

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 13, 2022

J. Peterson
Neustar
C. Wendt
Somos
November 9, 2021

Messaging Use Cases and Extensions for STIR
draft-ietf-stir-messaging-01

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 messaging space. This document considers the applicability of STIR's Persona Assertion Token (PASSporT) and certificate issuance framework to text and multimedia messaging use cases, both for instant messages carried or negotiated by SIP.

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 May 13, 2022.

Copyright Notice

Copyright (c) 2021 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents

carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	2
2. Terminology	3
3. Applicability to Messaging Systems	3
3.1. Message Sessions	4
3.2. PASSporTs and Messaging	4
3.2.1. PASSporT Conveyance with Messaging	5
4. Certificates and Messaging	6
5. Acknowledgments	6
6. IANA Considerations	6
6.1. JSON Web Token Claims Registration	6
6.2. PASSporT Type Registration	7
7. Privacy Considerations	7
8. Security Considerations	7
9. References	7
9.1. Normative References	8
9.2. Informative References	9
Authors' Addresses	10

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 field 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 native SIP cases, SIP URI) associated with the originator of the call.

The problem of bulk, unsolicited commercial communications is not however limited to telephone calls. Although the problem is not currently widespread, spammers and fraudsters are turning to messaging applications to deliver undesired content to consumers. In some respects, mitigating these unwanted messages resembles the email spam problem: textual analysis of the message contents can be used to fingerprint content that is generated by spammers, for example. 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. And 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, as well as ultimately helping to identify the source of emergency communications in general (including swatting attacks, see [RFC7340]).

This specification therefore explores how the PASSporT mechanism defined for STIR could be applied to providing protection for textual and multimedia messaging, but focuses particularly on those messages that use telephone numbers as the identity of the sender. It moreover considers the reuse of existing STIR certificates, which are beginning to see widespread deployment, for signing PASSporTs that protect messages.

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, baseline PASSporT [RFC8225] claims provide similar value to number-based messaging as they do to traditional 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: first, a PASSporT could be used to securely negotiate a session over which messages will be exchanged; and second, in sessionless scenarios, a PASSporT could be generated on a per-message basis with its own built-in message security.

3.1. Message Sessions

For the first case, where SIP negotiates a session where the media will be text messages, as for example with the Message Session Relay Protocol (MSRP) [RFC4975], the 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 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 [RFC8862] framework. Similar practices would apply to sessions that negotiate text over RTP via [RFC4103] or similar mechanisms. Messages can also be sent over a variety of other transports negotiated by SIP (including for example Real-Time Text [RFC5194]; any that can operate over DTLS/SRTP 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 baseline [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 multi-party conversations. Any solution in this space would likely require the implementation of STIR connected identity [I-D.peterson-stir-rfc4916-update], 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. For the most part, STIR does not intend to protect against man-in-the-middle attacks so much as spoofed origination, however, so the protection offered may be sufficient to mitigate nuisance messaging.

3.2. PASSporTs and Messaging

In the second case, SIP also has a method for sending messages in the body of a SIP request: the MESSAGE [RFC3428] method. MESSAGE is used for example 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, and potentially be reusable for cut-and-paste attacks. 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 CPIM [RFC3862] as a MIME body allows the integrity of messages to withstand interworking with non-SIP protocols. The interaction of [RFC8226] STIR certificates with S/MIME for messaging applications requires some further explication; and 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 JWT [RFC7519] claim "msgi" which provides a digest over a MIME body that contains a text or multimedia message. "msgi" MUST NOT appear in PASSporTs with a type other than "msg", but they are OPTIONAL in "msg" PASSporTs, as integrity for messages may be provided by some other service (e.g. [RFC8591]). Implementations of "msgi" MUST support the following hash algorithms: "SHA256", "SHA384", or "SHA512", which are defined as part of the SHA-2 set of cryptographic hash functions by the NIST.

