Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 8 January 2026

J. Peterson
TransUnion
C. Wendt
Somos

7 July 2025

Connected Identity for STIR
draft-ietf-stir-rfc4916-update-07

Abstract

The Session Initiation Protocol (SIP) Identity header field conveys cryptographic identity information about the originators of SIP requests. The Secure Telephone Identity Revisited (STIR) framework, however, provides no means for determining the identity of the called party in a traditional telephone-calling scenario. This document updates prior guidance on the "connected identity" problem to reflect the changes to SIP Identity that accompanied STIR, and considers a revised problem space for connected identity as a means of detecting calls that have been retargeted to a party impersonating the intended destination, as well as the spoofing of mid-dialog or dialog-terminating events by intermediaries or third parties.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on 8 January 2026.

Copyright Notice

Table of Contents

1. Introduction

The Session Initiation Protocol (SIP) [RFC3261] initiates sessions, and as a step in establishing sessions, it exchanges information about the parties at both ends. Called users review information about the calling party, for example, to determine whether to accept communications initiated by SIP, in the same way that users of the telephone network assess "Caller ID" information before picking up calls. This information may sometimes be consumed by automated systems to make authorization decisions. STIR [RFC8224] provides a cryptographic assurance of the identity of calling parties in order to prevent impersonation, which is a key enabler of unwanted robocalls, swatting, vishing, voicemail hacking, and similar attacks (see [RFC7375]).

There also exists a related problem: the identity of the party who answers a call can differ from that of the initial called party for various innocuous reasons such as call forwarding. In certain network environments, however, it is possible for attackers to hijack the route of a called number and direct it to a resource controlled by the attacker. It can potentially be difficult to determine why a call reached a target other than the one originally intended, and whether the party ultimately reached by the call is one that the caller should trust. The lack of mutual authentication of parties moreover makes it possible for outside attackers to inject forged messages (e.g., BYE) into a SIP session.

The property of providing the identity of the called party to the calling party is called "connected identity". Previous work on connected identity focused on fixing the core semantics of SIP. [RFC4916] allowed a mid-dialog request, such as an UPDATE [RFC3311], to convey identity in either direction within the context of an existing INVITE-initiated dialog. In an update to the original [RFC3261] behavior, [RFC4916] allowed that UPDATE to alter the From header field value for requests in the backwards direction: previously [RFC3261] required that the From header field values sent in requests in the backwards direction reflect the To header field value of the dialog-forming request. Under the original [RFC3261] rules, if Alice sent a dialog-forming request to Bob, then even if Bob’s SIP service forwarded that dialog-forming request to Carol, Carol would still be required to put Bob’s identity in the From header field value in any mid-dialog requests in the backwards direction.

One of the original motivating use cases for [RFC4916] was the use of connected identity with the SIP Identity [RFC4474] header field. While a mid-dialog request in the backwards direction (e.g., UPDATE) can be signed with Identity like any other SIP request, forwarded requests would not be properly signed without the ability to change the mid-dialog From header field value: Carol, say, would not be able to furnish a key to sign for Bob’s identity if Carol wanted to sign requests in the backwards direction. Carol would, however, be able to sign for her own identity in the From header field value if mid-dialog requests in the backwards direction were permitted to vary from the original To header field value.

With the obsolescence of [RFC4474] by [RFC8224], this specification supersedes the guidance of [RFC4916] to reflect the changes to the SIP Identity header field and the revised problem space of STIR. It also explores some new features that would be enabled by connected identity for STIR, including the use of connected identity to prevent route hijacking and to notify callers when an expected called party has successfully been reached. This document also addresses concerns about applying [RFC4916] connected identity to STIR discussed in the SIPBRANDY framework [RFC8862].

One area of connected identity that is not explored in this document is the implications for conferencing, especially meshed conferencing systems. The scope of this mechanism is solely two-party communications; multiparty sharing of connected identity is left for future work.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here. This document assumes familiarity with common messages, response codes, and header fields used in SIP [RFC3261], and the elements present in the PASSporT [RFC8225] token format.

3. Connected Identity Problem Statement for STIR

The STIR problem statement [RFC7340] enumerates robocalling, voicemail hacking, vishing, and swatting as problems with the modern telephone network that are enabled, or abetted, by impersonation: by the ability of a calling party to arbitrarily set the telephone number that will be rendered to end users to identify the caller.

