Network Working Group
Internet-Draft
Expires: December 25, 2002

B. Campbell
J. Rosenberg
dynamicsoft
June 26, 2002

CPIM Mapping of SIMPLE Presence and Instant Messaging
draft-ietf-simple-cpim-mapping-01

Abstract

The SIMPLE work group has defined a SIP events package for distribution of presence information. It has also proposed a MESSAGE extension for the transport of instant messages. This document describes how those mechanisms map to the abstract CPIM service, in order to interoperate with other CPIM compliant presence and instant messaging services.

Table of Contents

1. Introduction

Common Presence and Instant Messaging (CPIM) [2] describes the semantics of an abstract presence and instant messaging service. Concrete service protocols, such as SIMPLE, that conform to the CPIM should be able to interoperate with each other using CPIM compliant gateways.

The SIMPLE work group designed SIP [1] based protocols for the distribution of instant messages and presence documents. Presence [3] may be distributed using a SIP event [5] package. Instant Messages may be transferred using the MESSAGE [4] method extension to SIP.

This document describes how the SIMPLE presence and instant message mechanisms map to the abstract CPIM service.

2. The CPIM Abstract Gateway Service

A SIMPLE based service may interoperate with other CPIM compliant services through the use of a gateway. This document describes a gateway to an abstract CPIM service. In any actual implementation, this gateway would convert SIMPLE to some other concrete protocol. As long as that protocol also maps to CPIM, the gateway semantics will be the same.

For the purposes of this document, we show the CPIM abstract gateway as handling both presence and instant messages. In a concrete implementation this may or not be true--a single gateway might handle both, or there might be a separate gateway for each service.

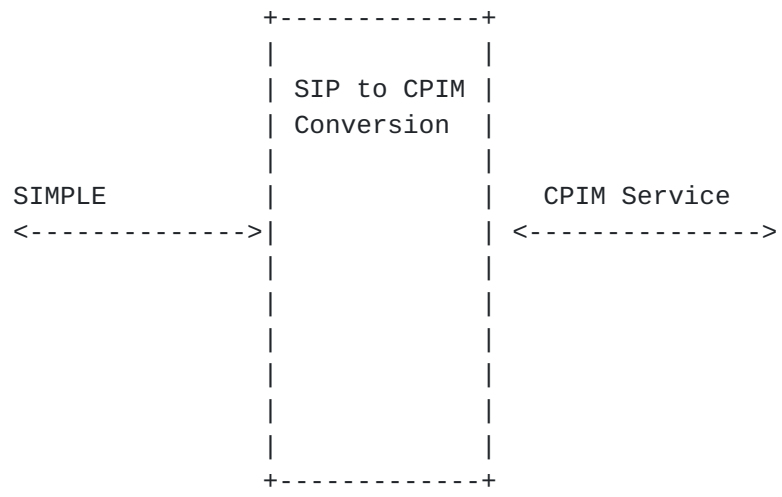

Figure 1: CPIM Abstract Gateway

3. Mapping SIMPLE Presence to CPIM

This section defines how a SIP SUBSCRIBE and NOTIFY requests may be converted to CPIM, and how CPIM messages are converted to SIP for presence. SIP to CPIM conversion occurs when a SIP system sends a SUBSCRIBE request that contains a pres URL or SIP URL that corresponds to a user in a domain that runs a different presence protocol. CPIM to SIP involves the case where a user in a different protocol domain generates a subscription that is destined for a user in a SIP domain.

Note that the process defined below requires that the gateway store both transaction and subscription state. The transaction state is needed to map the SIP transaction identifiers to the CPIM transID value. Subscription state is needed to store the SIP dialog information associated with the subscription.

From the SIP perspective, the CPIM gateway is an endpoint, that is, it is the terminating point for the SIP transactions and dialogs. The gateway can be thought of as a b2bua, except that the opposite

side implements the abstract CPIM service (or some concrete CPIM compliant service.)

3.1 Mapping SUBSCRIBE reqests to CPIM

The SUBSCRIBE process begins when the CPIM gateway receives a SIP SUBSCRIBE requests. First, the gateway MUST determine if the request is an initial request or a mid-dialog request. If it is a mid-dialog request, the gateway MUST treat it as a refresh. Note that since CPIM does not allow duplicate subscriptions. the gateway MUST reject any new SUBSCRIBE request that would result in watcher and target identies that match an existing subscription with a 486 response.

Otherwise, the The gateway generates a corresponding CPIM subscription request message in the following fashion:

- Copy the watcher identity from the SIP From header.If the From header contains a SIP URL, the gateway converts it to a presence URL. This mapping is based on the local policy or the gateway.

- Copy the Request-URI from the SUBSCRIBE request to the target value of the CPIM message. This URL may also require conversion to the "pres" scheme.

- Copy the Expires header from the SUBSCRIBE request to the duration parameter in the CPIM message. If the SUBSCRIBE request does not contain an Expires header, choose a value based on local policy. If there is no policy to the contrary, this value SHOULD be one hour.