A "msgi" message digest is computed over the entire MIME body of a SIP message, which per [RFC3428] may any sort of MIME body, including a multipart body in some cases, especially when multimedia content is involved. The digest becomes the value of the JWT "msgi" claim, as per this example:

```
"msgi" :  
"sha256-H8BRh8j48O9oYatfu5AZzq6A9RINQZngK7T62em8MUt1FLm52t+eX6xO"
```

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 field in that request. The authentication and verification service procedures for populating that PASSporT would follow [RFC8224], with the addition of the "msgi" claim defined in Section 3.2.

In text messaging today, multimedia message system (MMS) messages are often conveyed with SMTP. There are thus a suite of additional email security tools available in this environment for sender authentication, such as 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 might itself have some way of conveying PASSporTs. But there will surely be cases where legacy transmission of messages will not permit an accompanying PASSporT, in which case something like out-of-band [RFC8816] conveyance would be the only way to deliver the PASSporT. This may be necessary to support cases where legacy SMPP systems cannot be upgraded, for example.

A MESSAGE request can be sent to multiple destinations in order to support multiparty messaging. In those cases, the "dest" field of the PASSporT can accommodate the multiple targets of a MESSAGE without the need to generate a PASSporT for each target of the message. If however 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 [RFC8946] PASSporTs to sign for its target set.

4. Certificates and Messaging

The [RFC8226] STIR certificate profiles 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.

As the "orig" and "dest" field of PASSporTs may contain URIs containing SIP 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 certification authorities who are appropriate to sign for non-telephone number "orig" values.

5. Acknowledgments

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

6. IANA Considerations

6.1. JSON Web Token Claims Registration

This specification requests that the IANA add one new claim to the JSON Web Token Claims registry as defined in [RFC7519].

Claim Name: "msgi"

Claim Description: Message Integrity Information

Change Controller: IESG

Specification Document(s): [RFCThis]

6.2. PASSporT Type Registration

This specification defines one new PASSporT type for the PASSport Extensions Registry defined in [RFC8225], which resides at <https://www.iana.org/assignments/passport/passport.xhtml#passport-extensions>. It is:

"msg" as defined in [RFCThis] Section 3.2.

7. 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.

8. 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 well.

Note that a variety of non-SIP protocols, both those integrated into the traditional 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.

9. References

9.1. 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>>.
- [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>>.
- [RFC7159] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", RFC 7159, DOI 10.17487/RFC7159, March 2014, <<https://www.rfc-editor.org/info/rfc7159>>.
- [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>>.

9.2. Informative References

- [I-D.peterson-stir-rfc4916-update] Peterson, J. and C. Wendt, "Connected Identity for STIR", draft-peterson-stir-rfc4916-update-04 (work in progress), July 2021.
- [RCC.07] GSMA RCC.07 v9.0 | 16 May 2018, "Rich Communication Suite 8.0 Advanced Communications Services and Client Specification", 2018.
- [RCC.15] GSMA PRD-RCC.15 v5.0 | 16 May 2018, "IMS Device Configuration and Supporting Services", 2018.
- [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>>.
- [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>>.
- [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>>.
- [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>>.

Authors' Addresses

Jon Peterson
Neustar, Inc.

Email: jon.peterson@team.neustar

Chris Wendt
Somos

Email: chris-ietf@chriswendt.net

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 28 April 2022

C. Wendt
Comcast
J. Peterson
Neustar Inc.
25 October 2021

PASSport Extension for Rich Call Data
draft-ietf-stir-passport-rcd-14

Abstract

This document extends PASSport, a token for conveying cryptographically-signed call information about personal communications, to include rich meta-data about a call and caller that can be signed and integrity protected, transmitted, and subsequently rendered to the called party. This framework is intended to include and extend caller and call specific information beyond human-readable display name comparable to the "Caller ID" function common on the telephone network. The JSON element defined for this purpose, Rich Call Data (RCD), is an extensible object defined to either be used as part of STIR or with SIP Call-Info to include related information about calls that helps people decide whether to answer an incoming set of communications from another party. This signing of the RCD information is also enhanced with a integrity mechanism that is designed to protect the authoring and transport of this information between authoritative and non-authoritative parties generating and signing the Rich Call Data for support of different usage and content policies.

