End-to-End Identity Important in the Session Initiation Protocol (SIP)
draft-elwell-sip-e2e-identity-important-00.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 January 8, 2009.

Abstract

This document surveys existing mechanisms in the Session Initiation Protocol (SIP) for identifying and authenticating the source of a SIP request (or caller identification). It describes how identification and authentication are not always end-to-end and the problems that this can lead to, particularly since media security based on techniques such as DTLS-SRTP is dependent on end-to-end authenticated identification of parties.

This work is being discussed on the sip@ietf.org mailing list.
Table of Contents

1. Introduction .................................................. 3
2. Overview of existing mechanisms and their shortcomings .... 3
   2.1. The From header field URI ............................... 4
   2.2. The P-Asserted-Identity (PAI) header field ............. 4
   2.3. Authenticated Identity Body (AIB) ....................... 5
   2.4. SIP Identity ............................................. 5
   2.5. Problems with SIP URIs based on E.164 numbers ......... 6
   2.6. Other causes of URI change at intermediate domains .... 7
   2.7. Problems with PSTN interworking ......................... 7
3. Why end-to-end identification is important .................. 8
   3.1. Example 1 ............................................... 8
   3.2. Example 2 ............................................... 8
   3.3. Example 3 ............................................... 9
   3.4. Example 4 ............................................... 9
   3.5. Example 5 ............................................... 9
   3.6. Example 6 .............................................. 10
   3.7. Example 7 .............................................. 10
   3.8. Example 8 .............................................. 11
   3.9. Example 9 .............................................. 11
   3.10. Example 10 .............................................. 11
   3.11. Example 11 .............................................. 12
   3.12. Example 12 .............................................. 12
   3.13. Summary of examples ................................. 12
4. Why end-to-end authentication of identity is important ...... 13
5. Conclusions .................................................. 14
6. IANA considerations ........................................... 14
7. Security considerations ....................................... 15
8. Acknowledgements .............................................. 15
9. Informative References ....................................... 15
Author’s Address ................................................ 16
Intellectual Property and Copyright Statements ................. 17
1. Introduction

The Session Initiation Protocol (SIP) [RFC3261] provides two basic mechanisms for identifying users involved in a session or call: the From header field URI [RFC3261] and the P-Asserted-Identity header field [RFC3325]. Used alone, these are vulnerable to misuse, but two mechanisms exist for providing authentication of the From header field URI: Authenticated Identity Body [RFC3893] and the Identity and Identity-Info header fields (SIP Identity, [RFC4474]). These various mechanisms provide to the recipient of a SIP request (the UAS and its user) identification (with or without authentication) of the source of a SIP request (the UAC’s user).

Further, by binding an end of a secure bidirectional medium using SRTP [RFC3711] to a SIP request whose source has been identified, the recipient of that SIP request can know the identity of the user who is the source and sink of that medium. This is the principle behind DTLS-SRTP [I-D.ietf-sip-dtls-srtp-framework], which uses certificates in the endpoints to agree a security context for SRTP. DTLS-SRTP also exchanges fingerprints of those certificates in SIP messages, thereby binding the media to those SIP messages. If a SIP message carrying such a certificate fingerprint also includes the authenticated identity of the user on behalf of which the SIP message has been sent, the secure media are bound to that user. DTLS-SRTP currently relies on the From header field URI and SIP Identity to achieve this.

This is the theory, but there are a number of practical considerations that make this very difficult to deploy in many situations, particularly when there are intermediaries that change identity information or break signatures. This has led to a number of proposed work-arounds, but has also led to a questioning of the need for end-to-end authenticated identification. This document explains why end-to-end identification is important.

Although the primary function of SIP is to initiate sessions (Session Initiation Protocol), it also includes some methods for use outside the context of a session, e.g., MESSAGE, SUBSCRIBE, NOTIFY, PUBLISH. Although the main focus of this document is on identifying users involved in sessions, many of the considerations apply equally to other uses of SIP.

