status, advanced push services etc.

- Enhanced existing services

  Existing services may also be significantly enhanced by exploiting the presence information. For example a user may dynamically arrange for his wireless services to be supported through his corporate PABX whilst he is on-site, require media to be converted and directed to specific devices (e.g. user cannot accept a voice call whilst in a meeting, but is prepared to receive the voice call converted to text in the form of an SMS/MMS/e-mail message). The presence service may also be used to enable the creation of advanced versions of CS/PS services, enable terminal capabilities support etc.

The following figure 1 represents a logical overview of how services could exploit the presence service to create advanced services.

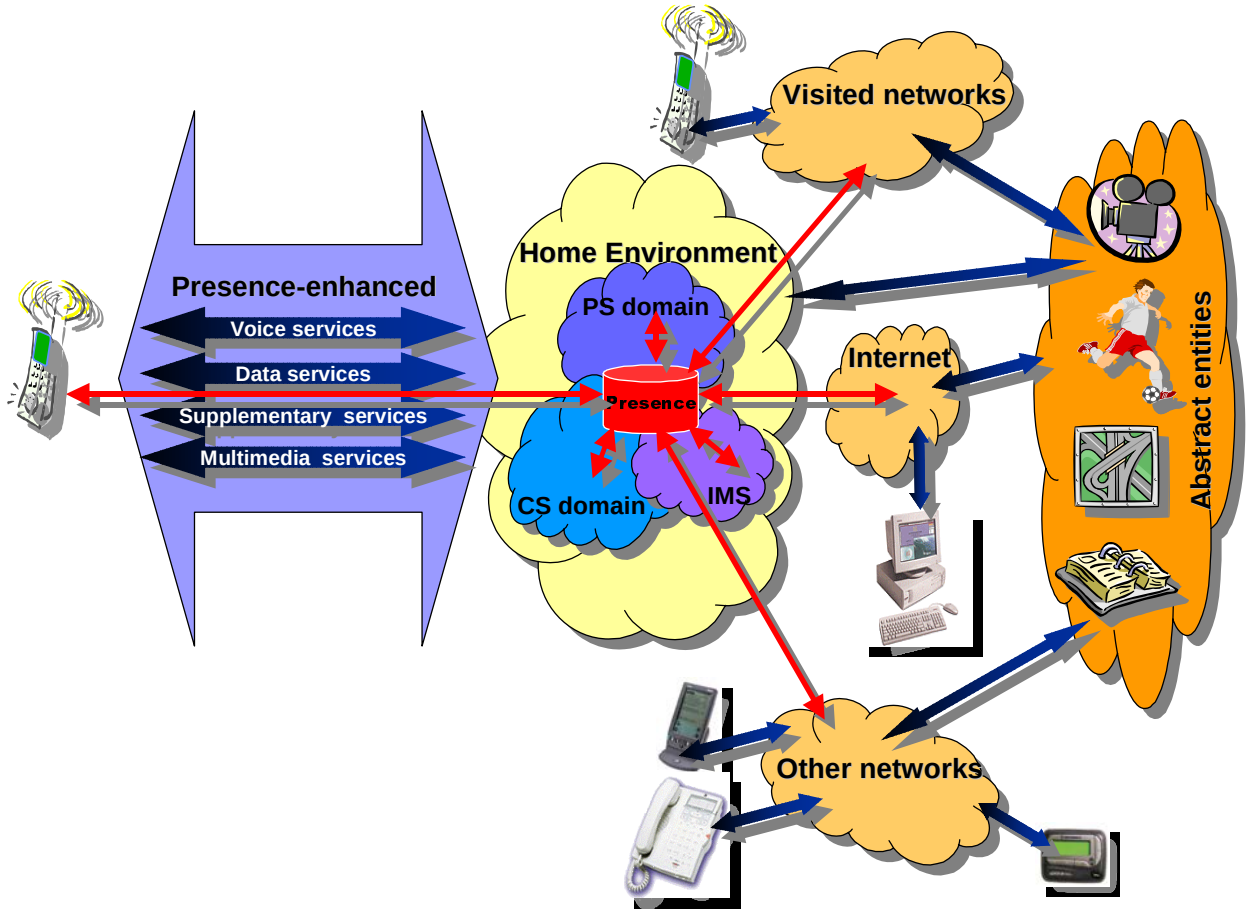

Figure 1: Logical presence service support of services

A presence-enabled service as observed by the user is a service in which the user can control the dissemination of his presence information to other users and services, and also be able to explicitly identify specifically which other users and services to which he provides presence status. Combined with the capability of other users' control of their own presence status, virtually infinite combinations of users and services interacting at different levels can be created.

The exploitation of the presence service is already available in the internet world, although unfortunately with different non interoperable mechanisms. This specification identifies the requirements for support of an enhanced version of the presence service through the support of attributes (e.g. services, media components of a multimedia service, location information) in an interoperable manner within both wireless and fixed networks, and with external networks.

1 Scope

This TS defines the stage one description for the presence service. Stage one is the set of requirements which shall be supported to enable the exploitation of the presence service, seen primarily from the users' and home environments' points of view.

This TS includes information applicable to the home environment, device and network manufacturers which are sufficient to provide complete support of the presence service.

Additional functionalities not documented in this TS are considered outside the scope of this TS. Such additional functionality may be on a network-wide basis, nation-wide basis or particular to a group of users. Such additional functionality shall not compromise conformance to the requirements of the presence service defined in this specification.

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: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

[2] Void

[3] RFC 2778: "A Model for Presence and Instant Messaging"; http://www.ietf.org/rfc.html.

[4] RFC 2779 "Instant Messaging / Presence Protocol Requirement"; http://www.ietf.org/rfc.html.

[5] RFC 3863 " Presence Information Data Format (PIDF)"; C:\DOCUME~1\Michele\LOCALS~1\Documents and Settings\Michele\Local Settings\Temp\ZipTemp\ http:\www.ietf.org\internet-drafts\draft-ietf-impp-cpim-05.txtC:\DOCUME~1\Michele\LOCALS~1\Documents and Settings\Michele\Local Settings\Temp\ZipTemp\ http:\www.ietf.org\internet-drafts\draft-ietf-impp-cpim-05.txtC:\DOCUME~1\Michele\LOCALS~1\Documents and Settings\Michele\Local Settings\Temp\ZipTemp\ http:\www.ietf.org\internet-drafts\draft-ietf-impp-cpim-05.txt http://www.ietf.org/rfc.html.