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 28 April 2022.

Copyright Notice

Copyright (c) 2021 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	3
2. Terminology	4
3. Overview of the use of the Rich Call Data PASSporT extension	4
4. Overview of Rich Call Data Integrity	5
5. PASSporT Claim "rcd" Definition and Usage	7
5.1. PASSporT "rcd" Claim	7
5.1.1. "nam" key	7
5.1.2. "apn" key	8
5.1.3. "jcd" key	8
5.1.4. "jcl" key	9
6. "rcdi" RCD Integrity Claim Definition and Usage	9
6.1. Creation of the "rcd" element digests	10
6.2. JWT Claim Constraints for "rcd" claims only	13
7. JWT Claim Constraints usage for "rcd" and "rcdi" claims	14
8. PASSporT "crn" claim - Call Reason Definition and Usage	15
8.1. JWT Constraint for "crn" claim	15
9. Rich Call Data Claims Usage Rules	15
9.1. Verification rules	16
9.2. Example "rcd" PASSporTs	16
10. Compact form of "rcd" PASSporT	18
10.1. Compact form of the "rcd" PASSporT claim	18
10.2. Compact form of the "rcdi" PASSporT claim	19
10.3. Compact form of the "crn" PASSporT claim	19
11. Further Information Associated with Callers	19
12. Third-Party Uses	20
12.1. Signing as a Third Party	21
13. Levels of Assurance	22
14. Using "rcd" in SIP	22
14.1. Authentication Service Behavior	22
14.2. Verification Service Behavior	23

15. Using "rcd" as additional claims to other PASSporT extensions	24
15.1. Procedures for applying "rcd" as claims only	25
15.2. Example for applying "rcd" as claims only	25
16. Acknowledgements	26
17. IANA Considerations	26
17.1. JSON Web Token Claim	26
17.2. PASSporT Types	27
17.3. PASSporT RCD Types	27
18. Security Considerations	27
18.1. The use of JWT Claim Constraints in delegate certificates to exclude unauthorized claims	28
19. References	28
19.1. Normative References	28
19.2. Informative References	30
Authors' Addresses	31

1. Introduction

PASSporT [RFC8225] is a token format based on JWT [RFC7519] for conveying cryptographically-signed information about the parties involved in personal communications; it is used to convey a signed assertion of the identity of the participants in real-time communications established via a protocol like SIP [RFC8224]. The STIR problem statement [RFC7340] declared securing the display name of callers outside of STIR's initial scope, so baseline STIR provides no features for caller name. This specification documents an optional mechanism for PASSporT and the associated STIR procedures which extend PASSporT objects to protect additional elements conveying richer information: information that is intended to be rendered to assist a called party in determining whether to accept or trust incoming communications. This includes the name of the person or entity on one side of a communications session, the traditional "Caller ID" of the telephone network, along with related display information that would be rendered to the called party during alerting, or potentially used by an automaton to determine whether and how to alert a called party.

Traditional telephone network signaling protocols have long supported delivering a 'calling name' from the originating side, though in practice, the terminating side is often left to derive a name from the calling party number by consulting a local address book or an external database. SIP similarly can carry this information in a 'display-name' in the From header field value from the originating to terminating side, or alternatively in the Call-Info header field. However, both are unsecured fields that really cannot be trusted in most interconnected SIP deployments, and therefore is a good starting point for a framework that utilizes STIR techniques and procedures for protecting call related information including but not limited to calling name.

