

SIPPING WG
Internet-Draft
Updates: RFC [3325](#)
(if approved)
Intended status: Informational
Expires: March 27, 2009

J. Elwell
Siemens Enterprise Communications
September 23, 2008

Updates to Asserted Identity in the Session Initiation Protocol (SIP)
draft-ietf-sipping-update-pai-06.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

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 Internet-Draft will expire on March 27, 2009.

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 certain SIP methods such as UPDATE, REGISTER, MESSAGE, PUBLISH and ACK, 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	3
2.	Introduction	3
3.	Discussion	4
3.1.	Inclusion of P-Asserted-Identity by a UAC	4
3.2.	Inclusion of P-Asserted-Identity in any request	5
3.3.	Inclusion of P-Asserted-Identity or P-Preferred-Identity in a response	6
3.3.1.	Inclusion of P-Asserted-Identity or P-Preferred-Identity by a UAS in a response	7
3.3.2.	Inclusion of P-Asserted-Identity by a proxy in a response	7
3.4.	Dialog implications	8
4.	Behaviour	8
4.1.	UAC Behaviour	8
4.1.1.	Request handling	8
4.1.2.	Response handling	9
4.2.	Proxy Behaviour	9
4.2.1.	Request handling	9
4.2.2.	Response handling	9
4.3.	Registrar Behaviour	10
4.4.	UAS Behaviour	10
4.4.1.	Request handling	10
4.4.2.	Response handling	10
4.5.	General handling	10
5.	IANA considerations	11
6.	Security considerations	11
7.	Acknowledgements	12
8.	References	12
8.1.	Normative References	12
8.2.	Informative References	13
	Author's Address	13
	Intellectual Property and Copyright Statements	14

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 [\[RFC2119\]](#).

This document uses the concepts of Trust Domain and Spec(T), as specified in [section 2.3 of RFC 3324](#) [\[RFC3324\]](#).

2. Introduction

The Session Initiation Protocol (SIP) is specified in [RFC 3261](#) [\[RFC3261\]](#). [RFC 3325](#) [\[RFC3325\]](#) specifies a mechanism for conveying within a Trust Domain the asserted identity of the originator of a SIP request. This is achieved by means of the P-Asserted-Identity header field, which is specified for use in requests using a number of SIP methods, in particular the INVITE method.

[RFC 3325](#) does not specify the insertion of the P-Asserted-Identity 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 certain SIP methods such as UPDATE [\[RFC3311\]](#), REGISTER, MESSAGE [\[RFC3428\]](#), PUBLISH [\[RFC3903\]](#) and ACK. Finally, [RFC 3325](#) 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 any request and, under certain conditions, allowing use of this header field in SIP responses. This document also allows the use of the P-Preferred-Identity header field in some of these situations.

[RFC 3325](#) allows the P-Asserted-Identity and P-Preferred-Identity header fields each to contain at most two URIs, where one is a SIP or SIPS URI [\[RFC3261\]](#) and the other is a TEL URI [\[RFC3966\]](#). This may be unduly restrictive in future, for example if there is a need to allow other URI schemes, if there is a need to allow both a SIP and a SIPS URI or if there is a need to allow more than one URI with the same scheme (e.g., a SIP URI based on a telephone number and a SIP URI that is not based on a telephone number). This document therefore provides forwards compatibility by mandating tolerance to the receipt of unexpected URIs.

This document does not alter the fact that the asserted identity mechanism has limited applicability, i.e., within a Trust Domain.

For general applicability, including operation outside a Trust Domain (e.g., over the public Internet) or between different Trust Domains, a different mechanism is needed. [RFC 4474](#) [[RFC4474](#)] specifies the Identity header field, in conjunction with the From header field, for providing authenticated identity in such circumstances.

[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 downstream SIP entity. Examples of types of UAC that are often suitable for inclusion in a Trust Domain are:

- o PSTN gateways;
- o media servers;
- o application servers (or B2BUAs) that act as URI list servers [[I-D.ietf-sipping-uri-services](#)];
- o 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 behave in accordance with a Spec(T), and this principle needs to apply 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.

This update to [RFC 3325](#) clarifies that a UAC may include a P-Asserted-Identity header field in a request in certain circumstances.

3.2. Inclusion of P-Asserted-Identity in any 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) [[RFC3725](#)] 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. In other words, it would provide the new calling UA with the identity of the new called user and provide the new called UA(s) with the identity of the new calling user. This can be achieved by the B2BUA sending an UPDATE request with a P-Asserted-Identity header field on the dialogs concerned.

