INTERNET-DRAFT
Expires: June 9, 2000

Mark Day
Lotus

Sonu Aggarwal
Microsoft

Gordon Mohr
Activerse

Jesse Vincent
Arepa

Instant Messaging / Presence Protocol Requirements
draft-ietf-impp-reqts-04.txt

1. Status of this Memo

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

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.

This document and related documents are discussed on the impp mailing list. To join the list, send mail to impp-request@iastate.edu. To contribute to the discussion, send mail to impp@iastate.edu. The archives are at http://www.imppwg.org/ml_archives.html. The IMPP working group charter, including the current list of group documents, can be found at http://www.ietf.org/html.charters/impp-charter.html.

2. Abstract

Presence and Instant Messaging have recently emerged as a new medium of communications over the Internet. Presence is a means for finding, retrieving, and subscribing to changes in the presence information (e.g. "online" or "offline") of other users. Instant messaging is a means for sending small, simple messages that are delivered immediately to online users.

Applications of presence and instant messaging currently use

independent, non-standard and non-interoperable protocols developed by various vendors. The goal of the Instant Messaging and Presence Protocol (IMPP) Working Group is to define a standard protocol so that independently developed applications of instant messaging and/or presence can interoperate across the Internet. This document defines a minimal set of requirements that IMPP must meet.

3. Contents

1. Status of this Memo
2. Abstract
3. Contents
4. Terminology
5. Shared Requirements
5.1. Namespace and Administration
5.2. Scalability
5.3. Access Control
5.4. Network Topology
5.5. Message Encryption and Authentication
6. Additional Requirements for PRESENCE INFORMATION
6.1. Common Presence Format
6.2. Presence Lookup and Notification
6.3. Presence Caching and Replication
7. Additional Requirements for INSTANT MESSAGES
7.1. Common Message Format
7.2. Reliability
7.3. Performance
7.4. Presence Format
8. Security Considerations
8.1. Requirements related to SUBSCRIPTIONS
8.2. Requirements related to NOTIFICATION
8.3. Requirements related to receiving a NOTIFICATION
8.4. Requirements related to INSTANT MESSAGES
9. References
10. Authors' Addresses
11. Appendix: Security Expectations and Deriving Requirements
11.1. Presence Information
11.1.1. Subscription
11.1.2. Publication
11.1.3. Publication for Notification
11.1.4. Receiving a Notification
11.2. Instant Messaging
11.2.1. Named Instant Messaging
11.2.2. Anonymous Instant Messaging
11.2.3. Administrator Expectations

4. Terminology

The following terms are defined in [Model] and are used with those definitions in this document:

ACCESS RULES
CLOSED
FETCHER
INSTANT INBOX
INSTANT MESSAGE
NOTIFICATION
OPEN
POLLER
PRESENCE INFORMATION
PRESENCE SERVICE
PRESENTITY
PRINCIPAL
PROXY
SERVER
STATUS
SUBSCRIBER
SUBSCRIPTION
WATCHER

The terms MUST and SHOULD are used in the following sense while specifying requirements:

MUST: A proposed solution will have to meet this requirement.
SHOULD: A proposed solution may choose not to meet this requirement.

Note that this usage of MUST and SHOULD differs from that of RFC2119.

Additionally, the following terms are used in this document and defined here:

ADMINISTRATOR: A PRINCIPAL with authority over local computer and network resources, who manages local DOMAINS or FIREWALLS. For security and other purposes, an ADMINISTRATOR often needs or wants to impose restrictions on network usage based on traffic type, content, volume, or endpoints. A PRINCIPAL's ADMINISTRATOR has authority over some or all of that PRINCIPAL's computer and network resources.

DOMAIN: A portion of a NAMESPACE.

ENTITY: Any of PRESENTITY, SUBSCRIBER, FETCHER, POLLER, or WATCHER (all defined in [Model]).

FIREWALL: A point of administrative control over connectivity. Depending on the policies being enforced, parties may need to take unusual measures to establish communications through the FIREWALL.

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 IDENTIFIERS in other systems. Numeric IP addresses like 10.0.0.26 are not, and

neither are URLs containing numerous CGI parameters or long arbitrary identifiers.

INTENDED RECIPIENT: The PRINCIPAL to whom the sender of an INSTANT MESSAGE is sending it.

NAMESPACE: The system that maps from a name of an ENTITY to the concrete implementation of that ENTITY. A NAMESPACE may be composed of a number of distinct DOMAINS.