As such, the baseline use-case for this document extends PASSporT to provide cryptographic protection for the "display-name" field of SIP requests as well as further "rich call data" (RCD) about the caller, which includes the contents of the Call-Info header field or other data structures that can be added to the PASSporT. This document furthermore specifies a third-party profile that would allow external authorities to convey rich information associated with a calling number via a new type of PASSporT. Finally, this document describes how to preserve the integrity of the RCD in scenarios where there may be non-authoritative users initiating and signing RCD and therefore a constraint on the RCD data that a PASSporT can attest via certificate-level controls.

2. Terminology

The keywords "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. Overview of the use of the Rich Call Data PASSporT extension

The main intended use of the signing of Rich Call Data (RCD) using STIR within SIP [RFC8224] or more generally as a PASSporT extension [RFC8225] is for the entity that originates a call, either directly the caller themselves, if they are authoritative, or a service provider or third-party service that may be authoritative over the rich call data on behalf of the caller.

The RCD associated with the identity of the calling party described in this document is of two main categories. The first data is a more traditional set of info about a caller associated with "display-name" in SIP [RFC3261], typically a textual description of the caller, or alternate presentation numbers often used in From Header field

[RFC3261] or P-Asserted-ID [RFC3325]. The second category is a set of RCD that is defined as part of the jCard definitions or extensions to that data. [I-D.ietf-sipcore-callinfo-rcd] describes the optional use of jCard in Call-Info header field as RCD with the "jcard" Call-Info purpose token. Either or both of these two types of data can be incorporated into a "rcd" claim defined in this document.

Additionally, in relation to the description of the specific communications event itself (versus the identity description in previous paragraph), [I-D.ietf-sipcore-callinfo-rcd] also describes a "call-reason" parameter intended for description of the intent or reason for a particular call. A new PASSporT claim "crn", or call reason, can contain the string or object that describes the intent of the call. This claim is intentionally kept separate from the "rcd" claim because it is envisioned that call reason is not the same as information associated with the caller and may change on a more frequent, per call, type of basis.

4. Overview of Rich Call Data Integrity

When incorporating call data that represents a user, even in traditional calling name services today, often there is policy and restrictions around what data is allowed to be used. Whether preventing offensive language or icons or enforcing uniqueness, potential trademark or copyright violations or other policy enforcement, there might be the desire to pre-certify or "vet" the specific use of rich call data. This document defines a mechanism that allows for a direct or indirect party that controls the policy to approve or certify the content, create a cryptographic digest that can be used to validate that data and applies a constraint in the certificate to allow the recipient and verifier to validate that the specific content of the RCD is as intended at its creation and approval or certification.

There are two mechanisms that are defined to accomplish that for two distinct categories of purposes. The first of the mechanisms include the definition of an integrity claim. The RCD integrity mechanism is a process of generating a sufficiently strong cryptographic digest for both the "rcd" claim contents (e.g. "nam", "jcd", "jcl") defined below and the resources defined by one or more globally unique HTTPS URLs referenced by the contents (e.g. an image file referenced by "jcd" or a jCard referenced by "jcl"). This mechanism is inspired by and based on the W3C Subresource Integrity specification (<http://www.w3.org/TR/SRI/>). The second of the mechanisms uses the capability called JWT Claim Constraints, defined in [RFC8226] and extended in [I-D.ietf-stir-enhance-rfc8226]. The JWT Claim Constraints specifically guide the verifier within the certificate used to sign the PASSporT for the inclusion (or exclusion) of specific claims and their values, so that the content intended by the signer can be verified to be accurate.

Both of these mechanisms, integrity digests and JWT Claims Constraints, can be used together or separately depending on the intended purpose. The first category of purpose is whether the rich call data conveyed by the RCD passport is pass-by-value or passed-by-reference; i.e., is the information contained in the passport claims and therefore integrity protected by the passport signature, or is the information contained in an external resource referenced by a URI in the RCD PASSporT. The second category of purpose is whether the signer is authoritative or has responsibility for the accuracy of the RCD based on the policies of the eco-system the RCD PASSporTs are being used.