Within a Trust Domain, a P-Asserted-Identity header field could advantageously be used in a REGISTER request between an edge proxy that has authenticated the source of the request and the registrar.

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.

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.

Within a Trust Domain, a P-Asserted-Identity header field could advantageously be used in an ACK request. Considering the 3PCC scenario in Flow I of [[RFC3725](#)], the asserted identity of user B may not be known when the B2BUA (controller) sends the initial INVITE request to UA A, but might be known when the B2BUA sends the ACK request to UA A (having received it in the 200 response from UA B).

Thus there are several examples where P-Asserted-Identity could be used in requests with methods that are not provided for in [RFC 3325](#) or any other RFC. This leaves a few methods for which use cases are less obvious, but the inclusion of P-Asserted Identity would not cause any harm. In any requests, the header field would simply assert the source of that request, whether or not this is of any use to the UAS. Similarly there are examples where P-Preferred-Identity could be used in requests with methods that are not provided for in [RFC 3325](#) or any other RFC.

This update to [RFC 3325](#) allows a P-Asserted-Identity or P-Preferred-Identity header field to be included in any request.

[3.3.](#) 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 responder. Some examples of the benefits to be gained include:

- o Asserted identity in a 2xx response to an INVITE request would indicate the identity of the connected user.
- o Asserted identity in a provisional response to an INVITE request would indicate the contacted (e.g., alerted) user.
- o Asserted identity in a 2xx response to a MESSAGE request would provide confirmation of where the message was delivered to.
- o 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 to identify the connected user 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.

Note that when the authenticated identity of the connected user is to be provided using the From and Identity header fields (as opposed to providing asserted identity using the P-Asserted-Identity header field), [RFC 4916](#) [RFC4916] requires this to be done in a mid-dialog request (e.g., UPDATE) in the reverse direction. This is because the Identity header field is defined only for use in requests.

[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 only mention requests.

[3.3.1](#). Inclusion of P-Asserted-Identity or P-Preferred-Identity by a UAS in a response

It should 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 SIP entity from which the request was received.

Between a UAS and a SIP entity 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.

This update to [RFC 3325](#) allows a UAS to insert a P-Asserted-Identity or P-Preferred-Identity header field in a response.

[3.3.2](#). Inclusion of P-Asserted-Identity by a proxy in a response

[Section 5 of RFC 3325](#) requires a proxy to authenticate the originator of a message from a node outside the Trust Domain before including a P-Asserted-Identity header field in the forwarded message. While this is achievable for requests using SIP digest authentication, it

is not achievable in the same way for responses. A proxy cannot challenge a response and cannot establish the authenticity of the sender of a response. In practice, there is no standardised manner by which a SIP proxy can authenticate the sender of the response. Therefore, a proxy must not include a P-Asserted-Identity header field when forwarding the response unless it has authenticated the UAS by some means. The means to authenticate the UAS is outside the scope of this document. However, future documents may define techniques for response authentication.

This update to [RFC 3325](#) allows a proxy to include a P-Asserted-Identity header field in certain circumstances when forwarding a response.

[3.4.](#) Dialog implications

A P-Asserted-Identity header field in a received request or response asserts the identity of the source of that request or response and says nothing about the source of subsequent received requests or responses claiming to relate to the same dialog. The recipient can make its own deductions about the source of subsequent requests or responses not containing a P-Asserted-Identity header field. This document does not change [RFC 3325](#) in this respect.

[4.](#) Behaviour

This document 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 or P-Preferred-Identity header field to appear in any request, and by allowing a P-Asserted-Identity header field to appear in a response in certain circumstances.

[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 SIP entity to which it sends the request and is connected to that SIP entity 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 or P-Preferred-Identity

header field in any request, i.e., not limited to the methods allowed in [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 it does not trust, 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 internally but it MUST ensure that it does not forward the information to any element that is not part of the Trust Domain if the responding 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.

Note that this implies that the proxy must have authenticated the sender of the request in accordance with the Spec(T) in force for the Trust Domain and determined that the sender is indeed part of the Trust Domain.

If a proxy receives a request containing a P-Asserted-Identity or P-Preferred-Identity header field, it MUST behave in accordance with the rules of [RFC 3325](#) for a proxy, even if the method is not one for which [RFC 3325](#) specifies use of that header field.

