Stream: Internet Engineering Task Force (IETF)
RFC: 9475
Category: Standards Track
Published: December 2023
ISSN: 2070-1721
Authors: J. Peterson *Neustar* C. Wendt *Somos*

RFC 9475
Messaging Use Cases and Extensions for Secure Telephone Identity Revisited (STIR)

Abstract

Secure Telephone Identity Revisited (STIR) provides a means of attesting the identity of a telephone caller via a signed token in order to prevent impersonation of a calling party number, which is a key enabler for illegal robocalling. Similar impersonation is sometimes leveraged by bad actors in the text and multimedia messaging space. This document explores the applicability of STIR's Personal Assertion Token (PASSporT) and certificate issuance framework to text and multimedia messaging use cases, including support for both messages carried as a payload in SIP requests and messages sent in sessions negotiated by SIP.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9475.

Copyright Notice

Table of Contents

1. Introduction

The STIR problem statement [RFC7340] describes widespread problems enabled by impersonation in the telephone network, including illegal robocalling, voicemail hacking, and swatting. As telephone services are increasingly migrating onto the Internet and using Voice over IP (VoIP) protocols such as SIP [RFC3261], it is necessary for these protocols to support stronger identity mechanisms to prevent impersonation. [RFC8224] defines a SIP Identity header capable of carrying PASSporT [RFC8225] objects in SIP as a means to cryptographically attest that the originator of a telephone call is authorized to use the calling party number (or, for SIP cases, SIP URI) associated with the originator of the call.

However, the problem of bulk, unsolicited commercial communications is not limited to telephone calls. Spammers and fraudsters are increasingly turning to messaging applications to deliver undesired content to consumers. In some respects, mitigating these unwanted messages resembles the email spam problem; for example, textual analysis of the message contents can be used to fingerprint content that is generated by spammers. However, encrypted messaging is becoming more common, and analysis of message contents may no longer be a reliable way to mitigate messaging spam in the future. As STIR sees further deployment in the telephone network, the governance structures put in place for securing telephone-network resources with STIR could be repurposed to help secure the messaging ecosystem.

One of the more sensitive applications for message security is emergency services. As next-generation emergency services increasingly incorporate messaging as a mode of communication with public safety personnel (see [RFC8876]), providing an identity assurance could help to mitigate denial-of-service attacks and ultimately help to identify the source of emergency communications in general (including swatting attacks, see [RFC7340]).

Therefore, this specification explores how the PASSporT mechanism defined for STIR could be applied in providing protection for textual and multimedia messaging, but it focuses particularly on those messages that use telephone numbers as the identity of the sender. Moreover, it considers the reuse of existing STIR certificates, which are beginning to see widespread deployment for signing PASSporTs that protect messages. For that purpose, it defines a new PASSporT type and an element that protects message integrity. It contains a mixture of normative and informative guidance that specifies new claims for use in PASSporTs as well as an overview of how STIR might be applied to messaging in various environments.

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.

3. Applicability to Messaging Systems

At a high level, PASSporT [RFC8225] claims provide similar value to number-based messaging as they do to telephone calls. A signature over the calling and called party numbers, along with a timestamp, could already help to prevent impersonation in the mobile-messaging ecosystem.

When it comes to protecting message contents, broadly, there are a few ways that the PASSporT mechanism of STIR could apply to messaging:

1. a PASSporT could be used to securely negotiate a session over which messages will be exchanged (see Section 3.1), and
2. in sessionless scenarios, a PASSporT could be generated on a per-message basis with its own built-in message security (see Section 3.2).

3.1. Message Sessions

In the first case, SIP negotiates a session in which the media will be text messages or MIME content, as, for example, with the Message Session Relay Protocol (MSRP) [RFC4975]. This usage of STIR would deviate little from [RFC8224]. An INVITE request sent with an Identity header containing a PASSporT with the proper calling and called party numbers would then negotiate an MSRP session the same way that an INVITE for a telephone call would negotiate an audio session. This could be applicable to MSRP sessions negotiated for Rich Communication Suite (RCS) [RCC.07]. Note that, if TLS is used to secure MSRP (per RCS [RCC.15]), fingerprints of those TLS keys could be secured via the "mky" claim of PASSporT using the framework described in [RFC8862]. Similar practices would apply to sessions that negotiate real-time text over RTP ([RFC4103], [RFC5194]); any that can operate over DTLS/SRTP (Secure Real-time Transport Protocol) should work with the "mky" PASSporT claim. For the most basic use cases, STIR for messaging should not require any further protocol enhancements.