The following table provides an overview of the framework for how integrity should be used with RCD. (Auth represents authoritative in this table)

Modes	No external URIs	Includes URI refs
Auth	1: No integrity req	2: RDC Integrity
Non-Auth	3: JWT Claim Const.	4: RCD Integ./JWT Claim Const.

The first and simplest mode is exclusively for when all RCD content is directly included as part of the claims (i.e. no external reference URIs are included in the content) and when the signer is authoritative over the content. In this mode, integrity protection is not required and the set of claims is simply protected by the signature of the standard PASSporT [RFC8225] and SIP identity header [RFC8224] procedures. The second mode is an extension of the first

where the signer is authoritative and a "rcd" claim contents include a URI identifying external resources. In this mode, an RCD Integrity or "rcdi" claim MUST be included. This integrity claim is defined later in this document and provides a digest of the "rcd" claim content so that, particularly for the case where there are URI references in the RCD, the content of that RCD can be comprehensively validated that it was received as intended by the signer of the PASSporT.

The third and fourth mode cover cases where there is a different authoritative entity responsible for the content of the RCD, separate from the signer of the PASSporT itself, allowing the ability to have forward control at the time of the creation of the certificate of the allowed or vetted content included in or referenced by the RCD claim contents. The primary framework for allowing the separation of authority and the signing of PASSporTs by non-authorized entities is detailed in [I-D.ietf-stir-cert-delegation] although other cases may apply. As with the first and second modes, the third and fourth modes differ with the absence or inclusion of externally referenced content using URIs.

5. PASSporT Claim "rcd" Definition and Usage

5.1. PASSporT "rcd" Claim

This specification defines a new JSON Web Token claim for "rcd", Rich Call Data, the value of which is a JSON object that can contain one or more key value pairs. This document defines a default set of key values.

5.1.1. "nam" key

The "nam" key value is a display name, associated with the originator of personal communications, which may for example derive from the display-name component of the From header field value of a SIP request or alternatively from the P-Asserted-Identity header field value, or a similar field in other PASSporT using protocols. This key MUST be included once as part of the "rcd" claim value JSON object. If there is no string associated with a display name, the claim value MUST then be an empty string.

5.1.2. "apn" key

The "apn" key value is an optional alternate presentation number associated with the originator of personal communications, which may for example derive from the user component of the From header field value of a SIP request (in cases where a network number is carried in the P-Asserted-Identity [RFC3325]), or alternatively from the Additional-Identity header field value [3GPP TS 24.229 v16.7.0], or a similar field in other PASSporT using protocols. Its intended semantics are to convey a number that the originating user is authorized to show to called parties in lieu of their default number, such as cases where a remote call agent uses the main number of a call center instead of their personal telephone number. The "apn" key value is a canonicalized telephone number per [RFC8224] Section 8.3. If present, this key MUST be included once as part of the "rcd" claim value JSON object.

The use of the optional "apn" key is intended for cases where the signer of an rcd PASSporT authorizes the use of an alternate presentation number by the user. How the signer determines that a user is authorized to present the number in question is a policy decision outside the scope of this document, however, the vetting of the alternate presentation number should follow the same level of vetting as telephone identities or any other information contained in an RCD PASSporT. This usage is intended as an alternative to conveying the presentation number in the "tel" key value of a jCard, in situations where no other rich jCard data needs to be conveyed with the call. Only one "apn" key may be present. "apn" MUST be used when it is the intent of the caller or signer to display the alternate presentation number even if "jcd" or "jcl" keys are present in a PASSporT with a "tel" key value.

