SIPPING WG
Internet-Draft
Updates: RFC 3325
(if approved)
Intended status: Informational
Expires: August 17, 2008

J. Elwell
Siemens Enterprise Communications
GmbH & Co KG
February 14, 2008

Updates to Asserted Identity in the Session Initiation Protocol (SIP) draft-ietf-sipping-update-pai-00.txt

Status of this Memo

Copyright Notice

Abstract

SIP has a mechanism for conveying the asserted identity of the originator of a request by means of the P-Asserted-Identity header field. This header field is specified for use in requests using a number of SIP methods, in particular the INVITE method. However, RFC 3325 does not specify the insertion of this header field by a trusted UAC, does not specify the use of this header field with the SIP

UPDATE, MESSAGE or PUBLISH methods, and is unclear on the use of this header field in responses. This document extends RFC 3325 to cover these situations.

This work is being discussed on the sipping@ietf.org mailing list.

Table of Contents

1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Introduction

SIP [RFC3261] has a mechanism for conveying within a Trust Domain the asserted identity of the originator of a request by means of the P-Asserted-Identity header field [RFC3325]. This header field is specified for use in requests using a number of SIP methods, in particular the INVITE method. However, RFC 3325 does not specify the insertion of this header field by a UAC in the same Trust Domain as the first proxy.

Also RFC 3325 does not specify the use of the P-Asserted-Identity header field with the SIP UPDATE method [RFC3311], the SIP MESSAGE method [RFC3428] or the SIP PUBLISH method [RFC3903], and is unclear on the use of this header field in responses. There are similar omissions concerning the P-Preferred-Identity header field.

This document extends RFC 3325 by allowing inclusion of the P-Asserted-Identity header field by a UAC in the same Trust Domain as the first proxy, allowing use of this header field in UPDATE, MESSAGE and PUBLISH requests and, under certain conditions, allowing use of this header field in SIP responses. It also allows the use of the P-Preferred-Identity header field in some of these situations.

OPEN ISSUE 1: Should we allow use of PAI in REGISTER requests (between an authenticating edge proxy and the registrar)?

OPEN ISSUE 2: Should we allow use of PAI in all mid-dialog requests (including PRACK, INFO, BYE etc.) rather than just UPDATE? The present motivation in this document is that an identity may change mid-dialog, and although the new identity can at present be conveyed in a re-INVITE request, this needs extending to UPDATE requests. I don't think any other method would need to be used to convey a new identity mid-dialog. Therefore the only motivation for extending to all mid-dialog requests is to provide an explicit assertion that the source of each request has been authenticated.

3. Discussion

3.1. Inclusion of P-Asserted-Identity by a UAC

RFC 3325 does not include procedures for a UAC to include the P-Asserted-Identity header field in a request. This can be meaningful if the UAC is in the same Trust Domain as the first proxy. Examples of types of UAC that are often suitable for inclusion in a Trust Domain are:

- PSTN gateways;
- media servers;
- application servers (or B2BUAs) that act as URI list servers [I-D.ietf-sipping-uri-services];
- application servers (or B2BUAs) that perform third party call control.

In the particular case of a PSTN gateway, the PSTN gateway might be able to assert an identity received from the PSTN, the proxy itself having no means to authenticate such an identity. Likewise, in the case of certain application server or B2BUA arrangements, the application server or B2BUA may be in a position to assert an identity of a user on the other side of that application server or B2BUA.

In accordance with RFC 3325, nodes within a Trust Domain must be connected using TLS with a certain cipher suite, and this principle needs to apply to the connection between a UAC and its proxy as part of the condition for considering the UAC to be within the same Trust Domain. Normal proxy procedures of RFC 3325 ensure that the header field is removed or replaced if the first proxy considers the UAC to be outside the Trust Domain.

3.2. Inclusion of P-Asserted-Identity in an UPDATE request

There are several use cases that would benefit from the use of the P-Asserted-Identity header field in an UPDATE request. These use cases apply within a Trust Domain where the use of asserted identity is appropriate (see RFC 3325).