Current usage of [RFC8224] Identity is largely confined to INVITE requests that initiate telephone calls. RCS-style applications would require PASSporTs for all conversation participants, which could become complex in multiparty conversations. Any solution in this space would likely require the implementation of STIR-connected identity [CONNECT-ID-STIR], but the specification of PASSporT-signed session conferencing is outside the scope of this document.

Also note that the assurance offered by [RFC8862] is "end-to-end" in the sense that it offers assurance between an authentication service and verification service. If those are not implemented by the endpoints themselves, there are still potential opportunities for tampering before messages are signed and after they are verified. However, for the most part, STIR does not intend to protect against machine-in-the-middle attacks so much as spoofed origination; so the protection offered may be sufficient to mitigate nuisance messaging.

3.2. PASSporTs and Individual Messages

In the second case described in Section 3, SIP also has a method for sending messages in the body of a SIP request: the MESSAGE method [RFC3428]. For example, MESSAGE is used in some North American emergency services use cases. The interaction of STIR with MESSAGE is not as straightforward as the potential use case with MSRP. An Identity header could be added to any SIP MESSAGE request, but without some extension to the PASSporT claims, the PASSporT would offer no protection to the message content; it would potentially be reusable for cut-and-paste attacks where the Identity header field from a legitimate request for one user is reused in a request for a different user. As the bodies of SIP requests are MIME encoded, S/MIME [RFC8591] has been proposed as a means of providing integrity for MESSAGE (and some MSRP cases as well). The use of Common Presence and Instant Messaging (CPIM) [RFC3862] as a MIME body allows the integrity of messages to withstand interworking with protocols that are not SIP. The interaction of STIR certificates with S/MIME (see [RFC8226]) for messaging applications would require further specification; additionally, PASSporT can provide its own integrity check for message contents through a new claim defined to provide a hash over message contents.

In order to differentiate a PASSporT for an individual message from a PASSporT used to secure a telephone call or message stream, this document defines a new "msg" PASSporT type. "msg" PASSporTs may carry a new optional JSON Web Token (JWT) [RFC7519] claim "msgi", which provides a digest over a MIME body that contains a text or multimedia message. Authentication services **MUST NOT** include "msgi" elements in PASSporT types other than "msg", but "msgi" is **OPTIONAL** in "msg" PASSporTs, as integrity for messages may be provided by some other service (e.g. [RFC8591]). Verification services **MUST** ignore the presence of "msgi" in non-"msg" PASSporT types.

The claim value of the "msgi" claim key is a string that defines the crypto algorithm used to generate the digest concatenated by a hyphen with a digest string. Implementations **MUST** support the hash algorithms SHA-256, SHA-384, and SHA-512. These hash algorithms are identified by "sha256", "sha384", and "sha512", respectively. SHA-256, SHA-384, and SHA-512 are part of the SHA-2 set of cryptographic hash functions [RFC6234] defined by the US National Institute of Standards and Technology (NIST). [SHA2] implementations **MAY** support additional recommended hash algorithms in the "COSE Algorithms" registry; that is, the hash algorithm has "Yes" in the "Recommended" column of the IANA registry. Hash algorithm identifiers **MUST** use only lowercase letters, and they **MUST NOT** contain hyphen characters. The character following the algorithm string **MUST** be a hyphen character ("-" or ASCII character 45).

The subsequent characters in the claim value are the base64-encoded [RFC4648] digest of a canonicalized and concatenated string or binary-data-based MIME body of the message. An "msgi" message digest is computed over the entirety of the MIME body (be it carried via SIP or not); per [RFC3428], this may be any sort of MIME body, including a multipart body in some cases, especially when multimedia content is involved. Those MIME bodies may or may not contain encrypted content or as the sender desires. The digest becomes the value of the JWT "msgi" claim, as per this example:

"msgi" : "sha256-H8BRh8j48O9oYatfu5AZzq6A9RINQZngK7T62em8MUt1FLm52t+eX6xO"

Per [RFC8224], this specification leaves it to local policy to determine how messages are handled after verification succeeds or fails. Broadly, if a SIP-based verification service wants to communicate back to the sender that the "msgi" hash does not correspond to the received message, using a SIP 438 response code would be most appropriate.

Note that, in some CPIM environments, intermediaries may add or consume CPIM headers used for metadata in messages. MIME-layer integrity protection of "msgi" would be broken by a modification along these lines. Any such environment would require a profile of this specification that reduces the scope of protection only to the CPIM payload, as discussed in Section 9.1 of [RFC8591].