5.1.3. "jcd" key

The "jcd" key value is defined to contain a jCard [RFC7095] JSON object. This jCard object is intended to represent and derives from the Call-Info header field value defined in [I-D.ietf-sipcore-callinfo-rcd] with a type of "jcard". As also defined in [I-D.ietf-sipcore-callinfo-rcd], format of the jCard and properties used should follow the normative usage and formatting rules and procedures. It is an extensible object where the calling party can provide both the standard types of information defined in jCard or can use the built-in extensibility of the jCard specification to add additional information. The "jcd" key is optional. If included, this key MUST only be included once in the "rcd" JSON object and MUST NOT be included if there is a "jcl" key included. The use of "jcd" and "jcl" keys are mutually exclusive.

The jCard object value for "jcd" MUST only have referenced content for URI values that do not further reference URIs. Future specifications may extend this capability, but as stated in [I-D.ietf-sipcore-callinfo-rcd] it constrains the security properties of RCD information and the integrity of the content referenced by URIs.

Note: even though we refer to [I-D.ietf-sipcore-callinfo-rcd] as the definition of the jcard properties for usage in a "rcd" PASSporT, other protocols can be adapted for use of "jcd" (or similarly "jcl" below) key beyond SIP and Call-Info.

5.1.4. "jcl" key

The "jcl" key value is defined to contain a HTTPS URL that refers the recipient to a jCard [RFC7095] JSON object hosted on a HTTPS enabled web server. The web server MUST use the MIME media type for JSON text as application/json with a default encoding of UTF-8 [RFC4627]. This link may derive from the Call-Info header field value defined in [I-D.ietf-sipcore-callinfo-rcd] with a type of "jcard". As also defined in [I-D.ietf-sipcore-callinfo-rcd], format of the jCard and properties used should follow the normative usage and formatting rules and procedures. The "jcl" key is optional. If included, this key MUST only be included once in the "rcd" JSON object and MUST NOT be included if there is a "jcd" key included. The use of "jcd" and "jcl" keys are mutually exclusive.

The jCard object referenced by the URI value for "jcl" MUST only have referenced content for URI values that do not further reference URIs. Future specifications may extend this capability, but as stated in [I-D.ietf-sipcore-callinfo-rcd] it constrains the security properties of RCD information and the integrity of the content referenced by URIs.

6. "rcdi" RCD Integrity Claim Definition and Usage

The "rcdi" claim is included for the second and fourth modes described in integrity overview section of this document. If this claim is present it MUST be only included once with the corresponding single "rcd" claim. The value of the "rcdi" claim is a JSON object that is defined as follows.

The claim value of "rcdi" claim key is a JSON object with a set of JSON key/value pairs. These objects correspond to each of the elements of the "rcd" claim object that require integrity protection with an associated digest over the content referenced by the key string. The individual digest of different elements of the "rcd" claim data and external URI referenced content is kept specifically

separate to allow the ability to verify the integrity of only the elements that are ultimately retrieved or downloaded or rendered to the end-user.

The key value references a specific object within the "rcd" claim value using a JSON pointer defined in [RFC6901] with a minor additional rule to support external URI references that include JSON objects themselves, for the specific case of the use of "jcl". JSON pointer syntax is the key value that specifies exactly the part of JSON that is used to generate the digest which produce the resulting string that makes up the value for the corresponding key. Detailed procedures are provided below, but an example "rcdi" is provided here:

```
"rcdi" : {  
  "/jcd": "sha256-7kdCBZqH0nqMSPsmABvsKlHPhZESTgjojhdSJGRr3rk",  
  "/jcd/1/2/3": "sha256-jL4f47fF82LuwcrOrSyckA4SWr1ElfARHkW6kYo1JdI"  
}
```

The values of each key pair are a digest combined with a string that defines the crypto algorithm used to generate the digest. RCD implementations MUST support the following hash algorithms, "SHA256", "SHA384", and "SHA512". The SHA-256, SHA-384, and SHA-512 are part of the SHA-2 set of cryptographic hash functions defined by the National Institute of Standards and Technologies (NIST). Implementations MAY support additional algorithms, but MUST NOT support known weak algorithms such as MD5 or SHA-1. In the future, the list of algorithms may be re-evaluated based on security best practices. The algorithms are represented in the text by "sha256", "sha384", or "sha512". The character following the algorithm string MUST be a minus character, "-". The subsequent characters are the base64 encoded [RFC4648] digest of a canonicalized and concatenated string or binary data based on the JSON pointer referenced elements of "rcd" claim or the URI referenced content contained in the claim. The details of the determination of the input string used to determine the digest are defined in the next section.