In one example, an established call passes through a gateway to the PSTN. The gateway becomes aware that the remote party in the PSTN has changed, e.g., due to call transfer. By including the P-Asserted-Identity header field in an UPDATE request, the gateway can convey the identity of the new remote party to the peer SIP UA.

Note that the (re-)INVITE method could be used in this situation. However, this forces an offer-answer exchange, which typically is not required in this situation. Also it involves 3 messages rather than 2.

In another example, a B2BUA that provides third party call control (3PCC) wishes to join two calls together, one of which is still waiting to be answered and potentially is forked to different UAs. At this point in time it is not possible to trigger the normal offer-answer exchange between the two joined parties, because of the mismatch between a single dialog on the one side and potentially multiple early dialogs on the other side, so this action must wait until one of the called UAs answers. However, it would be useful to give an early indication to each user concerned of the identity of the user to which they will become connected when the call is answered. This can be achieved by the B2BUA sending an UPDATE request with a P-Asserted-Identity header field on the dialogs concerned.

OPEN ISSUE 3: Are there any use cases that justify the use of P-Preferred-Identity in an UPDATE request?

3.3. Inclusion of P-Asserted-Identity or P-Preferred-Identity in a MESSAGE request

Within a Trust Domain, a P-Asserted-Identity header field could advantageously be used in a MESSAGE request to assert the source of a page mode instant message. This would complement its use in an INVITE request to assert the source of an instant message session or any other form of session. Similarly, between a UAC and first proxy that are not within the same Trust Domain, a P-Preferred-Identity header field could be used in a MESSAGE request to express a preference when the user has several identities.

3.4. Inclusion of P-Asserted-Identity or P-Preferred-Identity in a PUBLISH request

Within a Trust Domain, a P-Asserted-Identity header field could advantageously be used in a PUBLISH request to assert the source of published state information. This would complement its use in SUBSCRIBE and NOTIFY requests. Similarly, between a UAC and first proxy that are not within the same Trust Domain, a P-Preferred-Identity header field could be used in a PUBLISH request to express a preference when the user has several identities.

3.5. Inclusion of P-Asserted-Identity or P-Preferred-Identity in a response

There are cases where the inclusion of the P-Asserted-Identity header field in responses would be useful. Retargeting of a request can result in the responding entity having a different identity from that placed in the To URI of the request. Inclusion of asserted identity in a response would provide the UAC with the identity of the sender. Some examples of the benefits to be gained include:

- Asserted identity in a 2xx response to an INVITE request would indicate the identity of the connected user.
- Asserted identity in a provisional response to an INVITE request would indicate the contacted (e.g., alerted) user.
- Asserted identity in a 2xx response to a MESSAGE request would give provide confirmation of where the message was delivered to.
- Asserted identity in certain 4xx/5xx/6xx responses would provide an indication of where the response originated.

In the case of a request that results in the formation of a dialog, a mid-dialog request (e.g., UPDATE) in the reverse direction can provide the identity of the user at the destination end of that dialog, and therefore the need to include asserted identity in a response to the dialog-forming request is debatable. There can be some benefits in terms of ease of interworking with PSTN, where such information is placed in the response to a call establishment request. For other responses, including successful responses to requests such as MESSAGE and PUBLISH and unsuccessful responses, the use of a request in the reverse direction is unsuitable.

RFC 3325 is ambiguous on inclusion of P-Asserted-Identity in a response. For example, section 4 of RFC 3325 talks about inclusion of the header field in messages, as opposed to requests. Moreover section 5 explicitly mentions "message (request or response)". However, there are other places (e.g., sections 6, 7 and 8) that talk only about requests.

