SIPPING WG
Internet-Draft
Updates: RFC 3325
(if approved)
Intended status: Informational
Expires: June 19, 2009

J. Elwell
Siemens Enterprise Communications

December 16, 2008

Updates to Asserted Identity in the Session Initiation Protocol (SIP) draft-ietf-sipping-update-pai-08.txt

Status of this Memo

This Internet-Draft will expire on June 19, 2009.

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 P-Asserted-Identity and P-Preferred-Identity header fields with certain SIP methods such as UPDATE, REGISTER, MESSAGE and PUBLISH, and does not specify how to handle an unexpected number of URIs or unexpected URI schemes in these header fields. 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].

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 and P-Preferred-Identity header fields with certain SIP methods such as UPDATE [RFC3311], REGISTER, MESSAGE [RFC3428] and PUBLISH [RFC3903]. 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 and allowing use of P-Asserted-Identity and P-Preferred-Identity header fields in any request except ACK and CANCEL. The reason for these two exceptions is that ACK and CANCEL requests cannot be challenged for digest authentication.

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. RFC 4916 [RFC4916] specifies the use of RFC 4474 in mid-dialog requests, in particular in requests in the reverse direction to the dialog-forming request as a means of providing authenticated connected identity.

RFC 3325 is unclear on the use of P-Asserted-Identity in responses. In contrast to requests, there is no means in SIP to challenge a UAS to provide SIP digest authentication in a response. As a result, there is currently no standardised mechanism whereby a proxy can authenticate a UAS. Since authenticating the source of a message is a pre-requisite for asserting an identity, this document does not specify the use of the P-Asserted-Identity header field in responses. This may be the subject of a future update to RFC 3325. Also this document does not specify the use of the P-Preferred-Identity header field in responses, as this would serve no purpose in the absence of the ability for a proxy to insert the P-Asserted-Identity header field.

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:

- PSTN gateways;
- media servers;
- application servers (or B2BUAs) that act as URI list servers [RFC5363];
- 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.

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. Inclusion of P-Asserted-Identity in a request requires that the original asserter of an identity be able to authenticate the source of the request. This implies the ability to challenge a request for SIP digest authentication, which is not possible with ACK and CANCEL requests. Therefore ACK and CANCEL requests need to be excluded.

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 (with the exception of ACK and CANCEL).

This update to RFC 3325 allows a P-Asserted-Identity or P-Preferred-Identity header field to be included in any request except ACK and CANCEL.

3.3. Dialog implications

A P-Asserted-Identity header field in a received request asserts the identity of the source of that request and says nothing about the source of subsequent received requests claiming to relate to the same dialog. The recipient can make its own deductions about the source of subsequent requests 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 and by allowing a P-Asserted-Identity or P-Preferred-Identity header field to appear in any request.

4.1. UAC Behaviour

A UAC MAY include a P-Asserted-Identity header field in any request except ACK and CANCEL 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.

4.2. Proxy Behaviour

If a proxy receives a request containing a P-Asserted-Identity header field 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 (other than ACK or CANCEL) 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.

4.3. Registrar Behaviour

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

asserted in the header field.

4.4. UAS Behaviour

If a UAS receives any request (other than ACK or CANCEL) containing a P-Asserted-Identity header field, it MUST behave 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.

4.5. General handling

If an entity receives a request 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:

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

In the absence of a Spec(T) determining otherwise, 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 or a Spec(T) determining otherwise, the RFC 3325 requirement means that an entity receiving a request containing a P-Asserted-Identity or P-Preferred-Identity header field must act as follows:

- ignore any URI with a scheme other than SIP, SIPS or TEL;
- ignore a second or subsequent SIP URI, a second or subsequent SIPS URI or a second or subsequent TEL URI; and
- 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 request 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 adding a P-Asserted-Identity header field to a message, an entity must have authenticated the source of the message by some means. One means is to challenge the sender of a message to provide SIP digest authentication. Responses cannot be challenged, and also ACK and CANCEL requests cannot be challenged. Therefore this document limits the use of P-Asserted-Identity to requests other than ACK and CANCEL.

When receiving a request 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. For this reason, this document does not specify the use of P-Asserted-Identity or P-Preferred-Identity in responses.

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, John-Luc Bakker, Jeroen van Bemmel, 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.

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.

[RFC5363] Camarillo, G. and A. Roach, "Framework and Security Considerations for Session Initiation Protocol (SIP) URI-List Services", RFC 5363, October 2008.

Author's Address

John Elwell
Siemens Enterprise Communications

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