- Construct the transID parameter by determining the SIP transaction identity as described in RFC3261 [1] and choosing a transID value that maps uniquely to the SIP transaction identity. How this mapping is achieved is a matter of gateway local policy.

The CPIM service then a "success", "failure", or "indeterminate" response. If the CPIM gateway can determine immediately (that is, quickly enough to avoid retransmissions on the part of the requestor) that a subscription is sucessful, it returns a 200 response. If it can immediately determine the request is unsuccessful, it generates a 603 response. If the result is indeterminate, or cannot be determined immediately, the gateway sends a 202 response.

In the event of a successful response, the gateway copies the

duration value into an Expires header of the SIP response. The gateway adds a Contact header to the SIP response which contains the target identity.

If the subscription was successful or indeterminant, the gateway MUST establish subscription state. This state maps the SIP dialog to the combination of CPIM watcher and target identities.

When the CPIM system generates a notification request, the gateway first checks that the target and watcher values match an existing subscription. If no match exists, the gateway ignores the request. If a match does exist, the gateway constructs and sends a SIP NOTIFY request according standard procedures for mid-dialog requests. In additon, the gateway populates the request in the following manner:

- Copy the watcher identity to the From header.

- Copy the target identity to the To header. (The Request-URI comes from the Contact header in the original subscribe.)

- Copies the presence information into the body of the NOTIFY request.

CPIM has no concept of responses to notifications, so for the most part the gateway simply consumes responses to SIP NOTIFY requests. However, if such a response indicates a failure of the NOTIFY request, the gateway SHOULD cease forwarding future NOTIFY requests from the CPIM service for the associated subscription. If the NOTIFY response was a 481, then the gateway MUST cease sending notifies for the associated subscription. If the gateway ceases forwarding of notifications on a subscription, it SHOULD initiate an unsubscribe request to the CPIM service.

The gateway handles subscription request refreshes simularly to initial subscription requests, except that the gateway will already have dialog state stored for the subscription.

The gateway handles an unsubscribe request, that is, a SIP SUBSCRIBE request with an Expires of zero, in exactly the same manner as a subscription refresh. This will result in a CPIM subscribe request with a duration or zero, which results in the removal of the subscription.

The CPIM response to the unsubscribe attempt is either success or failure. In the case of success, the gateway returns a SIP 2XX class

response. In the case of failure, the gateway returns a 6XX class response. The responses are constructed in the same manner as above. The gateway should remove any subscription state, if present.

3.2 Mapping CPIM subscriptions to SIP

The gateway maps CPIM subscriptions to SIP when a CPIM subscription request arrives at the gateway.

The gateway coverts the subscription request into a SIP SUBSCRIBE request. The gateway determines if this request is for an existing subsciption by comparing the target and watcher to those of existing subscriptions. If the there is a match, the request is for the refresh of an existing subscription.

For a new subscription, the gateway constructs a SUBSCRIBE request in the following manner:

- Set the From header to the watcher value of the CPIM request. This may require mapping of presence URIs to SIP URIs, based on the local policy of the gateway.

- Set the To header and the Request-URI to the target value of the CPIM request. This may require mapping of presence URIs to SIP URIs, based on the local policy of the gateway.

- Set the Expires header to the duration value from the CPIM request.

The gateway then sends the SUBSCRIBE request following normal SIP rules.

For a subscription refresh, the gateway determines the subscription dialog that matches the target and watcher in the CPIM request. It generates the SIP SUBSCRIBE request in much the same manner as for a new subscription, except that it must follow the normal SIP rules for a mid-dialog request.

When the gateway receives the SIP response, it constructs a response to the CPIM system in the following manner:

- Copy the Expires header to the duration value.

- Determine the transID from the stored transaction state.

o For a 202 response, make the status "indeterminate." For any other 2XX class response, make the status "success." For any non-2XX class final response, make the status "failure."

If the subscription was successful, the gateway MUST establish subscription state. This state maps the SIP dialog identifying information to the combination of CPIM watcher and target identities.

If the gateway receives an unsubscribe request from the CPIM service, it checks whether the subscription state exists based on the target and watcher value. If the subscription does exist, the gateway constructs a SUBSCRIBE request as described above, but with an Expires header of zero. If the subscription did not exist, the gateway returns a failure response to the CPIM service.

When the gateway receives a SIP NOTIFY request, it first determines if the request matches an existing dialog. If not, it returns a 481 response. If the request matches an existing subscription dialog, the gateway constructs a CPIM notification request in the following fashion:

o Set the watcher value to the Request-URI.

o Set the target to the URI in the From header.

o Generate a transID that maps uniquely to the SIP transaction.

The gateway then generates a 200 OK response to the NOTIFY request. Note that the CPIM service does not send a response to a notification request. The gateway SHOULD treat all notifies that match an existing dialog as successful.