2.1 Acknowledgement

This document contains extracts of documents, the copyright of which is vested in the Internet Society. The terms of the Internet Society copyright are fulfilled by the reproduction of the copyright and paragraph below. This copyright only applies to text in this document that has been directly reproduced from the appropriate RFC.

copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

3 Definitions, symbols and abbreviations

3.1 Definitions

Access rules: constraints on how the presence service makes presence information available to watchers. For each presentity's presence information, the applicable access rules are managed by the principal that controls the presentity.

availability: a property of a presentity denoting its ability and willingness to communicate based on factors such as the identity or properties of the watcher and the preferences and/or policies that are associated with the presentity

fetcher: a form of watcher that has asked the presence service for the presence information of one or more presentities, but is not requesting a notification from the presence service of (future) changes in a presentity's presence information.

identifier: a means of indicating a point of contact, intended for public use such as on a business card. Telephone numbers, email addresses, and typical home page URLs are all examples of identifier in other systems.

poller: a fetcher that requests presence information on a regular basis.

presence information: is a set of attributes characterising current properties of presentities such as status, an optional communication address and other optional attributes etc

presence service: the capability to support management of presence information between watchers and presentities, in order to enable applications and services to make use of presence information

presentity (presence entity): any uniquely identifiable entity that is capable of providing presence information to presence service. Examples of presentities are devices, services etc. Any presentity shall have one, and only one, principal associated with it.

principal: human, organisation, program, or collection of humans, organisations and/or programs that chooses to appear to the presence services as a single actor, distinct from all other principals. A principal is associated with one or more presentities and/or watchers. A principal is said to "own" a certain presentity or watcher if such an association exists. Within the context of this specification a subscriber may be a principal to one or more presentities and/or watchers. Examples: A subscriber may be a principal to the terminals (the presentities) he owns. A program, providing a stock exchange information service to customers, may be the principal to the market quotations (the presentities) it monitors.

Note: The case where a presentity is not a subscriber requires to be further considered

subscribed-watcher: a subscribed-watcher is a type of watcher, which requests notification from the presence service of changes in a presentity's presence information, resulting in a watcher-subscription, as they occur in the future.

watcher-subscription: the information kept by the presence service about a subscribed-watcher's request to be notified of changes in the presence information of one or more presentities

Note: This definition represents an entity's request to obtain presence information, and is not related to the term "subscription" in [1]. Within this specification the term watcher-subscription (and its derivatives) purely refers to this relationship.

watcher: any uniquely identifiable entity that requests presence information about a presentity, or watcher information about a watcher, from the presence service. Special types of watcher are fetcher, poller, and subscribed-watcher. Any watcher shall have one, and only one, principal associated with it.

watcher information: information about watchers that have received or may receive presence information about a particular presentity within a particular recent span of time.

3.2 Abbreviations

For the purposes of this document the following abbreviations apply:

IETF	Internet Engineering Task Force
LAN	Local Area Network
VHE	Virtual Home Environment

4 Presence models

4a A brief introduction to the Presence Service

This clause attempts to give a simplistic high level informative overview of what presence is from a user's perspective, and how it is used to published to, and accessed by, other users.

Mark's ability and willingness to be reached for communication is defined by a set of information known as presence information. Mark's presence information may be related to his mobile network connection status, however it represents much more than just whether he has network coverage or not. Mark also defines a set of access rules to control access to his presence information. For the presence service, Mark is represented by a presentity (presence entity) associated with Mark's presence information and set of access rules.. In this example, Mark's presence information consists of user status and location information.

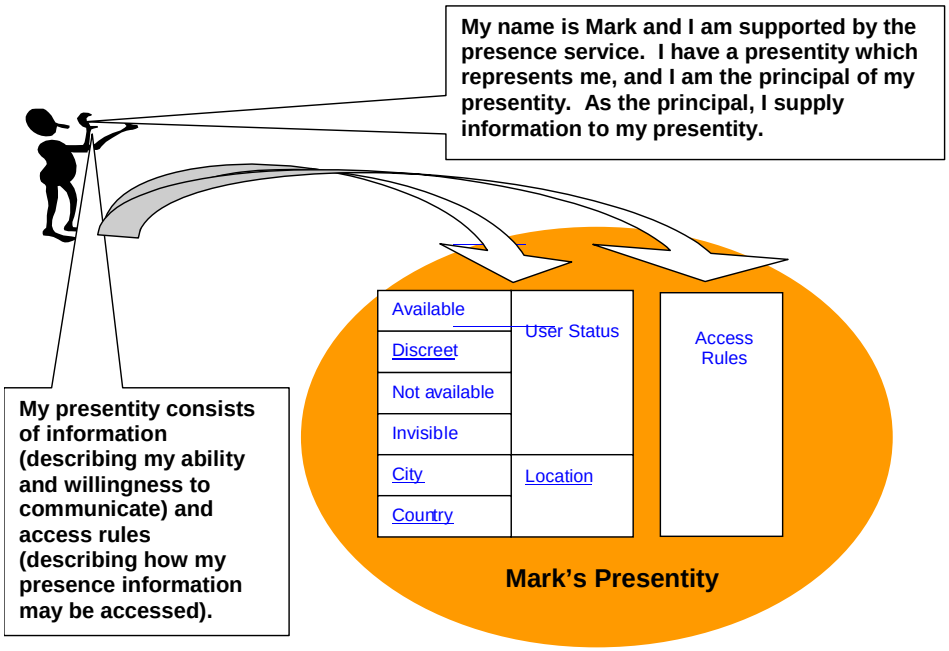

Figure 1: Principal and his representation in the presence information as a presentity

As well as representing a user such as Mark, a presentity may even be created to represent an abstract service or application (e.g. to provide road traffic information, sports results, news headlines etc.). The entity represented by the Presentity (in this case Mark) controls the supply of information for the presentity and is known as the principal; thus Mark is principal of his presentity (see Figure 1).

Paggy, Paul and Jude (e.g. Mark's callers or instant messaging buddies) who want to determine Mark's ability (and willingness) to communicate may do so by checking the status information in Mark's presentity. By doing so, Paggy, Paul and Jude become watchers of Mark (see Figure 2).