2. Overview of existing mechanisms and their shortcomings
2.1. The From header field URI

Although a UAC should place its Address of Record (AoR) in the From header field of a SIP request, it is a well known fact that in practice a UAC is free to place any value there. SIP proxies are not allowed to change the value, but a SIP proxy could demand that the UAC authenticate itself (using SIP digest authentication) and reject a request if the From URI does not match the authenticated user. A B2BUA could also do this, or could rectify the From URI and forward the request, as an alternative to rejecting the request.

However, a user is likely to have a SIP digest authentication shared secret only with a SIP entity (proxy or B2BUA) in the same domain, and any downstream SIP entities (in other domains) will not be in a position to challenge for digest authentication. Those SIP entities will have no means of knowing whether the request has been validated by an entity in the source user’s domain, and therefore no means of trusting the From URI.

2.2. The P-Asserted-Identity (PAI) header field

This was introduced to counter some of the problems with the From URI. A SIP entity that has validated the source of a SIP request can include a PAI header field containing the validated URI, which may differ from the From URI. A downstream entity in the same trust domain will place some trust in this value. Entities within the same trust domain must exchange SIP messages over a secure transport (e.g., TLS), so that the upstream entity is authenticated. That upstream entity is then trusted to provide a correct identity in the PAI header field.

This mechanism was introduced for use in closed environments where a trust domain could be established, rather than for use on the Internet. However, it has seen very considerable deployment.

The problem lies in its notion of transitive trust, i.e., A asserts an identity and sends it over a secure transport to B. B trusts the assertion, and passes the assertion on over a secure transport to C. C trusts B, and passes the assertion on over a secure transport to D, and so on. D trusts C, and has to rely on C’s trust of any upstream entities (in this case B). C has to rely on B’s trust of any upstream entities (in this case A). The problem is, a downstream entity does not know the entire upstream path of trust, so in trusting its neighbour it does not know who else it is being forced to trust. As SIP continues to grow, eventually a bad actor or malicious site will be trusted by another party many hops away.

Furthermore, when an entity receives a request from outside its trust domain...
domain it can place a default value in the PAI header field when forwarding the request. For example, when a service provider receives a request from an enterprise, if it does not trust the PAI received from the enterprise it is common practice to insert the default number for the enterprise, e.g., that of an attendant or reception desk. This can be misleading, particularly if the request originated outside the enterprise and has been forwarded by the enterprise to the service provider. Arguably it also violates [RFC3325], since the default number is being placed into PAI without having authenticated that number as the source of the SIP request. This practice can also cause the PAI URI to deviate from the From URI (typically they are the same in many simple situations), causing a dilemma for the UAS - which one to present to the user (or a dilemma for the user if both are presented).

2.3. Authenticated Identity Body (AIB)

With AIB, the UAC copies the From URI and some other header fields into a body of the SIP request and signs it using S/MIME [RFC3851]. The ability to include S/MIME in [RFC3261] (and likewise PGP [RFC2015] in the original version of SIP [RFC2543]) demonstrates that end-to-end security has always been considered important in SIP, and AIB binds the From URI to the end-to-end authentication that S/MIME provides. AIB has not been deployed because S/MIME has not been deployed, and that is turn can probably be blamed on the need for each SIP UA to have its own certificate and private key and the infrastructure needed to manage that. However, the mechanism is in theory capable of true end-to-end authenticated identity.

2.4. SIP Identity

SIP Identity addresses the impracticalities of AIB by having a SIP entity that has validated the source of a SIP request (e.g., using SIP digest authentication) place a signature over the From header field URI and other parts of the message to assert the correctness of the From URI and provide integrity protection over the signed parts. The signature is placed in the Identity header field and information needed for validating the signature is placed in the Identity-Info header field. This provides authenticated identification between the source domain and the UAS, or between the source domain and a verifying entity in the destination domain. Therefore it can be considered to provide end-domain-to-end-domain authentication. In the context of a session of call, the SIP Identity in the INVITE request can authenticate the calling user and SIP Identity in the reverse direction [RFC4916] can authenticate the connected user. DTLS-SRTP relies on SIP Identity to bind SRTP media to a calling or connected user.
However, SIP Identity has seen little (if any) deployment, and that is partly due to lack of a perceived need (many regard PAI as sufficient) and partly because it has been shown not to work in many common situations.