Note that a SIP NOTIFY can indicate the subscription has been terminated, by the inclusing of a Subscription-State header value of "terminated." CPIM has no similar concept. Therefore the gateway has no mechanism by which it can inform the CPIM service that a subscription has been terminated early.

If early termination occurs, the gateway MAY choose to simply drop state for the subscription. It MAY generate a NOTIFY request containing a presence body indicating that the current presence state of the presentity is no longer known (the mechanism for which is out of scope for this document). It MAY choose to generate a new SIP SUBSCRIBE request.

4. CPIM Mapping for Instant Messages

This section describes how the gateway may map instant messages between a SIP-based service and a CPIM service. The mapping of IMs is much simpler than presence, due to the fact that IMs do not initiate a SIP dialog.

4.1 Mapping SIP MESSAGE requests to CPIM

When the gateway receives a SIP MESSAGE request, it generates a CPIM message operation in the following manner:

- Create the source identity based on the sender's credentials or From header in the case of an unauthenticated message. However, the gateway SHOULD authenticate the MESSAGE request. If the request is authenticated, the source identity MUST be the authenticated credentials. If the sender's identity is not authenticated, then the gateway SHOULD indicate that fact in a display-name or comment section of the source parameter. Note that this may require converting the URL scheme from "sip:" to "im:", based on the local policy of the gateway.

- Copy the Request-URI to the destination parameter. Note that this may also require URL conversion.

- Generate a transID value, maintaining sufficient local transaction state to associate the CPIM response with the SIP request.

- Copy the body from the SIP MESSAGE request into the body of the CPIM message. If the body has a MIME type of message/cpim, it MUST be sent unchanged, to allow for end-to-end encryption and signatures of message/cpim bodies. Any other type MUST be imbedded into a message/cpim body part.

If the CPIM service responds with a "success", the gateway SHOULD generate a 200 response. If the CPIM service responds with "failure", the gateway SHOULD return a 603 response. If the gateway has a local policy to neither confirm or deny delivery of IMs, it MAY return a 202 to all requests. If the gateway UAS cannot determine the results of the message operation in a short enough time to avoid a SIP transaction timeout, it MUST return a 202 accepted response.

4.2 Mapping CPIM operations to SIP

When a gateway maps a CPIM message operation to SIP, it generates a

SIP MESSAGE request according to the following procedure:

- Copy the destination identity to the Request-URI and the To header, converting the URL schemes if required.

- Copy the CPIM body into the SIP body unchanged.

- Create the SIP dialog identifying information so that it uniquely maps to transID. The method for this mapping is a matter of local implementation.

- Establish local transaction state.

When the gateway receives a final response to the SIP request, it generates the CPIM response in the following manner:

- If the response was a 202, set the status to "indeterminate".

- If the response was any other 2XX class response, set the status to "success."

- If the response was any 4XX,5XX,or 6XX class response, set the status to "failure."

- Determine the transID from local transaction state.

5. Security Considerations

End-to-end security concerns for instant messaging were a primary driving force behind the creation of message/cpim. Application designers needing end-to-end security should study that work carefully. In all cases, gateways MUST NOT modify a message/cpim body part in any way.

There are several cases in this document where a gateway determines an IM source or watcher identity from a SIP message. While in some cases, the From header is the only source of such information, the From header is not the best choice. In general, gateways SHOULD authenticate the sender's identity in some manner. The nature of this authentication is beyond the scope of this document. If the gateway authenticates the sender's identity, it MUST determine the

source or watcher from the authenticated credentials instead of the From header.

6. Acknowledgments

The authors would like to thank the following people for their help in the creation of this document.

Adam Roach dynamicsoft
Robert Sparks dynamicsoft
and
All authors of the SIMPLE presence and IM drafts

References

[1] Rosenberg, J. and H. Schulzrinne, "SIP: Session Initiation Protocol", RFC 3261, February 2002.

[2] Crocker, D., Diacakis, A., Mazzoldi, F., Huitema, C., Klyne, G., Rose, M., Rosenberg, J., Sparks, R. and H. Sugano, "A Common Profile for Instant Messaging (CPIM)", draft-ietf-impp-cpim-02 (work in progress), November 2001.

[3] Rosenberg, et al, J., "SIP Extensions for Presence", draft-ietf-simple-presence-07 (work in progress), May 2002.

[4] Campbell, B. and J. Rosenberg, "SIP Extensions for Instant Messaging", draft-ietf-sip-message-05 (work in progress), June 2002.

[5] Roach, A., "SIP-Specific Event Notification", RFC 3265, February 2002.

Authors' Addresses

Ben Campbell
dynamicsoft
5100 Tennyson Parkway
Suite 1200
Plano, TX 75024

EMail: bcampbell@dynamicsoft.com

Jonathan Rosenberg
dynamicsoft
72 Eagle Rock Avenue
First Floor
East Hanover, NJ 07936

EMail: jdrosen@dynamicsoft.com

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.