Today, sophisticated adversaries can redirect calls on the Public Switched Telephone Network (PSTN) to destinations other than the intended called party. For some call centers, like those associated with financial institutions, healthcare, and emergency services, an attacker could hope to gain valuable information about people or to prevent some classes of important services. Moreover, on the Internet, the lack of any centralized or even federated routing system for telephone numbers has resulted in deployments where the routing of calls is arbitrary: calls to telephone numbers might be dumped on a PSTN gateway, they might be sent to a default intermediary that makes forwarding decisions based on a local configuration file, potentially using various mechanisms such as consulting a private ENUM [RFC6116], or routing might be determined

in some other, domain-specific way. In short, there are numerous attack surfaces that an adversary could explore to attempt to redirect calls for a particular number to someplace other than the intended destination.

Another motivating use case for connected identity is mid-dialog requests, including BYE. The potential for an intermediary to generate a forged BYE in the backwards direction has always been built in to the stateful dialog management of SIP. For example, there is a class of mobile fraud attacks ("call stretching") that rely on intermediary networks making it appear to one side as if a call has terminated, while maintaining that the call is still active to the other side, in order to create a billing discrepancy that could be pocketed by the intermediary. If BYE requests in both directions of a SIP dialog could be authenticated with STIR, in the same way as dialog-forming requests, then another impersonation vector leading to fraud in the telephone network could be shut down.

Finally, telephone numbers are widely used today for two-factor authentication (TFA) prior to accessing web resources, which typically rely on sharing some sort of one-time password or similar unique link to validate control of a telephone number. These systems are often capable of using either telephone calls or messages for TFA. Connected identity is very valuable for these use cases because it gives a strong assurance to the calling party that they have in fact reached the telephone for the called telephone number.

There are however practical limits to what securing the signaling can achieve. [RFC4916] rightly observed that once a SIP call has been answered, the called party can be replaced by a different party (with a different identity) due to call transfer, call park and retrieval, and so on. In some cases, due to the presence of a back-to-back user agent, it can be effectively impossible for the calling party to know that this has happened. The problem statement considered for STIR focuses solely on signaling, not whether media from the connected party should be rendered to the caller when a dialog has been established. This specification does not consider further any threats that arise from a substitution of media, though [RFC8862] contains related guidance.

4. Connected Identity without Diversion

In straightforward call setup, the address-of-record (AoR) of the party reached by an INVITE corresponds to the "dest" field of the PASSporT in the INVITE's Identity header field value. The calling party will, however, have no secure assurance that they have reached the proper party if an Identity header field cannot be sent to them in the backwards direction. Provided that the terminating side of

the dialog is STIR-capable, they should have the capacity to sign a PASSporT for the AoR of the called party.

This specification therefore adds provisional and final SIP responses, including the 100, 180, 183, and 200 responses, to the set of messages that may contain an Identity header field. PASSporTs that appear in SIP responses SHOULD use a "ppt" of "rsp", which is defined in Section 9 (although "div" [RFC8946] may additionally appear in responses, per Section 5). PASSporTs of the "rsp" type will be referred to throughout this specification as "rsp" PASSporTs. At a high level, an "rsp" PASSporT is signed similarly to the "div" [RFC8946] PASSporT, in so far as the certificate that signs a "rsp" PASSporT is signing the "dest" field, rather than the "orig" field. If the terminating side does not possess an appropriate credential to sign for the value of the "dest" element value in the PASSporT, it MUST NOT sign and send a "rsp" PASSporT in the backwards direction.

While it might seem attractive to provide identity for SIP failure response codes (4XX, 5XX, 6XX), those explicitly do not form dialogs or connections, and are thus outside the scope of this specification. The same applies to SIP redirect (3XX) response codes, though see [RFC8946], Section 7 for guidance on authentication redirection.

It is worth noting as well that at the time [RFC4916] was written, the Identity mechanism was far stricter about what counted as retargeting than [RFC8224], which has canonicalization processes that eliminate minor changes to the URIs, especially when telephone numbers are the identifiers used by the caller and callee. For basic use cases, a PASSporT in a 183 or 200 OK should be sufficient to secure media keys for the purposes of SIPBRANDY [RFC8862].

