Network Working Group   Krisztian Kiss (ed.)
Internet-Draft   Nokia
Expires: April 19, 2003   October 18, 2003

Requirements for Presence Service in 3GPP Wireless Systems
draft-kiss-simple-presence-wireless-reqs-03

Status of this Memo

   This document is an Internet-Draft and is in full conformance
   with all provisions of Section 10 of RFC2026 [1].

   Internet-Drafts are working documents of the Internet
   Engineering Task Force (IETF), its areas, and its working
   groups. Note that other groups may also distribute working
   documents as Internet-Drafts. Internet-Drafts are draft
   documents valid for a maximum of six months and may be
   updated, replaced, or obsoleted by other documents at any
   time. It is inappropriate to use Internet- Drafts as reference
   material or to cite them other than as "work in progress."

   The list of current Internet-Drafts can be accessed at
   http://www.ietf.org/ietf/1id-abstracts.txt

   The list of Internet-Draft Shadow Directories can be accessed
   at http://www.ietf.org/shadow.html.

   The distribution of this memo is unlimited.

Abstract

   This Internet-Draft defines requirements for Presence Service
   in 3GPP wireless systems.

Table of contents

[1](#).   Introduction

   This Internet-Draft lists the requirements for Presence
   Service in 3GPP wireless systems [24][25][26]. The 3GPP
   Presence Service requirements are defined in [27], the 3GPP
   Presence Service architecture is defined in [28], presence
   service information flows and protocol details are defined in
   [29]. The requirements on the Session Initiation Protocol
   (SIP) for the Release 5 of the 3GPP IP Multimedia Subsystem
   are described in [19]. Presence Service is referenced as
   defined in IMPP Working Group in documents [5] and [6].

   This document does not document requirements that have led to
   the creation and work in progress on a number of SIMPLE WG
   specifications, i.e. subscriptions and notifications of user
   presence [7], the SIP event notification extension for

collections [9], the SIP Event Template-Package for Watcher
Information documents [11][12], the content indirection
mechanism [17] and the SIMPLE Presence Publication Mechanism
[15]. Rather this document lists only requirements that are
additional to those that have led to the mechanisms proposed
in these documents.

The document also assumes the usage of the Common Presence and
Instant Messaging (CPIM) Presence Information Data Format
(PIDF) defined in [8] as the default presence document data
format, however some of the requirements presented here might
require extensions to PIDF.

The requirements presented in this document are proposed to be
evaluated by the SIMPLE Working Group. The result of this
evaluation process would help to determine the work expected
to be done in IETF and identify the work which might be done
in other standardization bodies, such as 3GPP. Thus, a more
precise work-share between standardization bodies could be
worked out. The overall goal of these requirements is to allow
the development of a fully standardized presence application
for wireless terminals, utilizing existing IETF and 3GPP
specifications.

Note that some of the requirements herein may be already
addressed in specific requirements documents, i.e. the data
manipulation requirements of SIMPLE systems [10], the presence
specific event notification filters requirements [14], the
rate limiting of event notifications requirements [16], the
watcher information filtering requirements [21], the SIMPLE
Presence Publication Requirements [23], the Efficient Delivery
of Presence Information requirements [37].

1.1   Conventions used in this document

This document does not specify any protocol of any kind.
Therefore, the use of the key words "MUST", "MUST NOT",
"REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT",

"RECOMMENDED", "MAY", and "OPTIONAL" in this document, as
described in RFC 2119 [2], does not apply.

2.   General characteristics of Wireless Systems

The radio interface of wireless systems is often a scarce
resource. As such, the message exchange over the radio
interface and the size of the messages should be efficiently
compact and kept to a minimum. All the mechanisms developed
should make an efficient use of the radio interface.

There are existing mechanisms to fulfill this requirement,
such as signaling compression [31], partial publication,
partial notification [20], content indirection [17]. These
mechanisms must not be exclusive and must be capable to work
together.