6.1. Creation of the "rcd" element digests

"rcd" claim objects can contain "nam", "apn", "jcd", or "jcl" keys as part of the "rcd" JSON object claim value. This specification defines the use of JSON pointer [RFC6901] as a mechanism to reference specific "rcd" claim elements.

In the case of "nam", the only allowed value is a "string". In order to reference the "nam" string value for a digest, the JSON pointer string would be "/nam" and the digest string would be created using only the string pointed to by that "/nam" following the rules of JSON pointer.

In the case of "apn", the only allowed value is a "string". In order to reference the "apn" string value for a digest, the JSON pointer string would be "/apn" and the digest string would be created using only the string pointed to by that "/apn" following the rules of JSON pointer.

In the case of "jcd", the value associated is a jCard JSON object, which happens to be a JSON array with sub-arrays. JSON pointer notation uses numeric indexes into elements of arrays, including when those elements are arrays themselves.

As example, for the following "rcd" claim:

```
"rcd": {
  "nam": "Q Branch Spy Gadgets",
  "jcd": ["vcard",
    [ ["version", {}, "text", "4.0"],
      [fn, {}, "text", "Q Branch"],
      [org, {}, "text", "MI6;Q Branch Spy Gadgets"],
      ["photo", {}, "uri",
        "https://example.com/photos/quartermaster-256x256.png"],
      ["logo", {}, "uri",
        "https://example.com/logos/mi6-256x256.jpg"],
      ["logo", {}, "uri",
        "https://example.com/logos/mi6-64x64.jpg"]
    ]
  ]
}
```

In order to use JSON pointer to refer to the URIs, the following example "rcdi" claim includes a digest for the entire "jcd" array string as well as three additional digests for the URIs, where, as defined in [RFC6901] zero-based array indexes are used to reference the URI strings.

```
"rcdi": {
  "/jcd": "sha256-7kdCBZqH0nqMSPsmABvsKlHPhzESTgjojhdsJGRr3rk",
  "/jcd/1/3/3": "sha256-RojgWwU6xUtI4q82+kHPyHm1JKbm7+663bMvzymhk14",
  "/jcd/1/4/3": "sha256-jL4f47fF82LuwcrOrSyckA4SWr1ElfARHkW6kYo1JdI",
  "/jcd/1/5/3": "sha256-GKNxxqlLRarbyBNh7hc/4lbZAdK6B0kMRf1AMRWPkSo"
}
```

For the use of JSON pointer in "jcd" and because array indexes are dependent on the order of the elements in the jCard, the digest for the "/jcd" corresponding to the entire jCard array string MUST be included to avoid any possibility of substitution or insertion attacks that may be possible to avoid integrity detection. Each URI referenced in the jCard array string MUST have a corresponding JSON pointer string key and digest value.