OUT OF CONTACT: A situation in which some ENTITY and the PRESENCE SERVICE cannot communicate.

SUCCESSFUL DELIVERY: A situation in which an INSTANT MESSAGE was transmitted to an INSTANT INBOX for the INTENDED RECIPIENT, and the INSTANT INBOX acknowledged its receipt. SUCCESSFUL DELIVERY usually also implies that an INBOX USER AGENT has handled the message in a way chosen by the PRINCIPAL. However, SUCCESSFUL DELIVERY does not imply that the message was actually seen by that PRINCIPAL.

5. Shared Requirements

This section describes non-security requirements that are common to both an PRESENCE SERVICE and an INSTANT MESSAGE SERVICE. Section 6 describes requirements specific to a PRESENCE SERVICE, while Section 7 describes requirements specific to an INSTANT MESSAGE SERVICE. Section 8 describes security considerations. The reader should note that Section 11 is an appendix that provides historical context and aids in tracing the origins of requirements in Section 8. Section 11 is not, however, a statement of current IMPP requirements.

It is expected that Presence and Instant Messaging services will be particularly valuable to users over mobile IP wireless access devices. Indeed the number of devices connected to the Internet via wireless means is expected to grow substantially in the coming years. It is not reasonable to assume that separate protocols will be available for the wireless portions of the Internet. In addition, we note that wireless infrastructure is maturing rapidly; the work undertaken by this group should take into account the expected state of the maturity of the technology in the time-frame in which the Presence and Instant Messaging protocols are expected to be deployed.

To this end, the protocols designed by this Working Group must be suitable for operation in a context typically associated with mobile wireless access devices, viz. high latency, low bandwidth and possibly intermittent connectivity (which lead to a desire to minimize round-trip delays), modest computing power, battery constraints, small displays, etc. In particular, the protocols must be designed to be reasonably efficient for small payloads.

5.1. Namespace and Administration

5.1.1. The protocols MUST allow a PRESENCE SERVICE to be available independent of whether an INSTANT MESSAGE SERVICE is available, and vice-versa.

5.1.2. The protocols must not assume that an INSTANT INBOX is necessarily reached by the same IDENTIFIER as that of a PRESENTITY. Specifically, the protocols must assume that some INSTANT INBOXes may have no associated PRESENTITIES, and vice versa.

5.1.3. The protocols MUST also allow an INSTANT INBOX to be reached via the same IDENTIFIER as the IDENTIFIER of some PRESENTITY.

5.1.4. The administration and naming of ENTITIES within a given DOMAIN MUST be able to operate independently of actions in any other DOMAIN.

5.1.5. The protocol MUST allow for an arbitrary number of DOMAINS within the NAMESPACE.

5.2. Scalability

5.2.1. It MUST be possible for ENTITIES in one DOMAIN to interoperate with ENTITIES in another DOMAIN, without the DOMAINS having previously been aware of each other.

The protocol MUST be capable of meeting its other functional and performance requirements even when

-- (5.2.2) there are millions of ENTITIES within a single DOMAIN.

-- (5.2.3) there are millions of DOMAINS within the single NAMESPACE.

-- (5.2.4) every single SUBSCRIBER has SUBSCRIPTIONS to hundreds of PRESENTITIES.

-- (5.2.5) hundreds of distinct SUBSCRIBERS have SUBSCRIPTIONS to a single PRESENTITY.

-- (5.2.6) every single SUBSCRIBER has SUBSCRIPTIONS to PRESENTITIES in hundreds of distinct DOMAINS.

These are protocol design goals; implementations may choose to place lower limits.

5.3. Access Control

The PRINCIPAL controlling a PRESENTITY MUST be able to control

-- (5.3.1) which WATCHERS can observe that PRESENTITY's PRESENCE INFORMATION.

-- (5.3.2) which WATCHERS can have SUBSCRIPTIONS to that PRESENTITY's PRESENCE INFORMATION.

-- (5.3.3) what PRESENCE INFORMATION a particular WATCHER will see for that PRESENTITY, regardless of whether the WATCHER gets it by fetching or NOTIFICATION.

-- (5.3.4) which other PRINCIPALS, if any, can update the PRESENCE INFORMATION of that PRESENTITY.

The PRINCIPAL controlling an INSTANT INBOX MUST be able to control

-- (5.3.5) which other PRINCIPALS, if any, can send INSTANT MESSAGES to that INSTANT INBOX.