As terminals could be rather small devices, the memory and
power consumption requirements, requirements for processing
power, and for screen size and rendering capabilities should
be kept to a minimum. Mandating support for additional
protocols and mechanisms in the wireless terminal must meet
this criteria.

3.   Requirements

This section lists the requirements for Presence Service in the
3GPP IP Multimedia Subsystem wireless environment. Generally,
these protocol requirements stem from the special characteristics
of wireless systems, and the specific set of capabilities
specified by the 3GPP. More information on these aspects can be
found in 3GPP TS 23.228 [24].

3.1   Addressing Requirements

ADDR-REQ1: It must be possible to use a single address to
    identify the presentity and the watcher.

ADDR-REQ2: Use of E.164 numbers [32] in addressing presence
    service entities must be supported.

3.2   Publishing requirements

Generic SIMPLE Presence Publication Requirements are listed in
[23].

PUBL-REQ1: Standardized mechanism to publish presence information
    There must be a standardized mechanism to publish the
    presence information.

PUBL-REQ2: Partial publishing
    The publish mechanism must allow a PUA to change only part
    of the presentity's presence information. For example, a
    PUA must be able to publish one single <tuple> element of
    the presentity's PIDF document, while the document
    contains several <tuple> elements.

PUBL-REQ3: Basic operations of publishing
    It must be possible for the PUA to add segments to the
    presence information as well as overwrite, modify or
    remove existing elements of the presence information.

PUBL-REQ4: Mandatory-to-implement MIME type for presence document
    There must be one mandatory-to-implement MIME type for the
    publish mechanism.

PUBL-REQ5: Inclusion of direct content in the presence document
    It must be possible for the presentity to include direct
    content in the presence document. If the direct content is
    part of the presence document, the signaling compression
    should be able to maintain the compression efficiency.

PUBL-REQ6: Multiple PUAs
    The publication mechanism must allow simultaneous
    publishing from multiple distinct PUAs of a single
    presentity.

PUBL-REQ7: Identifiers for PUAs
    It must be possible to allocate unique identifiers for
    every distinct PUAs of a particular presentity.

PUBL-REQ8: Identification of segments
    The PUA must be able to publish to a specific segment of
    the presence document, shared among many PUAs (the number
    of sources must neither be limited nor pre-defined). This
    means that the published segments need to be identified
    across all of the PUAs of a particular presentity. The PUA
    must be able to generate identifiers for the published
    segments.

PUBL-REQ9: Discovering existing segments
    It must be possible for the PUA to discover existing
    segment identifiers together with their content published
    by other PUAs belonging to the same presentity.

PUBL-REQ10: Hard-state segments
    It must be possible to include hard-state segments in the
    presence documents. This means that in case the PUAs do
    not refresh presence information, the hard-state segments
    remain available for the watchers.

PUBL-REQ11: Feedback on publishing
    The PUA must be able to receive feedback about the result
    of a publishing transaction, the feedback must contain
    enough information for the principal controlling the
    presentity to know that the published presence information
    was successfully composed into the presence document by
    the Presence Compositor.

3.3   Subscription and notification requirements

SUBNOT-REQ1: Presence information filtering
    It must be possible for a watcher to select certain
    elements from the presence information that he wants (or
    does not want) to receive notifications for. As an
    example, the watcher may only want to be notified when the
    presentity becomes available for conferencing.
    The Presence Server must be able to construct the presence
    document to be delivered to the watcher according to the
    watcher's filtering preferences.
    Note that when determining the elements to be included in
    the presence document, authorization rules are also needed
    to be taken into account.
    Note that there are detailed presence event filtering
    requirements listed in [14].

SUBNOT-REQ2: Limiting the rate of event notification
    The watcher must be able to limit the maximum rate at
    which the notifier can generate notifications in a
    subscription.
    Note that there are detailed requirements for the throttle
    mechanism listed in [16].