One difficulty is with SIP URIs based on E.164 number (see Section 2.5), which can result in B2BUAs changing the From header field URI, thereby breaking the original signature. Re-signing by the domain that modifies the From URI destroys the end-domain-to-end-domain principle and re-introduces the transitive trust problem that PAI suffers from.

Another difficult is with B2BUAs (e.g., Session Border Controller, SBC) that modify other parts of the signed information, in particular the SDP body. This tends to happen every time media is handed off to another service provider. Although this could perhaps be solved for an SBC in the end domain (or even for an SBC in the next domain, if it has a commercial arrangement with the end domain, for example allowing it to use the end domain’s private key), it can’t be solved in general if there are intermediate hand-offs of media with SBCs behaving in this way. SBC behaviour in this respect, and the reasons for it, are documented in [I-D.kaplan-sip-uris-change].

2.5. Problems with SIP URIs based on E.164 numbers

If a user receives a caller or connected identity in the form of a SIP URI containing a global E.164 number (e.g., sip:+123456789@example.com;user=phone), and if this information is made available to the user, how would the user interpret it? The user might recognise the telephone number and ignore the domain part. The user might treat the domain part as significant and disregard the number (particularly if she fails to recognise the number). Or the user might take account of both items of information.

Problems arise when the user attaches importance to the domain part, because there is no defined meaning for the domain part (other than that by routing a request to that URI to that domain, that domain should be able to route it onwards towards the user of the telephone number). In practice, the domain part is often changed by intermediate domains (typically to reflect their own domain), so a request starting out with sip:+123456789@mybank.com;user=phone in the From or PAI header field could end up with sip:+123456789@serviceprovider.net;user=phone in that header field when delivered to the UAS, where serviceprovider.net is the last domain it passed through. The recipient would not see that the request really originated in mybank.com, and this information may have been important to the recipient.
Moreover, any such change of From URI breaks the SIP Identity signature, as described earlier.

Clearly these problems do not exist with tel URIs [RFC3966] since there is no domain part and therefore no scope for change. Therefore they have the advantage of not providing a false or misleading domain part, but the disadvantage of not providing a domain part at all for users who would benefit from this information. Also tel URIs cannot be used with SIP Identity.

The E.164 problem is described in more detail in [I-D.elwell-sip-e164-problem-statement].

2.6. Other causes of URI change at intermediate domains

As described in Section 2.5, intermediate domains can change a URI based on an E.164 number, such that the recipient does not receive the original identifier. This is not the sole circumstance in which intermediate domains are known to change an identifier identifying the source of a SIP request. Another circumstance is where a domain does not accept a received identifier as a valid source and substitutes a default value. This often occurs when an enterprise submits an identifier to a service provider, the identifier not being within the range recognised by the service provider as belonging to that enterprise. There are legitimate reasons why an enterprise might submit an identify outside the recognised range, as highlighted by some of the examples in Section 3. When delivered to the UAS, the new identifier might be misleading.

2.7. Problems with PSTN interworking

A PSTN gateway will generally deliver a number received from PSTN as the From or PAI URI. The gateway has no means of validating that number and has either to trust the PSTN or disregard the number (placing its own identity or an anonymous value in the From URI). There are known means of a false caller number in PSTN (depending on country), and therefore trusting a number from PSTN can be dangerous.

Furthermore, from a DTLS-SRTP perspective, it can be dangerous to assume that media are secured all the way to a PSTN user. First, the PSTN has known vulnerabilities in terms of interception of calls for legal or other reasons. Second, there is no way of detecting whether the PSTN user is attached to the PSTN via an unsecured IP network. Therefore, at best, a call can be considered secure only as far as the gateway and true end-to-end (or end-domain-to-end-domain) security is not achievable. Solutions are required to the problem of misleading the user concerning the end-to-end security status of a call to/from PSTN, but this issue is not discussed further in this
3. Why end-to-end identification is important

In Section 2.5 and Section 2.6 it was shown how the identifier representing the source of SIP request can be modified by SIP intermediaries before being delivered to the UAS. Furthermore, Section 2.4 mentioned how an intermediate domain could change the From URI in order to "fix" a broken RFC 4474 signature. In these cases, identification delivery is not end-to-end and often fails to deliver information needed by the recipient. In this section a number of example use cases are given, only some of which deliver end-to-end identification.