-- (5.3.6) which other PRINCIPALS, if any, can read INSTANT MESSAGES from that INSTANT INBOX.

5.3.7. Access control MUST be independent of presence: the PRESENCE SERVICE MUST be able to make access control decisions even when the PRESENTITY is OUT OF CONTACT.

5.4. Network Topology

Note that intermediaries such as PROXIES may be necessitated between IP and non-IP networks, and by an end-user's desire to provide anonymity and hide their IP address.

5.4.1. The protocol MUST allow the creation of a SUBSCRIPTION both directly and via intermediaries, such as PROXIES.

5.4.2. The protocol MUST allow the sending of a NOTIFICATION both directly and via intermediaries, such as PROXIES.

5.4.3. The protocol MUST allow the sending of an INSTANT MESSAGE both directly and via intermediaries, such as PROXIES.

5.4.4. The protocol proxying facilities and transport practices MUST allow ADMINISTRATORS ways to enable and disable protocol activity through existing and commonly-deployed FIREWALLS. The protocol MUST specify how it can be effectively filtered by such FIREWALLS.

5.5. Message Encryption and Authentication

5.5.1. The protocol MUST provide means to ensure confidence that a received message (NOTIFICATION or INSTANT MESSAGE) has not been corrupted or tampered with.

5.5.2. The protocol MUST provide means to ensure confidence that a received message (NOTIFICATION or INSTANT MESSAGE) has not been recorded and played back by an adversary.

5.5.3. The protocol MUST provide means to ensure that a sent message (NOTIFICATION or INSTANT MESSAGE) is only readable by ENTITIES that the sender allows.

5.5.4. The protocol MUST allow any client to use the means to ensure non-corruption, non-playback, and privacy, but the protocol MUST NOT require that all clients use these means at all times.

6. Additional Requirements for PRESENCE INFORMATION

The requirements in section 6 are applicable only to PRESENCE INFORMATION and not to INSTANT MESSAGES. Additional constraints on PRESENCE INFORMATION in a system supporting INSTANT MESSAGES appear in Section 7.4.

6.1. Common Presence Format

6.1.1. All ENTITIES MUST produce and consume at least a common base format for PRESENCE INFORMATION.

6.1.2. The common presence format MUST include a means to uniquely identify the PRESENTITY whose PRESENCE INFORMATION is reported.

6.1.3. The common presence format MUST include a means to encapsulate contact information for the PRESENTITY's PRINCIPAL (if applicable), such as email address, telephone number, postal address, or the like.

6.1.4. There MUST be a means of extending the common presence format to represent additional information not included in the common format, without undermining or rendering invalid the fields of the common format.

6.1.5. The working group must define the extension and registration mechanisms for presence information schema, including new STATUS conditions and new forms for OTHER PRESENCE MARKUP.

6.1.6. The presence format SHOULD be based on IETF standards such as vCard [RFC 2426] if possible.

6.2. Presence Lookup and Notification

6.2.1. A FETCHER MUST be able to fetch a PRESENTITY's PRESENCE INFORMATION even when the PRESENTITY is OUT OF CONTACT.

6.2.2. A SUBSCRIBER MUST be able to request a SUBSCRIPTION to a PRESENTITY's PRESENCE INFORMATION, even when the PRESENTITY is OUT OF CONTACT.

6.2.3. If the PRESENCE SERVICE has SUBSCRIPTIONS for a PRESENTITY's PRESENCE INFORMATION, and that PRESENCE INFORMATION changes, the PRESENCE SERVICE MUST deliver a NOTIFICATION to each SUBSCRIBER,

unless prevented by the PRESENTITY's ACCESS RULES.

6.2.4. The protocol MUST provide a mechanism for detecting when a PRESENTITY or SUBSCRIBER has gone OUT OF CONTACT.

6.2.5. The protocol MUST NOT depend on a PRESENTITY or SUBSCRIBER gracefully telling the service that it will no longer be in communication, since a PRESENTITY or SUBSCRIBER may go OUT OF CONTACT due to unanticipated failures.

6.3. Presence Caching and Replication

6.3.1. The protocol MUST include mechanisms to allow PRESENCE INFORMATION to be cached.

6.3.2. The protocol MUST include mechanisms to allow cached PRESENCE INFORMATION to be updated when the master copy changes.

6.3.3 The protocol caching facilities MUST NOT circumvent established ACCESS RULES or restrict choice of authentication/encryption mechanisms.