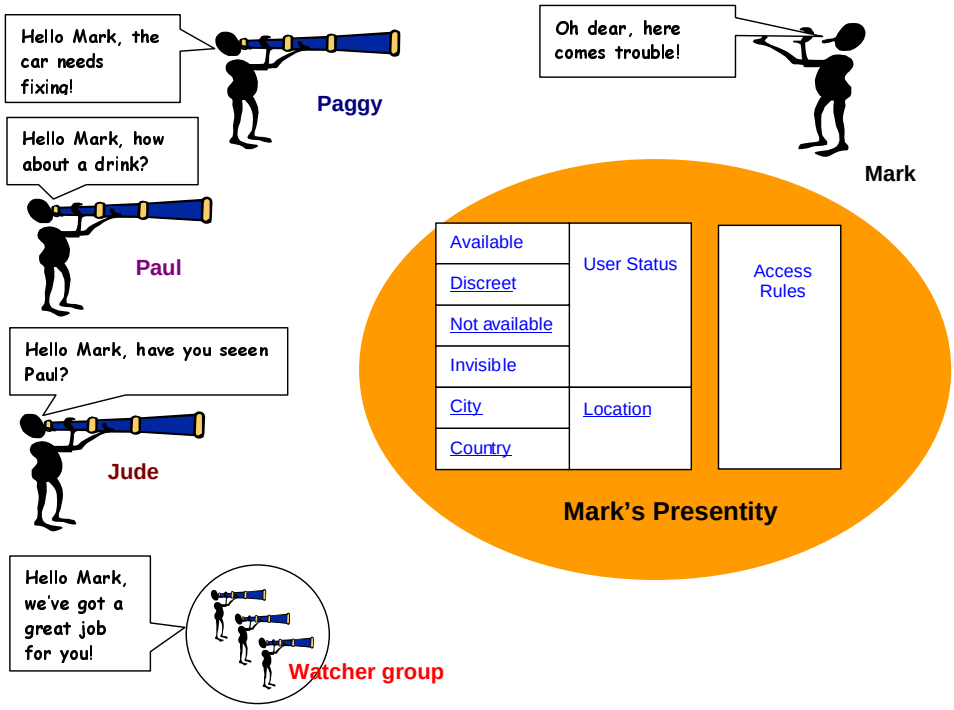

Figure 2: Watchers of Mark

To protect his privacy and confidentiality, Mark has full control over whether Paggy, Paul and Jude, or any other group of watchers, can access his presence information. Mark may give different watchers different levels of access so that, for example Paggy can see all of Mark's of presence information, Paul may only see part of it, and Jude can see none of it. Hence, Mark can control (per watcher) which parts of his presence information may be seen, and he may decide that specific watchers have restricted access, and that some do not have any access at all. Indeed, Mark may also define his presence information and set up his access rules so that some watchers are given different information (e.g. Jude is told that Mark is not available, when in fact he is available), see Figure 3.

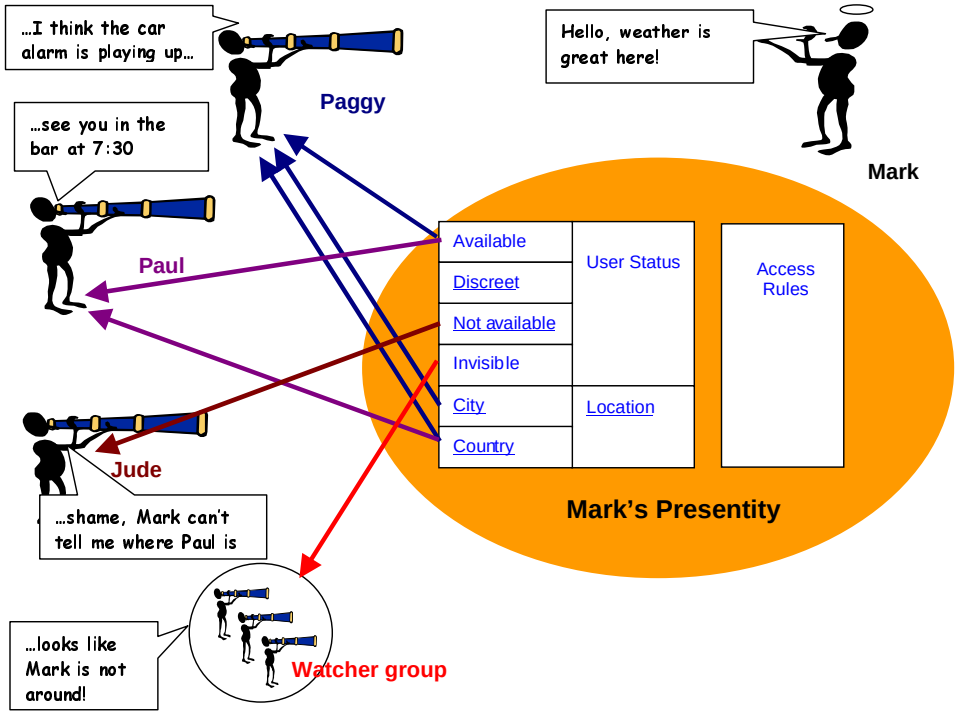

Figure 3: Application of Mark's access rules on watchers

Mark's presentity consists of dynamic and static information supplied directly by himself and/or by the network. Some of the dynamic information may be derived from a number of sources (e.g. equipment login/attachment, roaming status, keyboard activity monitoring, equipment type, location information etc.). An example of the static information could be a fixed telephone number. The network may also add further information to the presentity (e.g. the evening/night times when his mobile is usually switched offderived from his usage patterns) to provide customised presence information.

By supporting a presence service in the network, the operator has the capability to offer an exciting range of advanced presence-based services and applications.

4.1 Informative models

The below models of the presence service and presence information are not definitive, and no implementation model or architecture is implied or required by them, and are solely provided to describe the functions and roles that shall be provided by the presence service.