SUBNOT-REQ3: Anonymous subscription
    It must be possible for the watcher to request an
    anonymous subscription (i.e. the watcher's identifier will
    not be revealed to the presentity). The anonymous request
    may be accepted or rejected, depending on the presentity's

authorization rules as described by the AUTH-REQs.
Note that this requirement may be met with the overall
privacy solution for SIP.

SUBNOT-REQ4: Gathering information on presence information
It must be possible for the watcher to determine what presence
information is available for a particular presentity before
fetching or subscribing to the presence information elements
with actual values.

SUBNOT-REQ5: Direct content inclusion in presence information
It must be possible for the watcher to receive
notifications including direct contents. The mechanism
selected for notifying large size content must make
efficient use of the network resources and satisfy generic
wireless requirements as described in section 2.

SUBNOT-REQ6: Content indirection
Generic requirements for content indirection are listed in
[13]. In connection to presence the following requirements
have been identified: the Presence Server should be able
to perform content indirection. Watchers should have the
capability to indicate the support of content indirection.
The Presence Server must honor watcher's preferences
whether to perform content indirection or not when it
detects a situation where content indirection should be
performed.

SUBNOT-REQ7: Subscription on behalf of another user
It must be possible for a watcher to subscribe to the
presentityÆs presence information on behalf of another
user. As an example, an Application Server may act as a
network-based watcher to provide presence based call
control, or a Resource List Server may collect
notifications from the individual resources of the
presentity collection on behalf of the watcher.

3.4   Requirements for the content of the presence document

CONT-REQ1: Unique identifiers for presence segments
     The presence document contains presence segments. Each
     presence segment must contain a unique identity which
     makes it distinguishable from other presence segments
     inside the presence document.

CONT-REQ2: Application specific identifiers
     It must be possible to include application specific
     identifiers in a presence tuple. This means that a
     publishing application running in a PUA is able to address
     a specific presence tuple to its peer watcher application
     running in the watcher user agent.

CONT-REQ3: Rich content of the presence segments
     RFC 2778 [6] defines the presence information element to
     consist of a STATUS marker, an optional COMMUNICATION
     ADDRESS, and optional OTHER PRESENCE MARKUP. A
     COMMUNICATION ADDRESS includes a COMMUNICATION MEANS and a
     CONTACT ADDRESS.

     As a further requirement for this definition, it must be
     possible to define rich content for a presence information
     element (e.g. for the communication means: voice, video,
     instant messaging, application). One possible solution to
     fulfill this requirement is defined in [30], [35] and [36].

CONT-REQ4: Multivalue concept
     It must be possible to include multiple instances of the
     semantically same presence information in the presence
     document. The different instances should contain different
     values of the same presence information and used to be
     shown for different watchers. The different watchers must
     only receive those instances of the presence information
     they are authorized to by the presentity. As an example,
     one group of watchers is shown a different value for the
     status of presentity than the other.
     The Presence Server must be able to distinguish whether
     two presence information elements contain semantically
     different presence information or they are different
     instances of the semantically same presence information.

CONT-REQ5: Geographic location information
     There must be a standardized attribute for the geographic
     location information within the presence document.

CONT-REQ6: PresentityÆs status
There must be a standardized attribute for the
presentityÆs status within the presence document.

3.5   Authorization requirements

This section defines the requirements for how presentity is
able to authorize the presence subscriptions. Generic SIMPLE
data manipulation requirements are listed in [10].

AUTH-REQ1: Standardized setting of authorization policy
There must be a standardized mechanism for the presentity
to control the authorization policy related to his own
presence information.
This means that the authorization policy document format
and a set of manipulation operations upon that format must
be standardized.

AUTH-REQ2: Extensibility of authorization policy
It should be possible for network operators to extend the
format of the authorization policy document and the
operations upon that format based on local policy.