6.4 Performance

6.4.1 When a PRESENTITY changes its PRESENCE INFORMATION, any SUBSCRIBER to that information MUST be notified of the changed information rapidly, except when such notification is entirely prevented by ACCESS RULES. This requirement is met if each SUBSCRIBER's NOTIFICATION is transported as rapidly as an INSTANT MESSAGE would be transported to an INSTANT INBOX.

7. Additional Requirements for INSTANT MESSAGES

The requirements in section 7 are applicable only to INSTANT MESSAGES and not to PRESENCE INFORMATION, with the exception of Section **7.4. Section 7.4 describes constraints on PRESENCE INFORMATION that** are relevant only to systems that support both INSTANT MESSAGES and PRESENCE INFORMATION.

7.1. Common Message Format

7.1.1. All ENTITIES sending and receiving INSTANT MESSAGES MUST implement at least a common base format for INSTANT MESSAGES.

7.1.2. The common base format for an INSTANT MESSAGE MUST identify the sender and intended recipient.

7.1.3. The common message format MUST include a return address for the receiver to reply to the sender with another INSTANT MESSAGE.

7.1.4. The common message format SHOULD include standard forms of addresses or contact means for media other than INSTANT

MESSAGES, such as telephone numbers or email addresses.

7.1.5. The common message format MUST permit the encoding and identification of the message payload to allow for non-ASCII or encrypted content.

7.1.6. The protocol must reflect best current practices related to internationalization.

7.1.7. The protocol must reflect best current practices related to accessibility.

7.1.8. The working group MUST define the extension and registration mechanisms for the message format, including new fields and new schemes for INSTANT INBOX ADDRESSES.

7.1.9. The working group MUST determine whether the common message format includes fields for numbering or identifying messages. If there are such fields, the working group MUST define the scope within which such identifiers are unique and the acceptable means of generating such identifiers.

7.1.10. The common message format SHOULD be based on IETF-standard MIME [RFC 2045].

7.2. Reliability

7.2.1. The protocol MUST include mechanisms so that a sender can be informed of the SUCCESSFUL DELIVERY of an INSTANT MESSAGE or reasons for failure. The working group must determine what mechanisms apply when final delivery status is unknown, such as when a message is relayed to non-IMPP systems.

7.3 Performance

7.3.1. The transport of INSTANT MESSAGES MUST be sufficiently rapid to allow for comfortable conversational exchanges of short messages.

7.4 Presence Format

7.4.1. The common presence format MUST define a minimum standard presence schema suitable for INSTANT MESSAGE SERVICES.

7.4.2. When used in a system supporting INSTANT MESSAGES, the common presence format MUST include a means to represent the STATUS conditions OPEN and CLOSED.

7.4.3. The STATUS conditions OPEN and CLOSED may also be applied to messaging or communication modes other than INSTANT MESSAGE SERVICES.

8. Security Considerations

Security considerations are addressed in section 5.3, Access Control, and section 5.5, Message authentication and encryption.

This section describes further security-related requirements that the protocol must meet.

The security requirements were derived from a set of all-encompassing "security expectations" that were then evaluated for practicality and implementability and translated into requirements. In the appendix, we describe the expectations and the process used to transform them into requirements. In this section, we simply list the consolidated set of derived requirements.

Note that in the requirements, ADMINISTRATORs may have privileges beyond those allowed to PRINCIPALs referred to in the requirements. (Unless otherwise noted, the individual expectations specifically refer to PRINCIPALs.) It is up to individual implementations to control administrative access and implement the security privileges of ADMINISTRATORs without compromising the requirements made on PRINCIPALs.

Unless noted otherwise, A,B,C are all names of non-ADMINISTRATOR PRINCIPALS.

8.1. Requirements related to SUBSCRIPTIONS

When A establishes a SUBSCRIPTION to B's PRESENCE INFORMATION:

8.1.1. The protocol MUST provide A means of identifying and authenticating that the PRESENTITY subscribed to is controlled by B.

8.1.2. If A so chooses, the protocol SHOULD NOT make A's SUBSCRIPTION to B obvious to a third party C.

8.1.3. The protocol MUST provide B with means of allowing an unauthenticated subscription by A.

8.1.4. The protocol MUST provide A means of verifying the accurate receipt of the content B chooses to disclose to A.

8.1.5. B MUST inform A if B refuses A's SUBSCRIPTION. Note that B may choose to accept A's SUBSCRIPTION, but fail to deliver any information to it (so-called "polite blocking"). See 8.1.15.