4.2 Roles in the presence service

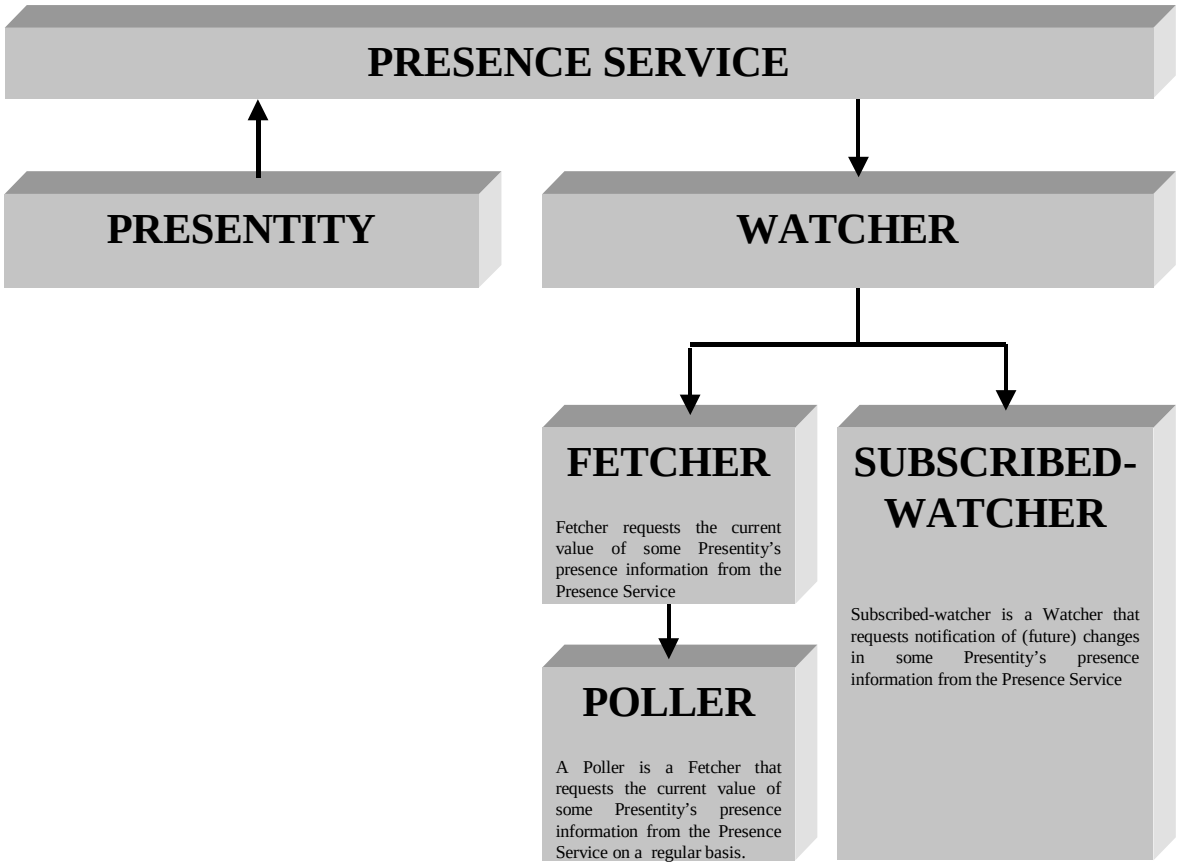

Figure 2: Presence service model

The presence service may be considered to support two main roles, as depicted in figure 2"Presence service model".

For the purposes of this TS, the following roles are identified to support the presence service:

- Suppliers of presence information

  This role represents those entities that supply presence information.

- Requesters of presence information

  This role represents those entities which request (and subsequently receive) presence information of a presentity. The presence information may also maintain data on requesters of presence information, which may also be potentially distributed (on request) to requesters of presence information. The term watchers is used to identify the requesters of presence information.

  The requesters of presence information may be associated with 2 modes of operation:

  - Information Mode

    This mode corresponds to a request-response mode and represents those entities (i.e. watchers) which simply request the current presence information of a presentity. The term "fetchers" is used to identify the receivers of this type of presence information of a presentity. The term “pollers” identifies the type of fetchers that request the presence information of a presentity on a regular or periodic basis.

  - Notification Mode

    This mode corresponds to a ‘push-type’ mode and represents those entities (i.e. watchers) which request notifications on (future) changes in presence information of a presentity. The term subscribed-watchers is used to identify the receivers of these notifications. Watcher-subscriptions for subscribed-watchers are soft-stated i.e. they are time-bound, notifications of presence information cease on expiry of the negotiated interval. The subscribed-watcher is allowed to ‘refresh’ a watcher-subscription at any time. Watcher-subscription refreshes overwrite an existing watcher-subscription for the same presentity, subject to the presentity's access rules.

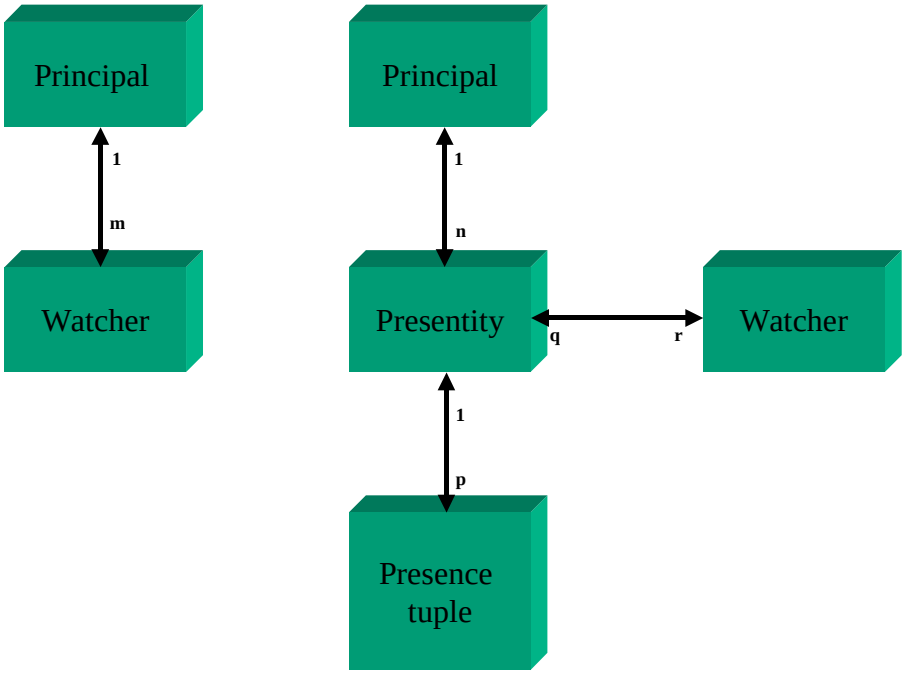

Figure 3: Presence Service Entity Relationships

The key concepts captured in figure 3 are as follows:

- a principal may be associated with one or more watchers
- a watcher is associated with one principal
- a presentity is associated with one principal
- a principal may be associated with one or more presentities.
- a presentity may be associated with one or more presence-tuples

- a watcher can have a watcher-subscription to one or more presentities
- a presentity may be watched by one or more watchers

4.3 Presence information

A logical model of a presentity's presence information consists of an arbitrary number of elements, known as presence tuples, as depicted in figure 4. Presence information for each presentity is identified by a unique identifier.