Finally, note that messages may be subject to store-and-forward treatment that differs from delivery expectations of SIP transactions. In such cases, the expiry freshness window recommended by [RFC8224] may be too strict, as routine behavior might dictate the delivery of a MESSAGE minutes or hours after it was sent. The potential for replay attacks can, however, be largely mitigated by the timestamp in PASSporTs; duplicate messages are easily detected, and the timestamp can be used to order messages displayed in the user inbox in a way that precludes showing stale messages as fresh. Relaxing the expiry timer would require support for such features on the receiving side of the message.

3.2.1. PASSporT Conveyance with Messaging

If the message is being conveyed in SIP, via the MESSAGE method, then the PASSporT could be conveyed in an Identity header in that request. The authentication and verification service procedures for populating that PASSporT would follow the guidance in [RFC8224], with the addition of the "msgi" claim defined in Section 3.2.

In text messaging today, Multimedia Messaging Service (MMS) messages are often conveyed with SMTP. Thus, there is a suite of additional email security tools available in this environment for sender authentication, such as "Domain-based Message Authentication, Reporting, and Conformance (DMARC)" [RFC7489]. The interaction of these mechanisms with STIR certificates and/or PASSporTs would require further study and is outside the scope of this document.

For other cases where messages are conveyed by some protocol other than SIP, that protocol itself might have some way of conveying PASSporTs. There will surely be cases where legacy transmission of messages will not permit an accompanying PASSporT; in such a situation, something like out-of-band [RFC8816] conveyance would be the only way to deliver the PASSporT. For example, this may be necessary to support cases where legacy Short Message Peer-to-Peer [SMPP] systems cannot be upgraded.

A MESSAGE request can be sent to multiple destinations in order to support multiparty messaging. In those cases, the "dest" claim of the PASSporT can accommodate the multiple targets of a MESSAGE without the need to generate a PASSporT for each target of the message. However, if the request is forked to multiple targets by an intermediary later in the call flow, and the list of targets is not available to the authentication service, then that forking intermediary would need to use diversion PASSporTs [RFC8946] to sign for its target set.

4. Certificates and Messaging

"Secure Telephone Identity Credentials: Certificates" [RFC8226] defines a way to issue certificates that sign PASSporTs, which attest through their TNAuthList a Service Provider Code (SPC) and/or a set of one or more telephone numbers. This specification proposes that the semantics of these certificates should suffice for signing for messages from a telephone number without further modification.

Note that the certificate referenced by the "x5u" of a PASSporT can change over time due to certificate expiry/rollover; in particular, the use of short-lived certificates can entail rollover on a daily basis or even more frequently. Thus, any store-and-forward messaging system relying on

PASSporTs must take into account the possibility that the certificate that signed the PASSporT, though valid at the time the PASSporT was generated, could expire before a user reads the message. This might require:

- storing some indicator of the validity of the signature and certificate at the time the message was received, or
- securely storing the certificate along with the PASSporT

so that the "iat" claim can be compared with the expiry freshness window of the certificate prior to validation.

As the "orig" and "dest" claims of PASSporTs may contain URIs without telephone numbers, the STIR for messaging mechanism contained in this specification is not inherently restricted to the use of telephone numbers. This specification offers no guidance on appropriate certification authorities for designing "orig" values that do not contain telephone numbers.

5. IANA Considerations

5.1. JSON Web Token Claims Registration

IANA has added one new claim to the "JSON Web Token Claims" registry that was defined in [RFC7519].

Claim Name: msgi

Claim Description: Message Integrity Information

Change Controller: IETF

Specification Document(s): RFC 9475

5.2. PASSporT Type Registration

This specification defines one new PASSporT type for the "Personal Assertion Token (PASSporT) Extensions" registry defined in [RFC8225].

ppt value: msg

Reference: Section 3.2 of RFC 9475

6. Privacy Considerations

Signing messages or message sessions with STIR has little direct bearing on the privacy of messaging for SIP as described in [RFC3428] or [RFC4975]. An authentication service signing a MESSAGE method may compute the "msgi" hash over the message contents; if the message is in cleartext, that will reveal its contents to the authentication service, which might not otherwise be in the call path.

The implications for anonymity of STIR are discussed in [RFC8224], and those considerations would apply equally here for anonymous messaging. Creating an "msg" PASSporT does not add any additional privacy protections to the original message content.

7. Security Considerations

This specification inherits the security considerations of [RFC8224]. The carriage of messages within SIP per Section 3.2 has a number of security and privacy implications as documented in [RFC3428], which are expanded in [RFC8591]; these considerations apply here as well. The guidance about store-and-forward messaging and replay protection in Section 3.2 should also be recognized by implementers.