8.1.6. The protocol MUST NOT let any third party C force A to subscribe to B's PRESENCE INFORMATION without A's consent.

8.1.7. A MUST be able to cancel her SUBSCRIPTION to B's PRESENCE INFORMATION at any time and for any reason. When A does so, the PRESENCE SERVICE stops informing A of changes to B's PRESENCE INFORMATION.

8.1.8. The protocol MUST NOT let an unauthorized party C cancel A's SUBSCRIPTION to B.

8.1.9. If A's SUBSCRIPTION to B is cancelled, the service SHOULD inform A of the cancellation.

8.1.10. A SHOULD be able to determine the status of A's SUBSCRIPTION to B, at any time.

8.1.11. The protocol MUST provide B means of learning about A's SUBSCRIPTION to B, both at the time of establishing the SUBSCRIPTION and afterwards.

8.1.12. The protocol MUST provide B means of identifying and authenticating the SUBSCRIBER's PRINCIPAL, A.

8.1.13. It MUST be possible for B to prevent any particular PRINCIPAL from subscribing.

8.1.14. It MUST be possible for B to prevent anonymous PRINCIPALS from subscribing.

8.1.15. It MUST be possible for B to configure the PRESENCE SERVICE to deny A's subscription while appearing to A as if the subscription has been granted (this is sometimes called "polite blocking"). The protocol MUST NOT mandate the PRESENCE SERVICE to service subscriptions that are treated in this manner.

8.1.16. B MUST be able to cancel A's subscription at will.

8.1.17. The protocol MUST NOT require A to reveal A's IP address to B.

8.1.18 The protocol MUST NOT require B to reveal B's IP address to A.

8.2. Requirements related to NOTIFICATION

When a PRINCIPAL B publishes PRESENCE INFORMATION for NOTIFICATION to another PRINCIPAL A:

8.2.1. The protocol MUST provide means of ensuring that only the PRINCIPAL A being sent the NOTIFICATION by B can read the NOTIFICATION.

8.2.2. A should receive all NOTIFICATIONS intended for her.

8.2.3. It MUST be possible for B to prevent A from receiving notifications, even if A is ordinarily permitted to see such notifications. It MUST be possible for B to, at its choosing, notify different subscribers differently, through different notification mechanisms or through publishing different content. This is a variation on "polite blocking".

8.2.4. The protocol MUST provide means of protecting B from another PRINCIPAL C "spoofing" notification messages about B.

8.2.5. The protocol MUST NOT require that A reveal A's IP address to B.

8.2.6. The protocol MUST NOT require that B reveal B's IP address to A.

8.3. Requirements related to receiving a NOTIFICATION

When a PRINCIPAL A receives a notification message from another principal B, conveying PRESENCE INFORMATION,

8.3.1. The protocol MUST provide A means of verifying that the presence information is accurate, as sent by B.

8.3.2. The protocol MUST ensure that A is only sent NOTIFICATIONS from entities she has subscribed to.

8.3.3. The protocol MUST provide A means of verifying that the notification was sent by B.

8.4. Requirements related to INSTANT MESSAGES

When a user A sends an INSTANT MESSAGE M to another user B,

8.4.1. A MUST receive confirmation of non-delivery.

8.4.2. If M is delivered, B MUST receive the message only once.

8.4.3. The protocol MUST provide B means of verifying that A sent the message.

8.4.4. B MUST be able to reply to the message via another instant message.

8.4.5. The protocol MUST NOT always require A to reveal A's IP address, for A to send an instant message.

8.4.6. The protocol MUST provide A means of ensuring that no other PRINCIPAL C can see the content of M.

8.4.7. The protocol MUST provide A means of ensuring that no other PRINCIPAL C can tamper with M, and B means to verify that no tampering has occurred.

8.4.8. B must be able to read M.

8.4.9. The protocol MUST allow A to sign the message, using existing standards for digital signatures.

8.4.10. B MUST be able to prevent A from sending him messages

9. References

[Aggarwal et al., 1998]
S. Aggarwal, M. Day, G. Mohr, "Presence Information Protocol Requirements", Work in progress, draft-aggarwal-pip-reqts-00.txt

[Day, 1998]
M. Day, "Requirements for Presence and Instant Messaging", Work in progress, draft-day-rpim-00.txt

[Model]
M. Day, J. Rosenberg, H. Sagano. "A Model for Presence." Work in progress, draft-ietf-impp-model-02.txt.