In the figures associated with the examples below, caller identification is shown in the From header field URI, but a similar problem can arise with PAI.

3.1. Example 1

Consider a call from an employee Bob at bank.com to Alice, who obtains a SIP service from service provider sp.net. Alice would be prepared to accept a call from her bank. Bob’s identifier is sip:bob@bank.com. In this case, hopefully Alice would receive this identifier unchanged. She might not know Bob, but at least she knows the call is from her bank and can accept the call on that basis.

```
+----------------------->      ------------------------>
bank.com  sp.net  Alice
From:sip:bob@bank.com       From:sip:bob@bank.com
--------------------------->     -------------------------->
```

This example delivers end-to-end identification, but in practice it is likely that any RFC 4474 signature provided by the originating domain will be broken because an intermediate B2BUA modifies signed information.

3.2. Example 2

Suppose the service provider removes Bob’s identifier and substitutes the default for the bank, based on the bank’s default telephone number +123456000 and the bank’s domain name. Alice would receive sip:+123456000@bank.com;user=phone.

```
+----------------------->      --------------------------->
bank.com  sp.net  Alice
From:sip:bob@bank.com       From:sip:+123456000@bank.com;user=phone
--------------------------->     -------------------------->
```
This example does not deliver end-to-end identification. In this case Alice still knows the call is from her bank but there is no indication of who at the bank is calling. Furthermore, if she were to make a return call the bank, it would arrive at a default user (e.g., attendant, receptionist) and would not reach Bob. This may be what the bank desires (in which case it would not disclose Bob’s identifier to the service provider), but in many cases it may not be what the bank desires.

3.3. Example 3

Suppose the service provider removes Bob’s identifier and substitutes the default for the bank, based on the bank’s default telephone number +123456000 and the service provider’s domain name. Alice would receive sip:+123456000@sp.net;user=phone.

```
bank.com   sp.net   Alice
From:sip:bob@bank.com From:sip:+123456000@sp.net;user=phone
----------------------> ---------------------------------->
```

This example does not deliver end-to-end identification. In this case Alice cannot tell from the received identifier that the call is from her bank, unless she happens to recognise the telephone number. This is no worse than PSTN (or no worse than if a tel: URI were used in SIP), but SIP has the potential to be better than PSTN. As for example 2, there is also a problem with return calls.

3.4. Example 4

Bob’s identifier is sip:+123456789@bank.com;user=phone. If the service provider delivers this to Alice she will see it is from her bank. She may or may not recognise the telephone number as belonging to Bob or to the bank.

```
bank.com   sp.net   Alice
From:sip:+123456789 From:sip:+123456789
@bank.com;user=phone @bank.com;user=phone
----------------------> ---------------------------------->
```

This example delivers end-to-end identification, but in practice it is likely that any RFC 4474 signature provided by the originating domain will be broken because an intermediate B2BUA modifies signed information.

3.5. Example 5

Suppose the service provider substitutes its own domain name for the bank’s domain name. Alice would receive
This example does not deliver end-to-end identification. In this case Alice cannot see that the call is from her bank, unless she happens to recognise the telephone number. However, the number is delivered end-to-end, which may be sufficient for some purposes.

3.6. Example 6

Suppose the service provider substitutes its own domain name for the bank's domain name, and also substitutes the default telephone number for the bank. Alice would receive sip:+123456000@sp.net;user=phone.

bank.com       sp.net             Alice
From:sip:+123456789       From:sip:+123456000
@bank.com;user=phone      @sp.net;user=phone
-------------------->      -------------------->

This example does not deliver end-to-end identification. Alice receives the same identifier as in example 3, and the same considerations apply.