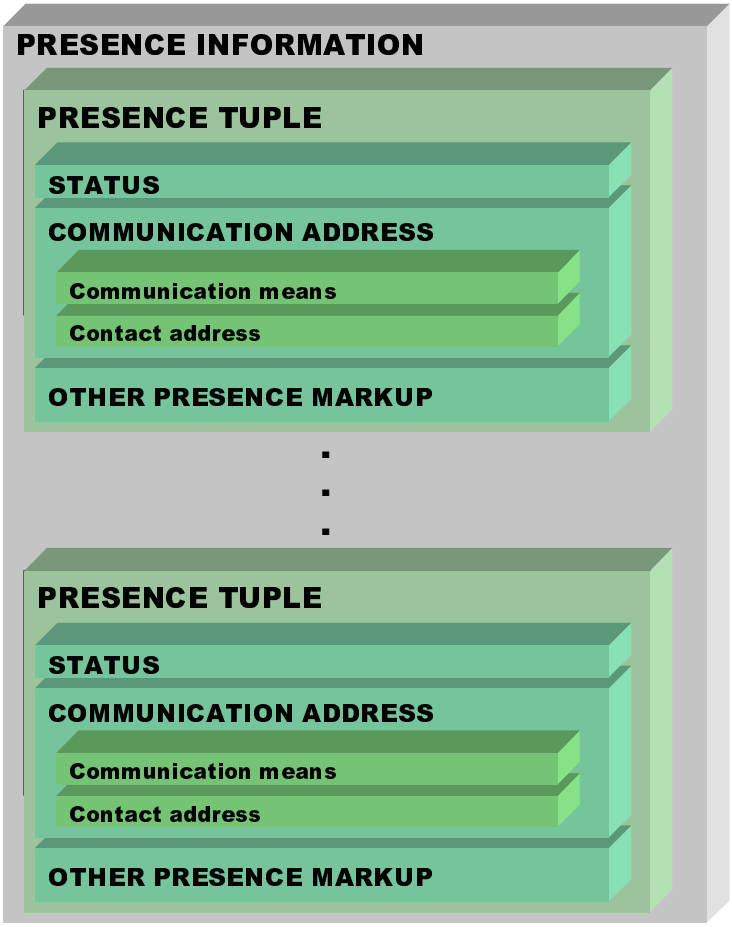

Figure 4: Presence information

Each such presence tuples contains the following information as described in RFC 2778 [3]:

- status

Table 1: Status

Item	Explanation	Example Values
status	Indicates the current condition of the device or service represented by the presence tuple	open, closed, online, offline, busy, away, do not disturb etc.

- communication address

  consists of a communication means and a contact address

Table 2: Communication address

Item	Explanation	Example Values
communication means	Information indicating a method whereby communication can take place	service type (e.g. telephony, SMS), media type (e.g. audio, video, text message), multimedia messaging service, instant messaging service etc.
contact address	Information indicating a specific point of contact via some communication means	E.164, URI, instant inbox address etc

- other presence markup

  any additional presence information

5 High level requirements

5.1 Home Environment requirements

The presence service shall provide the ability for the home environment to manage the presence information of users' devices, services and service media, even when roaming. The home environment shall be able to be both the supplier of presence information (i.e. presentities), as well as the requesters of presence information (i.e. watchers). The presence service can be regarded as a Home Environment service or a Home Environment – Value Added Service Provider (HE-VASP) service.

The home environment requirements for the support of the presence service are defined in 5.3 General requirements, and the applicable requirements in 5.4 Management requirements and 5.5 Notification and acknowledgement requirements.

> External networks (e.g. those in other PLMN's, the Internet, LANs etc.) currently support several different forms of presence service. The presence service shall enable the network to present a consistent and interoperable support of presence, such that the presence capability users can interwork with one or more other external presence services.

5.3 General requirements

The following general requirements for the presence service shall be supported:-

a) Presence information

   i) presence information for presentities shall be made available in a standardised presence information format to enable interoperability within networks.

   ii) presence information for presentities shall be made available in a standardised presence information format to enable interoperability with IETF specified presence information formats (e.g. RFC 2778 [3], RFC 2779 [4] and RFC3863 [5])

   iii) presence information for presentities shall be extensible to represent additional information, without undermining the standardised format (e.g. device capabilities)

   iv) presence information for presentities shall include a means to uniquely identify the presentity

   v) presence information for presentities shall define a particular type of presentity, representing a subscriber, with a minimum set of attributes as described below for interoperability within networks. The values for these attributes are to be determined in the Stage 2/3 specifications.

      In addition to the generic requirements described above, the presence information representing a subscriber:

      a) may include a subscriber's status attribute describing the subscriber's willingness to communicate (e.g. available, unavailable). It does not identify the status of the device (e.g. registration or attachment to the network) or of any application.

This attribute is controlled by the subscriber. It shall be possible for this subscriber's status to be provided by the subscriber, or by the network on behalf of the subscriber (subject to the subscriber's agreement). For example the subscriber could define that he's unavailable each day between 10 p.m. and 7 a.m., and the network would then be responsible for the subscriber's status update.

The format and values of this attribute shall be standardised.

Note: It is to be determined in the Stage 2/3 specifications how the Status field (in RFC2778 [3]) in notifications is completed, and whether or not the values in the subscriber status attribute, network status attribute or other information are used.

b) may include a network status attribute describing the connectivity state of the device used by the subscriber. This attribute could for example be defined using information describing the subscriber's state of connectivity to the network (e.g. attached, call active, CS attached, CS Call active with bearer information, IMS registered, PDP context information etc…).

This attribute is controlled by the network.

The format and values of this attribute shall be standardised.

Note: It is to be determined in the Stage 2/3 specifications how the Status field (in RFC2778 [3]) in notifications is completed, and whether or not the values in the subscriber status attribute, network status attribute or other information are used.

c) may include one or more communication means (e.g. SMS, telephone, e-mail, multimedia session…) and their contact addresses (e.g. MSISDN, e-mail address, NULL…) by which the subscriber may be contacted.

This attribute is controlled by the subscriber. It shall be possible for this information to be provided by the subscriber, or by the network on behalf of the subscriber (subject to the subscriber's agreement).

The format and values of the communication means shall be standardised, and the format of the contact address shall be standardised.

d) may include two types of location information, one provided by the network (e.g. geographical co-ordinates) and/or one provided by the subscriber (e.g. "at home").

The network provided location is controlled by the network, and the subscriber provided location information is controlled by the subscriber. It shall be possible for the subscriber provided location information to be furnished by the subscriber, or by the network on behalf of the subscriber (subject to the subscriber's agreement).

The format of the network provided location shall be standardised, and the format of the subscriber provided location shall be standardised.

e) may include a priority attribute giving a relative priority for each of the defined communication means and contact address pairs. It is via this priority attribute that the subscriber can indicate his preference for the order in which the communication means and contact address pairs should be used.

This attribute is controlled by the subscriber. It shall be possible for the priority information to be provided by the subscriber, or by the network on behalf of the subscriber (subject to the subscriber's agreement).

The format and values of this attribute shall be standardised.

f) may include a text attribute (e.g. "In a meeting until 4 p.m.")

This attribute is controlled by the subscriber. It shall be possible for the text information to be provided by the subscriber, or by the network on behalf of the subscriber (subject to the subscriber's agreement).