AUTH-REQ3: Expressiveness of authorization rules
It must be possible for the presentity to set separate
authorization rules for different watchers and groups of
watchers. With these rules the presentity must be able to
override the default behaviour of the presence server for
the generation of notifications and content of the
notifications. As an example, only watchers belonging to a
particular group are allowed to receive information
related to presentity's location.

Krisztian Kiss   3GPP Presence Requirements   October 2003

AUTH-REQ4: Managing the authorization policy from multiple sources
It must be possible for the presentity to manage the
authorization rules from multiple sources (e.g. from
different terminals of the presentity or by the service
provider on behalf of the presentity). It must be possible
for the presentity from one source to learn the changes in
the authorization rules changed by other sources belonging
to the same presentity.

AUTH-REQ5: Granularity of access rights
    It must be possible for the presentity to grant access
    rights separately for all elements of the presence
    information.
    RFC 2778 [6] defines a model for presence information.
    Based on this model more specific requirements can be
    stated:
    It must be possible for the Presence Server to decide
    based on authorization rules whether to include a certain
    tuple in the notification. It must be possible to base
    that decision on any element in the tuple. In the default
    case these must include at least TUPLE ID, CONTACT
    ADDRESS, COMMUNICATION MEANS and STATUS attributes. As a
    special case, it must be possible for the Presence Server
    to provide different status values for same COMMUNICATION
    ADDRESS or combination of COMMUNICATION ADDRESS and OTHER
    PRESENCE MARKUPs.

AUTH-REQ6: Expiry of access rights
    It must be possible to grant access rights with an expiry
    time to a particular watcher or group.

AUTH-REQ7: Presence authorization policy manipulation alignment
           with conferencing
    The solution for authorization policy manipulation should
    be aligned with other data manipulation operations used
    for similar purposes (such as conferencing).

AUTH-REQ8: Authorization of subscriptions generated on behalf
           of another user
    It must be possible for the Presence Server to authorize
    subscriptions to presentityÆs presence information which
    are generated on behalf of another user. It should be
    possible for the presentity to set authorization rules
    taking into account both the identity of the watcher and
    the identity of the user on whose behalf the subscription
    is made.

3.6   Watcher information requirements

WATCHINF-REQ1: Pending watcher notification
    It must be possible for a presentity to be informed of a
    pending watcher subscription from a currently unauthorized
    and/or unknown watcher.

WATCHINF-REQ2: Watcher information filtering
    It must be possible for the presentity to monitor the
    watcher status of certain watchers.
    Note that there are detailed watcher information filtering

requirements listed in [21].

WATCHINF-REQ3: Watcher history
     It must be possible for the presentity to fetch the list
     of the watchers who have accessed (by subscription or
     fetch) his presence information during a well-defined time-
     period (e.g. last 7 days).

3.7   Presencelist requirements

PRLIST-REQ1: Filtering for presentity collection
     It must be possible for the Resource List Server [9] to
     construct and store appropriate filtering rules for every
     URI in the presencelist based on the watcher's filtering
     preferences.

PRLIST-REQ2: Management of presentity collection data element
     Requirements for creating a presentity collection, adding
     new URIs to an existing presentity collection, modifying
     or removing existing URIs from an existing presentity
     collection, or deleting a presentity collection are listed
     in [10].

4.   Security requirements

Presence specifications must not preclude authentication on
behalf of presence entities by other entities within a trust
domain, and communication as defined by RFC 3325 [33].

Security requirements assume requirements that have led to
existing security mechanism described in [18]. Further
security requirements over and above this have not yet been
identified.

5.   Charging Requirements

This document refers to the charging requirements of [19], and
does not list any additional charging requirements at this
time.

6.   Proposal for next steps

It is proposed that SIMPLE Working Group evaluates the
requirements presented in this document and incorporates the
relevant ones in its current work items. Those requirements
possibly falling out of the scope of the SIMPLE WG should find
a more suitable home, possibly also in other standardization
bodies.

It is not expected that this document be published as an RFC by the
IETF, but rather serve as a reference to various working group
requirements documents. It is also expected that this document is
used as a check list as requirements get included to other documents.