[Calsyn & Dusseault, 1998]
M. Calsyn and L. Dusseault. "Presence Information Protocol Requirements", Work in progress, draft-dusseault-pipr-00.txt

[RFC 2426]
F. Dawson and T. Howes. "vCard MIME Directory Profile." RFC 2426, September 1998.

[RFC 2045]
N. Freed and N. Borenstein. "Multipurpose Internet Mail Extensions (MIME) - Part One: Format of Internet Message Bodies." RFC 2045, November 1996.

[RFC 2119]
S. Bradner. "Key Words for Use in RFCs to Indicate Requirement Levels." RFC 2119, March 1997.

10. Authors' Addresses

Mark Day
<mday@alum.mit.edu>
SightPath, Inc.
135 Beaver Street
Waltham, MA 02452
USA
(Formerly Mark_Day@lotus.com)

Sonu Aggarwal
<sonuag@microsoft.com>
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
USA

Gordon Mohr
<gojomo@usa.net>
(Formerly gojomo@activerse.com>

Jesse Vincent
<jesse@arepa.com>
Arepa, Inc.
100 Cambridgepark Drive
Cambridge, MA 02140
USA
(Formerly jvincent@microsoft.com)

11. Appendix: Security Expectations and Deriving Requirements

This appendix is based on the security expectations discussed on the impp mailing list and assembled by Jesse Vincent. The original form of numbering has been preserved in this appendix (so there are several different items labeled B1, for example). The derived requirements have new numbers that are consistent with the main body of the document. This appendix is included to provide a connection from discussions on the list to the requirements of Section 8, but it is not intended to introduce any new requirements beyond those presented in Sections 5 through 8.

11.1. PRESENCE INFORMATION

In the case of PRESENCE INFORMATION, the controlling PRINCIPAL's privacy interests are paramount; we agreed that "polite blocking" (denying without saying that the subscription is denied, or providing false information) should be possible.

11.1.1. Subscription

When a user Alice subscribes to another person, Bob's presence info, Alice expects:

A1. the PRESENTITY's PRINCIPAL, B, is identifiable and authenticated

> Discussion: Stands as a requirement. Note that the protocol should provide Alice the capability of authenticating, without requiring that Alice authenticate every SUBSCRIPTION. This caveat is made necessary by performance concerns, among others, and applies to many of the other requirements derived below. [Requirement 8.1.1]

A2. no third party will know that A has subscribed to B.

> Discussion: This is somewhat unreasonable to enforce as is. For example, in some topologies, nothing can prevent someone doing traffic analysis to deduce that A has subscribed to B. We should merely require that the protocol not expose subscription information in any obvious manner. [Requirement 8.1.2]

A3. A has the capability to subscribe to B's presence without B's knowledge, if B permits anonymous subscriptions.

> Discussion: An "anonymous subscription" above can have two

implications - (i) B may allow an unauthenticated subscription by A, and (ii) B may be unaware of A's stated identity. Requirement (i) is reasonable [Requirement 8.1.3], but (ii) doesn't appear to be a core requirement -- it can be adequately simulated via a subscription pseudonym.

A4. A will accurately receive what B chooses to disclose to A regarding B's presence.

Discussion: Stands as a requirement, with the "optional" caveat. [Requirement 8.1.4]

A5. B will inform A if B refuses A's subscription

Discussion: Stands as a requirement. [Requirement 8.1.5]

A6. No third party, C can force A to subscribe to B's presence without A's consent.

Discussion: Stands as a requirement. [Requirement 8.1.6]

A7. A can cancel her subscription to B's presence at any time and for any reason. When A does so, she will receive no further information about B's presence information.

Discussion: This essentially stands. However, implementations may have to contend with a timing window where A receives, after sending her cancellation request, a notification sent by B before B received the cancellation request. Therefore, the requirement should focus on B's ceasing to send presence information, rather than A's ceasing to receive it. [Requirement 8.1.7]

A8. no third party, C, can cancel A's subscription to B.

Discussion: Stands, although the administrative exception does apply. [Requirement 8.1.8]

A9. A is notified if her subscription to B is cancelled for any reason.

Discussion: Although the intent is reasonable, there are a number of scenarios (e.g. overburdened server, clogged network, server crash) where delivering a notification to A of the cancellation is undesirable or impossible. Therefore, the service should make an attempt to inform, but this is not required. [Requirement 8.1.9]

Bob expects:

B1. B will be informed that A subscribed to B's presence information, as long as A has not subscribed anonymously.