The format of this attribute shall be standardised.

b) A means to uniquely identify the watcher

c) Forward compatible presence service

Presence service shall leverage current and evolving presence technology by re-using existing standards as far as possible and proposing extensions (as necessary) to existing standards.

d) Interoperability with external presence services

External networks (e.g. those in other PLMN's, the Internet, LANs etc.) currently support several different forms of presence service. The presence service shall enable the network to present a consistent and interoperable support of presence, such that the presence capability users can interwork with one or more other external presence services.

e) Consistent and interoperable presence service

Regardless of the service using presence information, the presence service shall be supported in a consistent and interoperable manner between the UE and the network

f) Transport independence

It shall be possible to use the presence service independent of the bearer or transport mechanism. Restrictions may apply due to the nature of the underlying transport mechanism (e.g. a CS or PSTN terminal may not be capable to supply the same presence information as a terminal attached to the IM CN Subsystem)

g) Presence service quality of service

i) the Presence Service shall enable a watcher, if required, to request a time after which delivery of the requested information shall not take place.

ii) the Presence Service shall enable a presentity to indicate an expiry time for the presence information, if required.

iii) the Presence Service shall enable presence information delivered to a watcher to be marked with an expiry time, if required.

h) Presence and other user services

The operation of Presence Service may be offered both in parallel and independent of other services, e.g. supplementary services, teleservices, bearer services or any other services.

i) Simultaneous access to presence information from multiple terminals

It shall be possible to access presence information simultaneously from multiple terminals (e.g. presentity or watcher would be able to access the presence service via mobile phone and PC).

j) Access to the presence service from external applications

It shall be possible for external applications to be presentities/watchers.

5.4 Management requirements

The following management requirements shall be supported for the presence service:

a) Access control to the presence information

The presentity shall be able to manage the access to its presence information in compliance with the principal's privacy and access rules requirements detailed in 6.1 and 6.2.

The presentity shall have the ability to accept or reject a request for presence information on a per watcher basis, with the option:-

i) once only per watcher (e.g. set up access rules for known watcher, groups of watchers, anonymous watcher-subscriptions, etc.),

ii) for each presence information request (e.g. for watchers that are unknown or not set up in the current access rules).

It shall be possible for the presence service to make access control decisions on behalf of the presentity (e.g. when the presentity is out of contact) subject to the principal's privacy.

It shall be possible to inform the presentity of watcher-subscription requests

It shall be possible to report existing watcher-subscriptions to the presentity (on request or periodically).

It shall be possible for the presentity to request the watcher information.

b) Not used

c) Supplying data to the presence information

When supplying data it shall be possible to update only part of the presence information.

d) Requesting data from the presence information

It shall be possible to request the current value of presence information data on demand at any time (i.e. a fetcher) or on a periodic basis (i.e. a poller) subject to principal's privacy, or to be notified of subsequent changes in presence information data (except when such notification is prevented by access rules

It shall be possible for a watcher to define which parts of a presentity's presence information it receives, subject to the principal's privacy requirements.

It shall be possible for watcher to request presence information anonymously (i.e. the watcher's identifier will not be revealed to the presentity). This request can be accepted or rejected, depending on the principal's privacy.

A Watcher's interest to a presentity's presence information shall not be revealed to other watchers.

Watcher-subscription to a presentity's presence information

i) an entity shall be able to watcher-subscribe to a presentity's presence information at any time, i.e. to request notification from the presence service of (future) changes in any of the attributes or only in the attributes specified by the watcher (subject to the principal's privacy). Note, that by this watcher-subscription the entity becomes a subscribed-watcher.

ii) subscriptions are soft-stated. The subscribed-watcher shall be able to refresh a watcher-subscription to the presentity's presence information at any time. A watcher-subscription refreshes overwrite an existing watcher-subscription for the same presentity, subject to the presentity's access rules – the duration of a watcher-subscription starts from the time it is accepted.

iii) the subscribed-watcher shall be able to determine the status of his watcher-subscription to that presentity's presence information, at any time.

iv) the subscribed-watcher shall be able to cancel his watcher-subscription to a presentity's presence information at any time. Whenever a subscribed-watcher withdraws its watcher-subscription from a presentity's presence information, the subscribed-watcher shall no longer be receiving notifications regarding the presentity's presence information.

v) an unauthorised third party shall not be able to cancel a subscribed-watcher's watcher-subscription to a presentity's presence information

e) User availability and mobility

The presence service shall continue to be supported if the environment into which the user has moved supports presence service. The presence service shall take into account changes in the availability of users (e.g. the user is out of contact or not reachable, despite having activated his presence) or his mobility (e.g. wherever he may be in his home environment or in a visited network).

f) Not used

g) Access to presence service

i) it shall be possible for the presence service to accept presence information from a presentity at any time

ii) it shall be possible for the presence service to accept requests from, and provide presence information to, an authorised watcher at any time

5.5 Notification and acknowledgement requirements

The following notification and acknowledgement presence service requirements shall be supported:-

a) Presence data modification and monitoring requests

The presence service shall be able to support the acknowledgement of any requests to monitor a presentity's presence information (i.e. from watchers)

If a subscribed-watcher establishes a watcher-subscription to a presentity's presence information:-

i) the presence service, depending on the presentity's access rules, shall inform the subscribed-watcher if the presentity refused the subscribed-watcher's watcher-subscription

ii) if the subscribed-watcher's watcher-subscription to presentity's presence information is cancelled, the presence service shall inform the subscribed-watcher of the cancellation

iii) it shall be possible for the presentity to configure the presence service to deny a subscribed-watcher's subscription, whilst appearing to the subscribed-watcher as if the subscription has been granted (this is sometimes called "polite blocking")

6 Privacy

6.1 General privacy requirements

The privacy aspect of presence information and the need for authorisation before providing presence information shall be configurable by the user (i.e. presentity).

The following privacy requirements shall be supported:-

- principal’s privacy

  a principal of a presentity shall, at any time, be able to control to whom, for how long and what (all or part of) presence information of the presentity is provided, and a principal of a watcher shall, at any time, be able to control to whom, for how long and what (all or part of) watcher information of the watcher is provided

Note: need to consider where subscriber’s privacy (as distinct from principal’s privacy) requires to be addressed.

Any services using the presence information shall ensure privacy agreement before releasing presence information. The presence service does not address deployment specific issues (e.g. where agreements are stored or how they are negotiated). It only gives requirements for privacy management.

Specific local, national, and regional privacy regulations shall be complied with. In particular, an operator shall, at any time, be able to override principal’s privacy if required to do so.

6.2 Access rules

The principal that controls the presentity shall be able to define access rules, in order to control how the presentity’s presence information is made available for watchers.

These access rules shall define:

- a watcher or groups of watchers allowed access to the presentity’s presence information. For example: watchers x and y are allowed, or only watchers in group z are allowed, or all watchers and groups are allowed.

- the validity of the access authorisation granted for a given watcher or groups of watchers. The access to the presentity’s presence information can be restricted for a certain period (i.e. duration or number of requests), or during specific periods of the day.

- the attributes of the presentity's presence information that can be made available to a given watcher or groups of watchers.

- the ability to provide different presence information (i.e. both number of attributes and values of attributes) based on the watcher, and principal's preferences (e.g. its availability). For example: watcher x receives 'Online/Instant Messaging/im:a@there.com', while group y receives 'Offline/Instant Messaging/im:a@there.com'.