[4.2.2.](#) Response handling

The proxy behaviour specified in [RFC 3325](#) is applicable to responses with the following qualifications. A proxy MUST NOT include a

P-Asserted-Identity header field when forwarding a response from a node outside the Trust Domain unless it has authenticated the UAS by some means. The means to authenticate the UAS is outside the scope of this document.

The proxy behaviour specified in [RFC 3325](#) applies for handling a P-Asserted-Identity header field in a response from a node within the Trust Domain.

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 including a P-Asserted-Identity header field when forwarding a response.

[4.3.](#) Registrar Behaviour

If a registrar receives a REGISTER request containing a P-Asserted-Identity header field, it MUST disregard the asserted identity unless received over a secure transport from a node within the Trust Domain. Otherwise it MAY use this as evidence that the registering UA has been authenticated as representing the identity asserted in the header field.

[4.4.](#) UAS Behaviour

[4.4.1.](#) Request handling

If a UAS receives any 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, even if the method is not one for which [RFC 3325](#) specifies use of that header field.

[4.4.2.](#) 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 SIP entity from which it received the request and is connected to that SIP entity in accordance with the security requirements of [RFC 3325](#).

[4.5.](#) General handling

If an entity receives a request or response containing a P-Asserted-Identity or P-Preferred-Identity header field containing an

unexpected number of URIs or unexpected URI schemes it MUST act as follows:

- o ignore any URI with an unexpected URI scheme;
- o ignore any URI for which the expected maximum number of URIs with the same scheme occurred earlier in the header field; and
- o ignore any URI whose scheme is not expected to occur in combination with a scheme that occurred earlier in the header field.

This document does not change the [RFC 3325](#) requirement that allows each of these header fields to contain at most two URIs, where one is a SIP or SIPS URI and the other is a TEL URI, but future updates to this document may relax that requirement. In the absence of such a relaxation, the requirement above means that an entity receiving a request or response containing a P-Asserted-Identity or P-Preferred-Identity header field must act as follows:

- o ignore any URI with a scheme other than SIP, SIPS or TEL;
- o ignore a second or subsequent SIP URI, a second or subsequent SIPS URI or a second or subsequent TEL URI; and
- o ignore a SIP URI if a SIPS URI occurred earlier in the header field and vice versa.

A proxy MUST NOT forward a URI when forwarding a message if that URI is to be ignored in accordance with the requirement above.

5. IANA considerations

This document requires no IANA actions.

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, a proxy will trust the assertion only if the source is known to be within the Trust Domain and behaves in accordance with a Spec(T), which defines the security requirements. This applies regardless of the nature of the resource (UA or proxy). One example

where a trusted source might be a UA 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 SIP entity must not trust an identity asserted by a source outside the Trust Domain. Typically a UA under the control of an individual user (such as a desk phone or mobile phone) should not be considered part of a Trust Domain.

When receiving a response from a node outside the Trust Domain, a proxy has no standardised SIP means to authenticate the node. However, if authentication has taken place by other means, outside the scope of this document, this can be sufficient grounds for asserting an identity. In other circumstances a proxy must not assert identity for a responding user.

When receiving a REGISTER request containing a P-Asserted-Identity header field, a proxy will trust the asserted identity only if received over a secure connection from a proxy within the Trust Domain.

7. Acknowledgements

Useful comments were received from Francois Audet, Jeroen van Bommel, Hans Erik van Elburg, Vijay Gurbani, Cullen Jennings, Hadriel Kaplan, Paul Kyzivat, Jonathan Rosenberg, Thomas Stach and Brett Tate during drafting and review.

8. References

8.1. 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.
- [RFC3324] Watson, M., "Short Term Requirements for Network Asserted Identity", [RFC 3324](#), November 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.

[RFC3966] Schulzrinne, H., "The tel URI for Telephone Numbers", [RFC 3966](#), December 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.

[8.2.](#) Informative References

[RFC3725] Rosenberg, J., Peterson, J., Schulzrinne, H., and G. Camarillo, "Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)", [BCP 85](#), [RFC 3725](#), April 2004.

[RFC4474] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", [RFC 4474](#), August 2006.

[RFC4916] Elwell, J., "Connected Identity in the Session Initiation Protocol (SIP)", [RFC 4916](#), June 2007.

Author's Address

John Elwell
Siemens Enterprise Communications

Phone: +44 115 943 4989

Email: john.elwell@siemens.com

Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