Section 5 of RFC 3325 requires a proxy to authenticate the originator of a message before adding a P-Asserted-Identity header field to the forwarded message. In practice there is no SIP means to authenticate the sender of a SIP response message. However, authentication may be possible by other means. For example, if the proxy has TLS connectivity with the originator of the response and has previously authenticated the connected entity (e.g., using SIP digest authentication at registration time), then the originator of the

response can be considered to be authenticated. In such circumstances it is permissible for a proxy to insert a P-Asserted-Identity header field in a SIP response.

OPEN ISSUE 4: It has been suggested that we must be precise (at least in the normative section) as to the conditions under which a proxy may assert an identity in the response. One approach would be to say that the only acceptable condition is that given above as an example. Are there any other acceptable conditions?

It should also be permissible for a UAS to insert a P-Asserted-Identity header field into a response if it is within the same Trust Domain as the proxy from which the request was received (the last proxy).

Between a UAS and last proxy that are not within the same Trust Domain, a P-Preferred-Identity header field could be used in a response, in order to express a preference when the authenticated user has several identities.

4. Behaviour

This updates RFC 3325 by allowing a P-Asserted-Identity header field to be included by a UAC within the same Trust Domain, by allowing a P-Asserted-Identity header field to appear in an UPDATE, MESSAGE or PUBLISH request, and by allowing a P-Asserted-Identity header field to appear in a response in certain circumstances. It also allows a P-Preferred-Identity header field to appear in a MESSAGE or PUBLISH request or in a response.

4.1. UAC Behaviour

4.1.1. Request handling

A UAC MAY include a P-Asserted-Identity header field in a request to report the identity of the user on behalf of which the UAC is acting and whose identity the UAC is in a position to assert. A UAC SHOULD do so only in cases where it believes it is in the same Trust Domain as the first proxy and is connected to the first proxy in accordance with the security requirements of RFC 3325. A UAC SHOULD NOT do so in other circumstances and might instead use the P-Preferred-Identity header field. A UAC MUST NOT include both header fields.

A UAC MAY include a P-Asserted-Identity header field in an UPDATE request to report a changed identity mid-dialog. This can be an UPDATE request sent specially for this purpose or an UPDATE request sent for some other purpose. A UAC SHOULD do so only in cases where

it believes it is in the same Trust Domain as the first proxy and is connected to the first proxy in accordance with the security requirements of RFC 3325.

A UAC MAY include a P-Asserted-Identity or P-Preferred-Identity header field in a MESSAGE or PUBLISH request. A UAC SHOULD include a P-Asserted-Identity header field only in cases where it believes it is in the same Trust Domain as the first proxy and is connected to the first proxy in accordance with the security requirements of RFC 3325.

4.1.2. Response handling

Typically a UA renders the value of a P-Asserted-Identity header field that it receives in a response to its user. It may consider the identity provided by a Trust Domain to be privileged, or intrinsically more trustworthy than other information in the response. However, any particular behaviour is specific to implementations or services. This document also does not mandate any UA handling for multiple P-Asserted-Identity header field values that happen to appear in a response (such as a SIP URI alongside a tel URL).

However, if a UAC receives a response from a previous element outside the Trust Domain, it MUST NOT use the P-Asserted-Identity header field in any way.

If a UA is part of the Trust Domain from which it received a response containing a P-Asserted-Identity header field, then it can use the value freely but it MUST ensure that it does not forward the information to any element that is not part of the Trust Domain if the user has requested that asserted identity information be kept private.

4.2. Proxy Behaviour

4.2.1. Request handling

If a proxy receives a request from a UAC within the Trust Domain it MUST behave as for a request from any other node within the Trust Domain, in accordance with the rules of RFC 3325 for a proxy.

If a proxy receives an UPDATE, MESSAGE or PUBLISH request containing a P-Asserted-Identity header field, it MUST behave as for any other request in accordance with the rules of RFC 3325 for a proxy.

If a proxy receives a MESSAGE or PUBLISH request containing a P-Preferred-Identity header field, it MUST behave as for any other

request in accordance with the rules of RFC 3325 for a proxy.