Note that a variety of protocols that are not SIP, both those integrated into the telephone network and those based on over-the-top applications, are responsible for most of the messaging that is sent to and from telephone numbers today. Introducing this capability for SIP-based messaging will help to mitigate spoofing and nuisance messaging for SIP-based platforms only.

8. References

8.1. 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>.

[RFC3428] Campbell, B., Ed., Rosenberg, J., Schulzrinne, H., Huitema, C., and D. Gurle, "Session Initiation Protocol (SIP) Extension for Instant Messaging", RFC 3428, DOI 10.17487/RFC3428, December 2002, <https://www.rfc-editor.org/info/rfc3428>.

[RFC3862] Klyne, G. and D. Atkins, "Common Presence and Instant Messaging (CPIM): Message Format", RFC 3862, DOI 10.17487/RFC3862, August 2004, <https://www.rfc-editor.org/info/rfc3862>.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <https://www.rfc-editor.org/info/rfc4648>.

[RFC6234] Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", RFC 6234, DOI 10.17487/RFC6234, May 2011, <https://www.rfc-editor.org/info/rfc6234>.

[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>.

[RFC8226] Peterson, J. and S. Turner, "Secure Telephone Identity Credentials: Certificates", RFC 8226, DOI 10.17487/RFC8226, February 2018, <https://www.rfc-editor.org/info/rfc8226>.

8.2. Informative References

[CONNECT-ID-STIR] Peterson, J. and C. Wendt, "Connected Identity for STIR", Work in Progress, Internet-Draft, draft-ietf-stir-rfc4916-update-04, 23 October 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-stir-rfc4916-update-04>.

[RCC.07] GSMA, "Rich Communication Suite 8.0 Advanced Communications Services and Client Specification", Version 9.0, May 2018, <https://www.gsma.com/futurenetworks/wp-content/uploads/2019/09/RCC.07-v9.0.pdf>.

[RCC.15] GSMA, "IMS Device Configuration and Supporting Services", Version 7.0, October 2019, <https://www.gsma.com/newsroom/wp-content/uploads//RCC.15-v7.0.pdf>.

[RFC4103] Hellstrom, G. and P. Jones, "RTP Payload for Text Conversation", RFC 4103, DOI 10.17487/RFC4103, June 2005, <https://www.rfc-editor.org/info/rfc4103>.

[RFC4975] Campbell, B., Ed., Mahy, R., Ed., and C. Jennings, Ed., "The Message Session Relay Protocol (MSRP)", RFC 4975, DOI 10.17487/RFC4975, September 2007, <https://www.rfc-editor.org/info/rfc4975>.

[RFC5194] van Wijk, A., Ed. and G. Gybels, Ed., "Framework for Real-Time Text over IP Using the Session Initiation Protocol (SIP)", RFC 5194, DOI 10.17487/RFC5194, June 2008, <https://www.rfc-editor.org/info/rfc5194>.

[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>.

[RFC7489] Kucherawy, M., Ed. and E. Zwicky, Ed., "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", RFC 7489, DOI 10.17487/RFC7489, March 2015, <https://www.rfc-editor.org/info/rfc7489>.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <https://www.rfc-editor.org/info/rfc7519>.

[RFC8591] Campbell, B. and R. Housley, "SIP-Based Messaging with S/MIME", RFC 8591, DOI 10.17487/RFC8591, April 2019, <https://www.rfc-editor.org/info/rfc8591>.

[RFC8816] Rescorla, E. and J. Peterson, "Secure Telephone Identity Revisited (STIR) Out-of-Band Architecture and Use Cases", RFC 8816, DOI 10.17487/RFC8816, February 2021, <https://www.rfc-editor.org/info/rfc8816>.

[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>.

[RFC8876] Rosen, B., Schulzrinne, H., Tschofenig, H., and R. Gellens, "Non-interactive Emergency Calls", RFC 8876, DOI 10.17487/RFC8876, September 2020, <https://www.rfc-editor.org/info/rfc8876>.

[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>.

[SHA2] National Institute of Standards and Technology (NIST), "Secure Hash Standard (SHS)", FIPS PUB 180-3, 2008, <http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf>.

[SMPP] SMS Forum, "Short Message Peer-to-Peer Protocol Specification", Version 5.0, February 2003, <https://smpp.org/SMPP_v5.pdf>.

Acknowledgments

We would like to thank Christer Holmberg, Brian Rosen, Ben Campbell, Russ Housley, and Alex Bobotek for their contributions to this specification.

Authors' Addresses

Jon Peterson
Neustar, Inc.
Email: jon.peterson@team.neustar

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