A set of default access rules shall be defined by the principal.

7 Security

The use and access to the presence service shall be supported in a secure manner. It shall only be possible for the presence information to be supplied and/or updated by the presentity or the home environment as identified in clause 5 "High Level Requirements".

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

It shall be possible to authenticate at any time a watcher and/or a presentity requesting access to the presence service. Existing security mechanisms as well as mechanisms specific to presence service may be used.

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

- Presence information and notifications

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

8 Charging

The presence service shall be able to support various charging mechanisms both for On-line and Off-line charging. The following charging characteristics shall be considered:

- charging for a user's registration as a presentity

- charging for each subscription to presence information for a user

- charging for presence information retrieval for users

- charging for presence information notifications received for users

- charging for presence information usage when in a visited network

The above list is not exhaustive.

9 Administration

The following administration requirements shall be supported.

Note: The different logical steps (provision, registration, activation) might be combined. For example when a principal requests a watcher-subscription, a watcher associated with him is automatically registered in the Presence Service.

9.1 Provision

Provision is an action taken by the service provider to make the presence service available to a principal. Provision may be:

- General: where the service may be made available to all principals without prior arrangements being made with the service provider.

- Pre-arranged: where the service is made available to an individual principalonly after the necessary arrangements such as login name, password have been made with the service provider.

This provision action shall allow the principals to subsequently register within the Presence Service as a presentity, as a watcher or as both.

9.2 Withdrawal

Withdrawal is an action taken by the service provider to withdraw the presence service from the principal. Withdrawal may be:

- General: where the presence service is removed from all principals
- Specific: where the presence service is removed per principal.

9.3 Registration

Registration is an action taken by the service provider or the principal to provide information necessary for presentities and/or watchers to use the Presence Service. For example, a subscriber could request the creation of a presentity associated with him and provide the corresponding access rules.

It shall be possible to take this registration action under the condition that the presence service is available for the principal. (i.e. the provision has been performed previously).

This registration process may be performed at any time by the principal or service provider to create new presentities/watchers.

The service provider may provide privacy control at registration time on behalf of a presentity.

9.4 Erasure

Erasure is an action taken at any time by the service provider or the principal in order to cancel a registration.

9.5 Activation

Activation is an action taken at any time by the service provider, the presentity or the watcher to bring the Presence Service into the active state.

It shall be possible to activate the service once the presentity or watcher has been registered.

Once the presentity or watcher is in an active state,

- This presentity or watcher may invoke Presence Service features
- Other presentities or watchers may invoke Presence Service features concerning this presentity or watcher (e.g. by subscribing to its presence information)
- The Presence Service may invoke Presence Service features concerning this presentity or watcher (e.g. by notifying changes in the presence information)

9.6 Deactivation

Deactivation is an action taken at any time by the service provider, the presentity or the watcher to bring the Presence Service into the non-active state.

9.7 Invocation

Invocation is an action taken at any time by the presentity or watcher (e.g. by requesting presence information) or by the Presence Service as a result of a particular condition (e.g. by notifying presence information's changes) in order to invoke the Presence Service features.

Annex A (informative): Example presence service use cases

Immediate Messaging Use Case

- Premise:

  User is in-and-out of coverage

  Others wish to send a message and get a response - now

- Considerations

  User's Presence provides info regarding availability (Yields measure of Probability of message delivery)

- Presence capability can be separated from IM

  Functional Separation

- Sequence

  User is out and about (having meetings or just travelling)

  Availability status gets updated as needed (User control - change to 'unavailable - in meeting', Network control - out-of-coverage / busy-in-call)

- Co-worker wants to send you a note

  Check of Presence Info lets others see if user is available (If available - provides addressing info (e.g. IM server / account ids))

- IM Server handles message deliveries

  Status updates available at any time

Location Info in Presence Use Case

- Premise:

  User is travelling per a schedule

  Others looking to find out when user will arrive

  Alternative model is to know where to go to meet user

- Considerations

  User's Presence Info could have activity indicator (e.g. 'in a meeting' or 'driving')

- System may have access to location information on user

  Issue would be the granularity/resolution

- System may have access to user's 'calendar'

  Would make a plan available

- Security/authentication aspects of disclosures

- Sequence

  User is out and about (having meetings or just travelling (Assume that user activity indication available (For example: 'unavailable - driving')

  System could correlate location information with activity (Answer questions like - is user at planned meeting?, If travelling, could correlate distance with minimum transit time)

System could maintain progress on plan from calendar (System may be able to determine if user is running late or not, User could revise plan or provide annotated information)

Co-worker wants to know if you are available (System provides current activity, possible links to schedule)

- Family wants to know if user is on way home

  Activity indication of ‘driving’ may assist in determination

  Current location info could help determine how far from home

- Meet-me example

  Service may correlate matching info (Example where Activity Indication - ‘Shopping’ & Location - ‘Mall’, Friend with matching codes could be flagged, Could IM to determine which store or to have lunch)

  Service could manage meeting maker (May have appointment scheduled with others, Could check status to see if everybody was in right location)

Message Modality Control Use Case

- Premise:

  User has different means to communicate (voice, text…)

  User may indicate preferences

  Voice number is managed by entity monitoring status

- Considerations

  Content format adaptation available (e.g. text-to-speech (synthetic voice) or speech-to-text)

  User preferences set desired message format (May change the official communication device address)

  Related services subscribe to user status (Cell net could be watcher to provide value-add/quick routing)

- Sequence

  User is in a meeting (can’t take a phone call)

  Status shows ‘busy - in a meeting’ (Presence status listed as ‘unavailable for voice’, Option for speech-to-text delivery provided if available)

  If friend can send text - does so (Works as expected)

  If friend has a voice device (Calls into user’s number, Switch sees speech delivery disabled - conversion offered, Switch connects caller to speech-to-text converter, Text is sent to user, If caller stays on circuit, could engage in two-way dialog)

- Premise:

  User is travelling and changes plane

  Others looking to communicate with the user

  Service available to ‘take a message’

- Considerations

  Service has access to User’s state

  Service could be associated with User info (May be dependent on state or watcher identification)

  Service may deliver ‘markup’ contact for reply (Ideal is to enable programmable or responsive operations)

Traveler Changing Planes Use Case

- Sequence

  User is on a plane

  User (more correctly - device) is not connected to any network (Presence status listed as ‘unavailable’, Service (‘take a message’) shown as available)

  Friend wants to pass some info and sees ‘unavailable’ status (Uses ‘take a message’ to save a friendly note)

  Co-worker needs some specific info (Uses ‘take a message’ to record a ‘get back to me’ note)

- User arrives at airport

  User (more correctly - device) is not connected to any network (Presence status listed as ‘unavailable’, Service (‘take a message’) shown as available) ‘Take a Message’ Service gets update and sends a report (Provides an inbox type message)