Normative References

    1. S. Bradner, "The Internet Standards Process -- Revision 3",
    BCP 9, RFC 2026, October 1996.

    2. S. Bradner, "Key words for use in RFCs to Indicate
    Requirement Levels", BCP 14, RFC 2119, March 1997.

Informative References

    3. J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J.
    Peterson, R. Sparks, M. Handley, E. Schooler: "SIP, Session
    Initiation Protocol", RFC 3261, June 2002

    4. A. Roach, "ession Initiation Protocol (SIP)-Specific Event
    Notification", RFC 3265, June 2002

    5. M. Day, S. Aggarwal, G. Mohr, J. Vincent "Instant Messaging
    / Presence Protocol Requirements", RFC 2779

    6. M. Day, J. Rosenberg, H. Sugano, "A Model for Presence and
    Instant Messaging", RFC 2778

    7. J. Rosenberg et al., "SIP Extensions for Presence", draft-
    ietf-simple-presence-10.txt, January 2003, work in progress

    8. H. Sugano, S. Fujimoto, G. Klyne, A. Bateman: "CPIM
    Presence Information Data Format", draft-ietf-impp-cpim-pidf-
    08.txt, May 2003, work in progress

    9. A. Roach, J. Rosenberg, B. Campbell, "A Session Initiation

Protocol (SIP) Event Notification Extension for Collections",
draft-ietf-simple-event-list-04.txt, June 2003, work in
progress

10. J. Rosenberg, M. Isomaki, "Requirements for Manipulation
of Data Elements in SIMPLE Systems", draft-ietf-simple-data-
req-03.txt, June 2003, work in progress

11. J. Rosenberg, "A Session Initiation Protocol (SIP) Event
Template-Package for Watcher Information", draft-ietf-simple-
winfo-package-05.txt, January 2003, work in progress

12. J. Rosenberg, "An Extensible Markup Language (XML) Based
Format for Watcher Information", draft-ietf-simple-winfo-
format-04.txt, January 2003, work in progress

13. S. Olson, "Requirements for Content Indirection in SIP
Messages", draft-ietf-sipping-content-indirect-03.txt,
February 2003, work in progress

14. E. Leppanen, et al, "Requirements for Presence
specific Event Notification Filtering", draft-ietf-simple-
pres-filter-reqs-02, August 2003, work in progress

15. A. Niemi, et al, "Session Initiation Protocol (SIP)
Extension for Event State Publication", draft-ietf-sip-
publish-00, September 2003, work in progress

16. A. Niemi, "Requirements for Limiting the Rate of Event
Notifications", draft-niemi-sipping-event-throttle-reqs-02,
June 2003, work in progress

17. S. Olson, "A Mechanism for Content Indirection in SIP
Messages", draft-olson-sip-content-indirect-mech-02,
February 2003, work in progress

18. J. Arkko, V. Torvinen, G. Camarillo, T. Haukka, S. Sen,
"Security Mechanism Agreement for SIP Sessions", RFC 3329,
January 2003

19. M. Garcia-Martin, "3rd-Generation Partnership Project
(3GPP) Release 5 requirements on the Session Initiation
Protocol (SIP), draft-ietf-sipping-3gpp-r5-requirements-
00.txt, October 2002, work in progress

20. J. Costa-Requena, E. Leppanen, H. Khartabil, M. Lonnfors, "Partial Notification of Presence Information", draft-ietf-simple-partial-notify-00.txt, September 2003, work in progress

21. K. Kiss, E. Leppanen, H. Khartabil, "Requirements for Filtering of Watcher Information", draft-ietf-simple-winfo-filter-reqs-00.txt, May 2003, work in progress

22. J. Costa-Requena, E. Leppanen, H. Khartabil, M. Lonnfors, "Functional Description of Event Notification Filtering", draft-khartabil-simple-presence-filter-funct-00.txt, May 2003, work in progress