Discussion: This essentially stands. However, B can also choose to determine A's subscription after the fact. [Requirement 8.1.10]

B2. A is identifiable and authenticated.

Discussion: This stands as a requirement. [Requirement 8.1.11]

B3. B can prevent a particular user, D, from subscribing.

Discussion: This stands as a requirement. [Requirement 8.1.12]

B4. B can prevent anonymous users from subscribing.

Discussion: This stands as a requirement. [Requirement 8.1.13]

B5. B's presence information is not republished by A to a third party, E, who does not.

Discussion: This is practically impossible to enforce, so it is omitted from the requirement set.

B6. B can deny A's subscription without letting A know that she's been blocked.

Discussion: This "polite blocking" capability essentially stands; accepting a "denied" subscription should bear no implication on servicing it for status notifications. [Requirement 8.1.14]

B7. B can cancel A's subscription at will.

Discussion: Stands as a requirement. [Requirement 8.1.15]

Charlie, bob's network administrator expects:

C1. C knows who is subscribed to B at all times.

Discussion: Administrators should be able to determine who is subscribed, but needn't be continuously informed of the list of subscribers. Also, in some cases user agents (e.g. proxies) may have subscribed on behalf of users, and in these cases the administrator can only determine the identity of these agents, not their users. [Requirement 8.1.16]

C2. C can manage all aspects of A's presence information.

Discussion: This stands as a requirement. [Requirement 8.1.17]

C3. C can control who can access A's presence information and exchange instant messages with A.

Discussion: This stands in principle, but C should be able to waive these capabilities if C desires. [Requirement 8.1.18]

11.1.2. Publication

The publisher of status information, Bob, expects:

B1. That information about B is not provided to any entity without B's knowledge and consent.

Discussion: This is nearly impossible to accomplish, so it is omitted from the requirements.

11.1.3. Publication for Notification

When information is published for notification, B expects:

B1. only a person being sent a notification, A, can read the notification.

Discussion: Stands as a requirement. [Requirement 8.2.1]

B2. A reliably receives all notifications intended for her.

Discussion: This stands, although "Reliably" is a little strong (e.g. network outages, etc.). [Requirement 8.2.2]

B3. B can prevent A from receiving notifications, even if A is ordinarily permitted to see such notifications. This is a variation on "polite blocking."

Discussion: This stands as a requirement. Also incorporated into this requirement is the notifications equivalent of the next expectation, B4. [Requirement 8.2.3]

B4. B can provide two interested parties A and E with different status information at the same time. (B could represent the same event differently to different people.)

Discussion: This stands as a requirement; it has been incorporated into the corresponding requirement for B3 above.

B5. B expects that malicious C cannot spoof notification messages about B.

Discussion: Stands in principle, but it should be optional for B. [Requirement 8.2.4]

11.1.4. Receiving a Notification

When Alice receives a notification, the recipient, Alice, expects:

A1. That the notification information is accurate, truthful.

Discussion: Stands in principle, although being "truthful" can't be a requirement, and the verification is optional for Alice. [Requirement 8.3.1]

A2. That information about subscriptions remains private; people do not learn that A's subscription to B's information exists by watching notifications occur.

Discussion: This is omitted from the requirements, as traffic analysis, even of encrypted traffic, can convey this information in some situations.

A3. That she only receives notifications of things she's subscribed to.

Discussion: Stands as a requirement. [Requirement 8.3.2]

A4. Notifications come from the apparent sender, B.

Discussion: Stands in principle, although the verification should be optional for A. [Requirement 8.3.3]

A5. A can tell the difference between a message generated by the user, and a message legitimately generated by the agent on behalf of the user.

Discussion: This could be quite difficult to enforce and could unduly restrict usage scenarios; this is omitted from the requirements.

A6. That information given by agents on behalf of users can also be expected to be truthful, complete, and legitimately offered; the user permitted the agent to publish these notifications.

Discussion: This is difficult to enforce and is omitted from the requirements.

A7. A can prove that a notification from B was delivered in a timely fashion and can prove exactly how long the message took to be delivered.

Discussion: This is difficult to enforce and is omitted from the requirements. For example, such proof may entail global time synchronization mechanisms (since any system clocks have associated unreliability), which is outside the scope of this effort.

A8. A can prove that B was indeed the sender of a given message.