4.2.2. Response handling

The proxy behaviour specified in RFC 3325 is applicable to responses with the following qualifications. A proxy that receives a response from a node outside the Trust Domain cannot directly authenticate the UAS by SIP means. Therefore it MUST NOT include a P-Asserted-Identity header field when forwarding the response unless it has authenticated the UAS by other means. If a proxy receives a response from a UAS within the Trust Domain it MUST behave as for a response from any other node within the Trust Domain, in accordance with the rules of RFC 3325 for a proxy.

> One possible circumstance in which a proxy can include a P-Asserted-Identity header field when forwarding a response from a node outside the Trust Domain is when the proxy has direct TLS connectivity with the UAS and has authenticated the UA by some other means (e.g., SIP digest authentication) during that same TLS session.

The proxy behaviour specified in RFC 3325 for handling a received P-Preferred-Identity header field is applicable also to responses, subject to the qualification above concerning authentication of the UAS as a pre-requisite for inserting a P-Asserted-Identity header field.

4.3. UAS Behaviour

4.3.1. Request handling

If a UAS receives an UPDATE, MESSAGE or PUBLISH request containing a P-Asserted-Identity header field, it MUST behave as for any other request in accordance with the rules of RFC 3325 for a UAS.

4.3.2. Response handling

A UAS MAY include a P-Asserted-Identity or P-Preferred-Identity header field in a response to report the identity of the user on behalf of which the UAS is acting and whose identity the UAS is in a position to assert. A UAS SHOULD include a P-Asserted-Identity header field only in cases where it believes it is in the same Trust Domain as the last proxy and is connected to the last proxy in accordance with the security requirements of RFC 3325.

5. IANA considerations

None

6. Security considerations

The use of asserted identity raises a number of security considerations, which are discussed fully in [RFC3325]. This document raises the following additional security considerations.

When receiving a request or response containing a P-Asserted-Identity header field directly from a UA (rather than from another proxy), a proxy will trust the UA only if it is known to be within the Trust Domain and is connected by means of TLS as specified in RFC 3325. One example where this might be true is a UA that is a PSTN gateway. In this case the UA can assert an identity received from the PSTN, the proxy itself having no means to authenticate such an identity. A proxy must not trust an identity asserted by a UA outside the Trust Domain.

When receiving a response from a node outside the Trust Domain, a proxy has no direct SIP means to authenticate the node. However, if authentication has taken place by other means (e.g., an earlier use of SIP digest authentication) and the entity sending the response is known to be the same entity (e.g., connected via the same TLS session) this can be sufficient grounds for asserting an identity. In other circumstances a proxy must not assert identity for a responding user.

7. Acknowledgements

Useful comments were received from Jonathan Rosenberg and Cullen Jennings during drafting.

8. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[RFC3311] Rosenberg, J., "The Session Initiation Protocol (SIP)

UPDATE Method", RFC 3311, October 2002.

[RFC3325] Jennings, C., Peterson, J., and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", RFC 3325, November 2002.

[RFC3428] Campbell, B., Rosenberg, J., Schulzrinne, H., Huitema, C., and D. Gurle, "Session Initiation Protocol (SIP) Extension for Instant Messaging", RFC 3428, December 2002.

[RFC3903] Niemi, A., "Session Initiation Protocol (SIP) Extension for Event State Publication", RFC 3903, October 2004.

[I-D.ietf-sipping-uri-services] Camarillo, G. and A. Roach, "Framework and Security Considerations for Session Initiation Protocol (SIP) Uniform Resource Identifier (URI)-List Services", draft-ietf-sipping-uri-services-07 (work in progress), November 2007.

Author's Address

John Elwell
Siemens Enterprise Communications GmbH & Co KG
Hofmannstrasse 51
D-81379 Munich
Germany

Phone: +44 115 943 4989
Email: john.elwell@siemens.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).