The handling of an "rsp" PASSporT differs from the handling of a PASSporT received in a SIP request. Most importantly, note that SIP responses cannot be rejected, unlike SIP requests -- there is no way for the recipient of a response to report errors to the sender. The only protocol action that the calling party could take upon receiving a response carrying a problem PASSporT is to issue a CANCEL (for provisional dialogs) or BYE request in order to tear down the dialog (see Section 7). Moreover, provisional responses are not reliably delivered without using 100rel and PRACK [RFC3262], and provisional responses may be consumed (without forwarding) by intermediaries under a variety of conditions. In short, their delivery is not guaranteed.

5. Connected Identity with Diversion

Use cases involving authorized retargeting motivate connected identity: when a call acquires a new target (in its Request-URI) during transit, then the destination will no longer correspond to the target, the "dest" specified by the PASSporT in the dialog-forming request. If a PASSporT in a response came signed by a different destination than the caller intended, why should the caller trust it?

In STIR, the "div" PASSporT type [RFC8946] was created to securely record when a call was retargeted from one destination to another. Those "div" PASSporTs can be consumed on the terminating side by verification services to determine that a call has reached its eventual destination for the right reasons. As [RFC8946] explains the situation, the only way those diversion PASSporTs will be seen by the calling party is if redirection is used (SIP 3XX responses) instead of retargeting. Because some network policies aim to conceal service logic from the originating party, sending redirections in the backwards direction is the only currently defined way for secure indications of redirection to be revealed to the calling party. That in turn would allow the calling user agent to have a strong assurance that legitimate entities in the call path caused the request to reach a party that the caller did not anticipate.

This specification introduces another alternative. When sending a "rsp" PASSporT type in a SIP response, a User Agent Server (UAS) MAY also include (in Identity header field values) any "div" PASSporTs it received in the INVITE that initiated this dialog. Thus, PASSporTs of type "div" MAY also appear in SIP responses. These "div" PASSporTs can enable the originating side to receive a secure assurance that the call is being fielded by the proper recipient per the routing of the call. In this case, the "dest" signed in the "rsp" PASSporT MUST be the address-of-record of the party who was reached, rather than the "dest" of the PASSporT received in the dialog-initiating INVITE.

An "rsp" PASSporT that signs a different "dest" than the one that appeared in the PASSporT of the dialog-forming request MUST send at least one "div" PASSporT with it. If no "div" PASSporTs were received in a dialog-forming request with a different "dest" value than the original PASSporT claimed, then "rsp" PASSporTs MUST NOT be used in responses. "div" is not universally supported, so calls MAY be retargeted without generating a "div" PASSporT, in which case the use of "rsp" PASSporTs will not be possible. Note that the decision to trust any "div" or "rsp" PASSporT is, as always in STIR, a matter of local policy of the relying parties: some stricter systems may not want to trust any "rsp" that differs from the "dest" in the PASSporT of the original request.

Note that sending "div" PASSporTs in the backwards direction will potentially reveal service logic to the called party. As presumably this service logic is enacted on behalf of the called party, the called party can make a policy determination about reflecting those "div" PASSporTs back to the caller: connected identity may not be compatible with some operator policies.

This mechanism does not require altering the value of the From header field value in requests or responses in the backwards direction. While this was a major concern of [RFC4916], in many operating environments, the From header field value does not even contain the identity of the caller that has been asserted by the network, which is instead conveyed by the P-Asserted-Identity (PAID) header field [RFC3325]. The contents of PAID were never used for dialog matching, and so in environments where PAID is used, it can be altered more dynamically than the From (moreover, [RFC3261], by introducing tag parameters to the To and From header field values, eliminated the need for stability in From values for dialog identification some time ago). For retargeting that utilizes the [RFC4916] "from-change" option tag, see Section 10. STIR is, in general, more flexible in constructing the "dest" than the Identity header field managed addresses-of-record at the time [RFC4916] was written.

6. Connected Identity in Mid-Dialog and Dialog-Terminating Requests

The use of the connected identity mechanism here specified is not limited to provisional dialog requests. Once a dialog has been established with connected identity, any re-INVITEs from either the originating and terminating side, as well as any BYE requests, SHOULD contain Identity header fields with valid PASSporTs. If only the terminating side supports connected identity, obviously the originator cannot be expected to know that it needs to send PASSporTs for subsequent requests like BYE. Doing so prevents third parties from spoofing any mid-dialog requests in order to redirect media or similarly interfere with communications, as well as preventing denial of service teardowns by attackers.