  User may interact to read the messages (stored by service) (Messages could be selectively managed (read/forward/delete))

  Addresses in Notes are associated with status information (Effectively invokes a dynamically generated buddy list, May have been entities that were not part of regular buddy list, Very easy to ‘return the call’ with know availability information)

- User gets on next plane

  Status changes again - reverts to unavailable handling

Annex B (informative): Change history

Change history											
TSG SA#	SA Doc.	SA1 Doc	Spec	CR	Rev	Rel	Cat	Subject/Comment	Old	New	Work Item
			22.141					Produced during Presence Adhoc 18th-19th April, Seattle, Washington, USA	0.0.0	0.1.0	Presence
			22.141					Produced during S1 plenary 7th-11th May, Helsinki, Finland	0.1.0	0.2.0	Presence
			22.141					Produced for TSG-SA#12	0.2.0	1.0.0	Presence
			22.141					Produced during Presence adhoc 5th-6th June, Sophia Antipolis, France	1.0.0	1.1.0	Presence
			22.141					Produced during Presence adhoc 26th-28th June, Dallas, Texas, USA	1.1.0	1.2.0	Presence
			22.141					Produced during Presence adhoc 10th -11th July, Lake Tahoe, Nevada, USA	1.2.0	1.3.0	Presence
			22.141					Produced during Presence adhoc 10th -11th July, Lake Tahoe, Nevada, USA	1.3.0	2.0.0	Presence
SP-13	SP-010444	S1-010841	22.141			Rel-5		Approved at SA #13	2.0.0	5.0.0	Presence
SP-14	SP-010677	S1-011059	22.141	001		Rel-5	C	Protection against replay attacks	5.0.0	5.1.0	PRESNC
SP-14	SP-010677	S1-011210	22.141	002		Rel-5	C	Reserved for Presence	5.0.0	5.1.0	PRESNC
SP-14	SP-010677	S1-011211	22.141	003		Rel-5	C	Clarification to Presence access rules	5.0.0	5.1.0	PRESNC
SP-14	SP-010677	S1-011212	22.141	004		Rel-5	B	Clarification on charging mechanisms	5.0.0	5.1.0	PRESNC
SP-14	SP-010677	S1-011213	22.141	005		Rel-5	F	Clarification of registration and administration procedures	5.0.0	5.1.0	PRESNC
SP-14	SP-010677	S1-010960	22.141	006		Rel-5	F	Use of 'Principal' within TS 22.141	5.0.0	5.1.0	PRESNC
SP-14	SP-010677	S1-011218	22.141	008		Rel-5	F	Clarification of presence information requirements	5.0.0	5.1.0	PRESNC
SP-15	SP-020056	S1-020306	22.141	009		Rel-5	D	A brief introduction to the Presence Service	5.1.0	5.2.0	PRESNC
SP-15	SP-020056	S1-020307	22.141	010		Rel-5	D	Correction to the number of roles in the Presence Service	5.1.0	5.2.0	PRESNC
SP-15	SP-020056	S1-020430	22.141	011		Rel-5	C	CR 22.141 Rel.5 Selective Notifications	5.1.0	5.2.0	PRESNC
SP-15	SP-020056	S1-020602	22.141	012		Rel-5	F	CR to 22.141 - Clarifications on identifier's hiding	5.1.0	5.2.0	PRESNC
SP-15	SP-020056	S1-020619	22.141	013		Rel-5	C	CR to 22.141 on Multiple terminal support in presence service	5.1.0	5.2.0	PRESNC
SP-15	SP-020056	S1-020623	22.141	014		Rel-5	C	Access from external applications	5.1.0	5.2.0	PRESNC
SP-16	SP-020267	S1-021043	22.141			Rel-6		Updated from Rel-5 to Rel6; Rel5 deleted	5.2.0	6.0.0	
SP-17	SP-020560	S1-021592	22.141	015		Rel-6	F	Presence TS - Cleaning of requirements	6.0.0	6.1.0	PRESNC
SP-17	SP-020560	S1-021781	22.141	016		Rel-6	F	Presence TS - Tidy up of security requirements	6.0.0	6.1.0	PRESNC
SP-19	SP-030025	S1-030066	22.141	017	-	Rel-6	C	Clarification of network status attribute description within Presence Service Stage 1	6.1.0	6.2.0	PRESNC
								2004-07-02: Repair corrupt file.	6.2.0	6.2.1	
SP-26	SP-040728	S1-040993	22.141	018	-	Rel-6	F	Delete Requirements for IP session function	6.2.1	6.3.0	OSA3
SP-27	SP-050059	S1-050219	22.141	019	-	Rel-6	F	Removal of Reference to TS 22.121	6.3.0	6.4.0	TEI
						Rel-6		2005-07: File failed to open correctly in Word 2003.	6.4.0	6.4.1	

Change history											
TSG SA#	SA Doc.	SA1 Doc	Spec	CR	Rev	Rel	Cat	Subject/Comment	Old	New	Work Item
SP-30	SP-050806	-	22.141	0021	1	Rel-6	F	Correction to Reference in Presence TS	6.4.1	6.5.0	PRESNC
SP-30	SP-050747	S1-051225	22.141	0022	-	Rel-7	F	Introduction of generic (non-wireless specific) Presence Service	6.4.1	7.0.0	FBI
SP-42	-	-				Rel-8		Updated from Rel-7 to Rel-8	7.0.0	8.0.0	
SP-46	-	-	-	-	-	-	-	Updated to Rel-9 by MCC	8.0.0	9.0.0	
2011-03	-	-	-	-	-	-	-	Update to Rel-10 version (MCC)	9.0.0	10.0.0	
2012-09	-	-	-	-	-	-	-	Updated to Rel-11 by MCC	10.0.0	11.0.0	
2014-10	-	-	-	-	-	-	-	Update to Rel-12 version (MCC)	11.0.0	12.0.0	
2015-12		-	-	-	-	-	-	Updated to Rel-13 by MCC	12.0.0	13.0.0	
2017-03	-	-	-	-	-	-	-	Updated to Rel-14 by MCC	13.0.0	14.0.0	
2019-07	-	-	-	-	-	-	-	Update to Rel-15 version (MCC)	14.0.0	15.0.0	
SA#88e	-	-	-	-	-	-	-	Updated to Rel-16 by MCC	15.0.0	16.0.0	
2022-03	-	-	-	-	-	-	-	Updated to Rel-17 by MCC	16.0.0	17.0.0	
2024-03	-	-	-	-	-	-	-	Updated to Rel-18 by MCC (and issue with v.18.0.0 upload)	17.0.0	18.0.1	
2025-10	-	-	-	-	-	-	-	Updated to Rel-19 by MCC	18.0.1	19.0.0	

History

Document history		
V19.0.0	October 2025	Publication