Discussion: This is a duplication of expectation A4 above and is reflected in the corresponding requirement 8.3.3.

11.2. INSTANT MESSAGEs

11.2.1. Named Instant Messaging

When a user Alice sends an instant message M to another user Bob:

Alice expects that she:

A1. will receive notification of non-delivery

    Discussion: Stands as a requirement. [Requirement 8.4.1]

Alice expects that Bob:

B1. will receive the message

    Discussion: covered by A1 and is reflected in the corresponding requirement 8.4.1.

B2. will receive the message quickly

    Discussion: Stands as a requirement, although this is also covered elsewhere (in the non-security requirements), so this is omitted from the security requirements.

B3. will receive the message only once

    Discussion: Stands as a requirement. [Requirement 8.4.2]

B4. will be able to verify that Alice sent the message

    Discussion: Stands as a requirement. [Requirement 8.4.3]

B5. will not know whether there were BCCs

    Discussion: Emulating e-mail conventions and social protocols is not a core goal of this effort, and therefore references to standard mail fields are omitted from the requirements.

B6. will be able to reply to the message

    Discussion: Stands in principle; the recipient should be able to reply via an instant message. [Requirement 8.4.4]

B7. will know if he was a bcc recipient

    Discussion: Omitted, as noted above.

B8. will not be able to determine any information about A (such as her location or IP address) without A's knowledge and consent.

    Discussion: "Any information about A" is too general; the requirement should focus on IP address. Further, "without A's knowledge and consent" may be overkill. [Requirement 8.4.5]

Alice expects that no other user Charlie will be able to:

C1. see the content of M

Discussion: Stands in principle, although this should not be mandated for all IM communication. [Requirement 8.4.6]

C2. tamper with M

Discussion: Stands, with the same caveat as above. [Requirement 8.4.7]

C3. know that M was sent

Discussion: It is impossible to prevent traffic analysis, and this is therefore omitted from the requirements.

When a user Bob receives an instant message M from another user Alice:

Bob expects that Bob:

D1. will be able to read M

Discussion: Stands as a requirement. [Requirement 8.4.8]

D2. will be able to verify M's authenticity (both Temporal and the sender's identity)

Discussion: As noted earlier, it is not reasonable to directly require temporal checks. The protocol should, however, allow signing messages using existing standards for signing. [Requirement 8.4.9]

D3. will be able to verify M's integrity

Discussion: Stands as a requirement. [Requirement 8.4.10]

D4. will be able to prevent A from sending him future messages

Discussion: Stands as a requirement. [Requirement 8.4.11]

Bob expects that Alice:

E1. intended to send the message to Bob

Discussion: This is covered by the corresponding requirement 8.4.6 for C1 above.

E2. informed Bob of all CCs.

Discussion: As noted earlier, references to cc:'s are omitted from the requirements.

11.2.2. Anonymous Instant Messaging

Discussion: Anonymous instant messaging, as in "hiding the identity

of the sender", is not deemed to be a core requirement of the protocol and references to it are therefore omitted from the requirements. Implementations may provide facilities for anonymous messaging if they wish, in ways that are consistent with the other requirements.

When a user Alice sends an anonymous instant message to another user Bob:

Alice expects that Bob:

B1. will receive the message

B2. will receive the message quickly

B3. will receive the message only once

AB4.1. cannot know Alice sent it

AB4.2. will know that the IM is anonymous, and not from a specific named user

AB4.3 may not allow anonymous IMs

B5. will not know whether there were BCCs

B6. will be able to reply to the message

Alice expects that she:

C1. will receive notification of non-delivery

AC2. will receive an error if the IM was refused

Bob expects that he:

D1. will be able to read M

D2. will be able to verify M's authenticity (both temporal and the sender's identity)

D3. will be able to verify M's integrity

AD4. will know if an IM was sent anonymously

AD5. will be able to automatically discard anonymous IM if desired

AD6. will be able to control whether an error is sent to Alice if M is discarded.

11.2.3. Administrator Expectations

Charlie, Alice's network administrator expects:

C1. that C will be able to send A instant messages at any time.

C2. that A will receive any message he sends while A is online.

C3. that A will not be able to refuse delivery of any instant messages sent by C.

> Discussion for C1-C3: It is not clear this needs to be specially handled at the protocol level; Administrators may accomplish the above objectives through other means. For example, an administrator may send a message to a user through the normal mechanisms. This is therefore omitted from the requirements.