Theoretically, any SIP requests in a dialog could be signed in this fashion, though it is unclear how valuable it would be for some (e.g., OPTIONS). Requests with specialized payloads such as INFO or MESSAGE, however, would require additional specification for how integrity protection for their bodies could be implemented. Some work has been done toward that for MESSAGE (see [RFC9475]). This specification thus does not recommend PASSporTs for any requests sent in a dialog other than INVITE, UPDATE, and BYE.

It might seem tempting to require that, if an INVITE has been sent with an Identity header field containing a PASSporT, any CANCEL request received for the dialog initiated by that INVITE must also contain an Identity header field with a PASSporT. However, CANCEL requests can also be sent by stateful proxy servers engaged in parallel forking; for example, when branches need to be canceled because a final response has been received from a UAS. This specification does not forbid a User Agent Client (UAC) from sending a CANCEL for its own PASSporT-protected INVITE requests, as there may be limited use cases where it would be useful to relying parties, but recipients of a CANCEL should not expect PASSporTs to be present in connected identity cases.

Mid-dialog requests also require special handling in diversion cases. Relying parties who intended to trust an "rsp" PASSporT MUST validate any "div" chain back to the "rsp" PASSporT on any Identity header field values received in responses (per [RFC8946]). The dialog initiator can then treat the certificate that signed that "rsp" PASSporT as the appropriate certificate to sign any further mid-dialog or dialog-terminating requests received in the backwards direction. Furthermore, the "dest" element value in any requests or responses sent in the backwards direction during this dialog MUST be the same as the "dest" element value in the first response to the dialog-forming request that contains a PASSporT -- unless the "from-change" extension is used, per Section 10.

7. Authorization Policy for Callers

In a traditional telephone call, the called party receives an alerting signal and can make a decision about whether or not to pick up a phone. They may have access to displayed information, like "Caller ID", to help them arrive at an authorization decision. The situation is more complicated for callers, however: callers typically expect to be connected to the proper destination and are often holding telephones in a position that would not enable them to see displayed information if any were available for them to review -- moreover, their most direct response to a security breach would be to hang up the call they were in the middle of placing.

While this specification does not prescribe any user experience associated with placing a call, it assumes that callers might have some way to a set an authorization posture that will result in the right thing happening when the connected identity is not as expected. This is analogous to a situation where Secure Real-time Protocol (SRTP) negotiation fails because the keys exchanged at the media layer do not match the fingerprints exchanged at the signaling layer: when a user requests confidentiality services, and they are unavailable, media should not be exchanged. Thus we assume that

users have a way in their interface to require this criticality, on a per-call basis, or perhaps on a per-destination basis. Users will not always place calls where the connected identity is crucial, but when they do, they should have a way to tell their devices that the call should not be completed if it arrives at an unexpected or unauthenticated party.

8. Creating Pre-Association with Destinations

Any connected identity mechanism will work best if the user knows before initiating a call that connected identity is supported by the destination side. Not every institution that a user wants to connect to securely will support STIR and connected identity out of the gate. Some sort of directory service might exist that advertises support for connected identity, which institutions then could use to inform potential callers that, if connected identity is not supported when reaching them with SIP, there is a potential security problem. Similarly, user devices might keep some sort of log recording that a destination previously supported connected identity, so that if support is unavailable later, calling users could be alerted to a potential security problem.

The user interface of modern smartphones support an address book from which users select telephone numbers to dial. Even when dialing a number manually, the interface frequently checks the address book, which will display to users any provisioned name for the target of the call if one exists. Similarly, when clicking on a telephone number viewed on a web page, or similar service, smartphones often prompt users approve the access to the outbound dialer. These sorts of decision points, when the user is still interacting with the user interface before a call is placed, provide an opportunity to probe what identity would be reached as a destination, and potentially even to exchange STIR PASSporTs in order to validate whether or not the expected destination can be reached securely. Again, this is probably most meaningful for contacting financial, government, or emergency services, for cases where reaching an unintended destination may have serious consequences.