23. B. Campbell, S. Olson, J. Peterson, J. Rosenberg, B. Stucker, "SIMPLE Presence Publication Requirements", draft-ietf-simple-publish-reqs-00, February 2003, work in progress

24. 3GPP TS 23.228 "IP Multimedia Subsystem (IMS) (Stage 2) - Release 5", Version 6.3.0 available at ftp://ftp.3gpp.org/specs/latest/Rel-5/23_series/

25. 3GPP TS 24.228: "Signaling flows for the IP Multimedia call control based on SIP and SDP", Version 5.6.0 available at ftp://ftp.3gpp.org/specs/archive/24_series/24.228/

26. 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP, stage 3", Version 6.0.0 available at ftp://ftp.3gpp.org/specs/archive/24_series/24.229/

27. 3GPP TS 22.141: "Presence Service, Stage 1", Version 6.2.0 available at ftp://ftp.3gpp.org/specs/archive/22_series/22.141/

Krisztian Kiss   3GPP Presence Requirements   October 2003

28. 3GPP TS 23.141: "Presence Service, Architecture and Functional Description, Stage 2", Version 6.4.0 available at ftp://ftp.3gpp.org/specs/archive/23_series/23.141/

29. 3GPP TS 24.841: "Presence service based on Session Initiation Protocol (SIP); Functional models, information flows and protocol details", Version 1.1.0 available at ftp://ftp.3gpp.org/specs/latest-drafts

30. H. Schulzrinne, et al, "RPID -- Rich Presence Information Data Format", draft-ietf-simple-rpid-00.txt, July 2003, work in progress

31. R. Price, C. Bormann, J. Christoffersson, H. Hannu, Z. Liu, J. Rosenberg, "Signaling Compression (SigComp)", RFC 3320, January 2003

32. International Telecommunications Union, "The International Public Telecommunication Numbering Plan", ITU-T Recommendation E.164, 1991.

33. C. Jennings, J. Peterson, M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", RFC 3325, November 2002

34. J. Costa-Requena, E. Leppanen, H. Khartabil, M. Lonnfors, "An Extensible Markup Language (XML) Based Format for Event Notification Filtering", draft-khartabil-simple-presence-format-00.txt, April 2003, work in progress

35. H. Schulzrinne, et al, "CIPID -- Contact Information in Presence Information Data Format", draft-ietf-simple-cipid-00.txt, August 2003, work in progress

36. M. Lonnfors, K. Kiss, "Device capability PIDF status extension", draft-lonnfors-simple-prescaps-ext-02, October 2003, work in progress

37. M. Lonnfors, et al, "Requirements for Efficient Delivery of Presence Information ", draft-ietf-simple-presinfo-deliv-req-00.txt, May 2003, work in progress

Author's address

Krisztian Kiss
Nokia
12278 Scripps Summit Drive
San Diego, CA 92131, USA
Phone: +1 858 2049141
Email: krisztian.kiss@nokia.com

[Appendix A](#). Contributors

The author would like to thank the following people for their interest, support and efforts when writing this Internet-Draft:

>   Gabor Bajko (Nokia), Markus Isomaki (Nokia), Mikko Lonnfors (Nokia), Juha Kalliokulju (Nokia), Eva-Maria Leppanen (Nokia), Georg Mayer (Nokia), Mark Beckmann (Siemens), Sonia Garapaty (Nortel), Jayshree Bharatia (Nortel), Keith Drage (Lucent), Andrew Allen, Kevan Hobbis (3), Alexandre Harmand (O2), Duncan Mills (Vodafone), Miguel A. Garcia (Ericsson), Milo Orsic (Lucent), Hugh Shieh (AWS), Aki Niemi (Nokia).

Although not an official communication of the 3GPP, this document has been discussed and commented by a number of delegates in the relevant 3GPP working groups.

PARTICULAR PURPOSE.

Acknowledgement