3.7. Example 7

Consider a call from Carol at client.org to Dave at example.com. Dave is working at home and has arranged for calls to be forwarded to him via his SIP service provider sp.net. Suppose Carol’s identifier is carol@client.org and this identifier reaches example.com, where it is forwarded, with the INVITE request, to sp.net. If sp.net delivers this unchanged to Dave at home, Dave will see that the call is from Carol at his client and can accept the call on that basis. Also he can make a return call, e.g., if he is unable to answer at the time and Carol’s identifier is stored in his missed call log.

client.org       example.com       sp.net          Alice
From:sip:carol     From:sip:carol   From:sip:carol
@client.org       @client.org      @client.org
-------------------->      -------------------->    -------------------->

This example delivers end-to-end identification, but in practice it is likely that any RFC 4474 signature provided by the originating domain will be broken because an intermediate B2BUA modifies signed information.
3.8. Example 8

Suppose the service provider does not accept sip:carol@client.org as an identifier received from example.com and substitutes the default identifier for example.com, based on its default number and its domain name (sip:+123456000@example.com;user=phone).

```
client.org   example.com   sp.net   Alice
From:sip:carol   From:sip:carol     From:+123456000
@client.org     @client.org       @example.com
                   ;user=phone
```

This example does not deliver end-to-end identification. Dave will now see that the call comes from his own company, and will not have a clue that it comes from his client. Similarly if the service provider’s domain name is used (sip:+123456000@sp.net;user=phone), Dave would presumably recognise his company’s own default telephone number but would not see that the call is from his client. Also any attempted return call would just go to his company’s default answering point.

3.9. Example 9

Suppose Carol’s identifier is E.164-based: sip:+123498765@client.org;user=phone. If this is delivered to Dave, he will see the calling telephone number, which he may recognise (or software in his phone may match it with an existing contact) and he will also see that it is from client.org.

```
client.org   example.com   sp.net   Alice
From:+123498765   From:+123498765   From:+123498765
@client.org    @client.org     @client.org
                   ;user=phone
```

This example delivers end-to-end identification, but in practice it is likely that any RFC 4474 signature provided by the originating domain will be broken because an intermediate B2BUA modifies signed information.

3.10. Example 10

Suppose the identifier in the last example is not accepted by the service provider, not only because of the domain part (client.org rather than example.com) but also because the telephone number does not fall within the range assigned to example.com. As in example 8 it might substitute a default identifier.
client.org  example.com  sp.net  Alice
From:sip:+123498765  From:sip:+123498765  From:sip:+123498000
@client.org  @client.org  @sp.net
;user=phone  ;user=phone  ;user=phone
------------------->  ------------------->  ------------------>

This example does not deliver end-to-end identification.
Consequences are similar to those in example 8.

3.11. Example 11

Eve in the US office of enterprise e.com
(sip:+123456789@e.com;user=phone) makes a call to Fred, who has a UK
telephone number (+44...) and is served by UK service provider
uksp.net. The US proxy in e.com forwards the request to the UK proxy
of e.com, where the call "breaks out" to uksp.net. The service
provider does not accept a non-UK identifier and substitutes a
default value for the enterprise (sip:+4456780000@e.com;user=phone).

e.com  uksp.net  Fred
From:sip:+123456789  From:sip:+445678000
@e.com;user=phone  @e.com;user=phone
------------------->  ------------------------>

This example does not deliver end-to-end identification. In this
case Fred still knows the call is from e.com, but is not aware that
Eve is calling or that the caller is in the US.

3.12. Example 12

Suppose the service provider uses its own domain name in the modified
SIP URI.

e.com  uksp.net  Fred
From:sip:+123456789  From:sip:+445678000
@e.com;user=phone  @uksp.net;user=phone
------------------->  ------------------------>

This example does not deliver end-to-end identification. In this
case Fred does not know that the call is from e.com (unless he
happens to recognise the UK telephone number). Also Fred is not
aware that Eve is calling or that the caller is in the US.