The establishment of media-less dialogs has long been specified as a component of third-party call control in SIP [RFC3725], in which an INVITE is sent with no SDP. Similar media-less dialogs have been proposed for certain automated systems per [RFC5552]. In the STIR context, a media-less dialog is established by sending an INVITE with an Identity header field but no SDP. STIR-aware UASes that support this specification, upon receiving an INVITE with no SDP, carrying a PASSporT, with a 100rel in the Require header field value, SHOULD follow the mechanism described in Section 4 to send a provisional response carrying a PASSporT in the backwards direction. The PASSporT received in the backwards direction could be rendered to the originating user to help them decide if they want to place the call.

9. The 'rsp' PASSporT Type

This specification defines a "rsp" PASSporT type that is sent only in SIP responses; it MUST NOT be sent in SIP requests. Any "rsp" PASSporTs received in requests MUST be ignored.

The header of a "rsp" PASSporT shows a "ppt" of "rsp":

```
{ "typ":"passport",
  "ppt":"rsp",
  "alg":"ES256",
  "x5u":"https://www.example.com/cert.cer" }
```

The payload of an "rsp" PASSporT looks entirely like a normal PASSporT -- the only difference is in semantics, as the certificate signs for the "dest" header field rather than the "orig".

```
   { "orig":{"tn":"12155551212"},
     "dest":{"tn":["12155551214"]},
     "iat":1443208345 }
```

No restrictions are placed here on additional elements appearing in the payload of an "rsp" type PASSporT.

10. UPDATE Procedures for Provisional Dialogs

[RFC4916] identified a means of sending Identity header field values in the backwards direction before a final response to a dialog has been received by the UAC. It relied on negotiating support for "from-change" options tags on both sides, followed by the use of the UPDATE method to send the connected identity in the backwards direction. This can only happen after the UAS has received and responded to a PRACK [RFC3262] from the UAC, which would in turn have been triggered by a provisional 1xx response sent earlier by the UAC.

However, the complexity of this mechanism makes it impractical to deploy for both the primary use case and the diversion use case described above. It may still have utility for corner cases with legacy versions of SIP (that date before the addition of the To and From header field value tags) or more complex call parking scenarios. As such, this specification does not deprecate [RFC4916] "from-change" behavior, nor does it provide an update for it for STIR -- that is left for future work.

11. IANA Considerations

This specification defines a new PASSporT type for the "Personal Assertion Token (PASSporT) Extensions" registry defined in [RFC8225], which resides at https://www.iana.org/assignments/passport/:

ppt value "rsp"

Reference [RFCThis], Section 9

12. Privacy Considerations

Note that sending connected identity can reveal information about the called party. If a called party does not wish to be identified, it is especially important not to share rich call data (RCD) in the backwards direction, particular in business-to-consumer calling cases. From a user experience perspective, this would likely work similarly to current systems for sharing numbers, names, and even pictures from calling parties to called parties -- users have considerable control over that experience, and similarly for connected identity, this must be an opt-in choice for users. In general, RCD is more commonly used by enterprises than by individual users.

13. Security Considerations

The security considerations of [RFC8224] and [RFC8225] apply to the use of the "rsp" PASSporT. In general, a PASSporT of type "rsp" has similar security properties to a [RFC8946] diversion ("div") PASSporT. Relying parties leverage a "rsp" PASSporT to determine the recipient of a request, and as with "div," the "dest" element of an "rsp" PASSporT is signed, rather than the "orig" element.

The major threat that "rsp" addresses is the impersonation of a SIP response or mid-dialog/dialog-terminating request. For the latter, this might include forging a BYE for a denial-of-service attack, or, for example, forging a re-INVITE that negotiates media channels controlled by an attacker. For the former, some form of route hijacking or similar attack can be mounted by forging a dialog-

forming response that appears to the caller to initiate a dialog with the intended destination. The "rsp" mechanism uses PASSporTs to provide a non-repudiable assurance of the signer of such responses and requests.

The value of a "rsp" PASSporT to relying parties, as with all PASSporTs, depends on the relying party trusting the certificate that signs the PASSporT, and having a reasonable assurance that the certificate in question is eligible to sign responses/requests for the number in the "dest" field of the "rsp" PASSporT. For STIR certificates that use Service Provider Codes (SPCs), effectively the relying party knows the network operator who is vouching for that "rsp". This in turn enables traceback and similar mitigations.

As was mentioned in Section 5, the use of "div" along with "rsp" in responses may reveal the service logic of diversions to calling parties. However, since the called party ultimately invokes the "rsp" mechanism, any necessary policy controls can prevent the sending of "rsp" when that service logic must be protected.

The use of PASSporTs within responses creates a novel potential vector for amplification attacks, as many responses may be sent in response to a single SIP request, and the presence of a PASSporT meaningfully increases the size of SIP responses. However, given that PASSporTs can only be present in responses to requests carrying a PASSporT, and thus requests with strong sender authentication, called parties have adequate means to authorize the source of requests and disregard spoofs intended to trigger amplification attacks.

14. References

14.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <https://www.rfc-editor.org/info/rfc3261>.

[RFC3262] Rosenberg, J. and H. Schulzrinne, "Reliability of Provisional Responses in Session Initiation Protocol (SIP)", RFC 3262, DOI 10.17487/RFC3262, June 2002, <https://www.rfc-editor.org/info/rfc3262>.

[RFC3311] Rosenberg, J., "The Session Initiation Protocol (SIP) UPDATE Method", RFC 3311, DOI 10.17487/RFC3311, October 2002, <https://www.rfc-editor.org/info/rfc3311>.

[RFC3325] Jennings, C., Peterson, J., and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", RFC 3325, DOI 10.17487/RFC3325, November 2002, <https://www.rfc-editor.org/info/rfc3325>.

[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, DOI 10.17487/RFC3725, April 2004, <https://www.rfc-editor.org/info/rfc3725>.

[RFC4916] Elwell, J., "Connected Identity in the Session Initiation Protocol (SIP)", RFC 4916, DOI 10.17487/RFC4916, June 2007, <https://www.rfc-editor.org/info/rfc4916>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8224] Peterson, J., Jennings, C., Rescorla, E., and C. Wendt, "Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 8224, DOI 10.17487/RFC8224, February 2018, <https://www.rfc-editor.org/info/rfc8224>.

[RFC8225] Wendt, C. and J. Peterson, "PASSporT: Personal Assertion Token", RFC 8225, DOI 10.17487/RFC8225, February 2018, <https://www.rfc-editor.org/info/rfc8225>.

[RFC8862] Peterson, J., Barnes, R., and R. Housley, "Best Practices for Securing RTP Media Signaled with SIP", BCP 228, RFC 8862, DOI 10.17487/RFC8862, January 2021, <https://www.rfc-editor.org/info/rfc8862>.

[RFC8946] Peterson, J., "Personal Assertion Token (PASSporT) Extension for Diverted Calls", RFC 8946, DOI 10.17487/RFC8946, February 2021, <https://www.rfc-editor.org/info/rfc8946>.

14.2. Informative References

[RFC4474] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 4474, DOI 10.17487/RFC4474, August 2006, <https://www.rfc-editor.org/info/rfc4474>.

[RFC5552] Burke, D. and M. Scott, "SIP Interface to VoiceXML Media Services", RFC 5552, DOI 10.17487/RFC5552, May 2009, <https://www.rfc-editor.org/info/rfc5552>.

[RFC6116] Bradner, S., Conroy, L., and K. Fujiwara, "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)", RFC 6116, DOI 10.17487/RFC6116, March 2011, <https://www.rfc-editor.org/info/rfc6116>.

[RFC7340] Peterson, J., Schulzrinne, H., and H. Tschofenig, "Secure Telephone Identity Problem Statement and Requirements", RFC 7340, DOI 10.17487/RFC7340, September 2014, <https://www.rfc-editor.org/info/rfc7340>.

[RFC7375] Peterson, J., "Secure Telephone Identity Threat Model", RFC 7375, DOI 10.17487/RFC7375, October 2014, <https://www.rfc-editor.org/info/rfc7375>.

[RFC9475] Peterson, J. and C. Wendt, "Messaging Use Cases and Extensions for Secure Telephone Identity Revisited (STIR)", RFC 9475, DOI 10.17487/RFC9475, December 2023, <https://www.rfc-editor.org/info/rfc9475>.

Acknowledgments

We would like to thank Russ Housley, Jonathan Rosenberg, and Orie Steele for their contributions to this specification.

Authors' Addresses

Jon Peterson
TransUnion
Email: jon.peterson@transunion.com

Chris Wendt
Somos
Email: chris-ietf@chriswendt.net