3.13. Summary of examples

Examples 1, 4, 7 and 9 are fine, because identification of the caller
is end-to-end (although, as pointed out, any RFC 4474 signature might
be broken). In the remaining examples, identification is not end-to-
end, leading to problems.

More complex examples can be derived with more domains involved. Clearly the more domains involved, the more there is scope for failure to deliver an identifier end-to-end, and the greater the consequences for the recipient, both in terms of recognising the source of the call and being able to make a return call. These examples illustrate the importance of delivering an identifier end-to-end, without changing it at intermediate domains.

4. Why end-to-end authentication of identity is important

Assuming an identifier is delivered end-to-end, where authenticated identity is required it is important that the assertion of authenticity is provided at source, or at least in the originating domain. This is what SIP Identity aims to achieve. However, because of the difficulties with SIP Identity, as described in Section 2.4, some have asked why hop-by-hop assertions are insufficient. PAI is one solution to hop-by-hop assertions. Another possibility would be for each domain to provide its own cryptographic signature. Note that SIP Identity does not allow this, because the signer has to have the same domain name as that in the From URI, so only the originating domain can sign (unless the identifier is also changed, which would mean that requirements for end-to-end identification would not be met).

With end-to-end authentication, the relying party has to trust the originating domain, which also means trusting the certificate chain up to the top level certification authority. This is similar to other applications using PKI-based security, such as secure web pages. In many cases there will just be the signing domain’s certificate and a single CA certificate. The relying party can see the whole chain and make its own judgements.

With hop-by-hop authentication based on PAI, the relying party knows only that the upstream neighbour domain is asserting that domain. It does not know how many further upstream domains there are, what those domains are, and how far the trust domain extends. Just because the relying party trusts its own domain and perhaps its upstream neighbour domain, does not mean that it would trust further domains that its upstream neighbour domain trusts.

For example, consider a call from Alice in enterprise1.biz (sip:alice@enterprise1.biz), via service provider sp1.net, via second service provider sp2.org, and terminating at Bob in enterprise2.com (sip:bob@enterprise2.com). The call is routed that way because enterprise1.biz routes all external calls through sp1.net, and
enterprise2.com only accepts external calls that have arrived via sp2.org. Bob is happy to accept a secure call from enterprise1.biz. With hop-by-hop authentication, Bob would have to rely on an assertion by enterprise2.com, which in turn would rely on an assertion by sp2.org, and so on. Bob has no visibility of the upstream entities, although he would probably be aware of his enterprise’s own service provider (sp2.org). He would be unlikely to be aware of sp1.net, and even if he were aware, he may not have heard of sp1.net and may not wish to trust such an assertion. It could be that sp1.net is located in a country where practices are not of the standard expected in Bob’s country.

Suppose also that DTLS-SRTP is to be used to secure media between Alice and Bob. If authentication is hop-by-hop, Bob can be sure that media is secured as far as sp2.org, but cannot be sure that there is no man-in-the-middle between sp2.org and enterprise1.biz. End-to-end authentication is required to give Bob the assurance he needs.

Referring back to the examples in Section 4, those that deliver end-to-end identification have the potential to deliver end-to-end authentication, but in practice, SIP Identity as specified in [RFC4474] is often broken by the actions of B2BUAs. The remaining examples, because they do not deliver end-to-end identification, cannot deliver end-to-end authentication.

5. Conclusions

This documented has demonstrated the importance of end-to-end identifiers (or at least end-domain-to-end-domain identifiers) and authentication of those identifiers in SIP. Although in many simple cases hop-by-hop identification or hop-by-hop assertions can be shown to be adequate, there are many cases where this is simply not the case.

SIP Identity as a solution to end-to-end authenticated identifiers is known to have some shortcomings, and these need to be fixed, either by enhancement to SIP Identity or by provision of an alternative mechanism.

6. IANA considerations

This document requires no IANA actions.
7. Security considerations

Authentication of parties involved in a call is an essential part of this document and is fully discussed in the preceding sections. There are no other security considerations.

8. Acknowledgements

The author received valuable comments from Kai Fischer, Hadriel Kaplan and Dan Wing during drafting.

9. Informative References


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


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

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.