In the case of the use of a "jcl" URI reference to an external jCard, the procedures are similar to "jcd" with the exception and the minor modification to JSON pointer, where "/jcl" is used to refer to the external jCard array string and any following numeric array indexes added to the "jcl" (e.g. "/jcl/1/2/3") are treated as if the externally referenced jCard was directly part of the overall "rcd" claim JSON object. The following example illustrates a "jcl" version of the above "jcd" example.

```
"rcd": {
  "nam": "Q Branch Spy Gadgets",
  "jcl": "https://example.com/qbranch.json"
},
"rcdi": {
  "/jcl": "sha256-Gb0l0Kj7Z9+plqbOkN32H+YX0Yav3fbioSk7DxQdGZU",
  "/jcl/1/3/3": "sha256-RojgWwU6xUtI4q82+kHPyHm1JKbm7+663bMvzymhkl4",
  "/jcl/1/4/3": "sha256-jL4f47fF82LuwcrOrSyckA4SWrlElfARHkW6kYo1JdI",
  "/jcl/1/5/3": "sha256-GKNxxqlLRarbyBNh7hc/41bZAdK6B0kMRf1AMRWPkSo"
}

https://example.com/qbranch.json:
["vcard",
 [ ["version", {}, "text", "4.0"],
   [fn, {}, "text", "Q Branch"],
   [org, {}, "text", "MI6;Q Branch Spy Gadgets"]
   ["photo", {}, "uri",
    "https://example.com/photos/quartermaster-256x256.png"]
   ["logo", {}, "uri",
    "https://example.com/logos/mi6-256x256.jpg"]
   ["logo", {}, "uri",
    "https://example.com/logos/mi6-64x64.jpg"]
 ]
]
```

In order to facilitate proper verification of the digests and whether the "rcd" elements or content referenced by URIs were modified, the input to the digest must be completely deterministic at three points in the process. First, at the certification point where the content is evaluated to conform to the application policy and the JWT Claim Constraints is applied to the certificate containing the digest.

Second, when the call is signed at the Authentication Service, there may be a local policy to verify that the provided "rcd" claim corresponds to each digest. Third, when the "rcd" data is verified at the Verification Service, the verification is performed for each digest by constructing the input digest string for the element being verified and referenced by the JSON pointer string.

The procedure for the creation of each "rcd" element digest string corresponding to a JSON pointer string key is as follows.

1. The JSON pointer either refers to an element that is a part or whole of a JSON object string or to a string that is a URI referencing an external resource.
2. For a JSON formatted string, serialize the element JSON to remove all white space and line breaks. The procedures of this deterministic JSON serialization are defined in [RFC8225], Section 9. The resulting string MUST be a Base64 encoded [RFC4648] digest string (for sha256 this should result in approximately 44 characters).
3. For any URI referenced content, the content can either be a string as in jCard JSON objects or binary content. For example, image and audio files contain binary content. If the URI referenced content is JSON formatted, follow the procedures defined in list item 2 above. Either the binary data or string content of the file is used to create a resulting string which MUST be a Base64 encoded [RFC4648] digest string (for sha256 this should result in approximately 44 characters).

6.2. JWT Claim Constraints for "rcd" claims only

For the third mode described in the integrity overview section of this document, where only JWT Claim Constraints for "rcd" claims without an "rcdi" claim is required, the procedure when creating the certificate with the intent to always include an "rcd" claim, to include a JWT Claim Constraints on inclusion of an "rcd" claim with the intended values required to be constrained by the certificate used to sign the PASSporT.

The "permittedValues" for the "rcd" claim may optionally contain multiple entries, to support the case where the certificate holder is authorized to use different sets of rich call data.

Only including "permittedValues" for "rcd" (with no "mustInclude") provides the ability to either have no "rcd" claim or only the set of constrained "permittedValues" values for an included "rcd" claim.

7. JWT Claim Constraints usage for "rcd" and "rcdi" claims

The integrity overview section of this document describes a fourth mode where both "rcdi" and JWT Claim Constraints is used. The use of this mode implies the signing of an "rcdi" claim is required to be protected by the authoritative certificate creator using JWT Claims Constraints in the certificate. The intension of the use of both of these mechanisms is to constrain the signer to construct the "rcd" and "rcdi" claims with the "rcd" jCard object including reference external content via URI. Once both the contents of the "rcd" claim and any linked content is certified by the party that is authoritative for the certificate being created and the construction of the "rcdi" claim is complete, the "rcdi" claim is linked to the STIR certificate associated with the signature in the PASSporT via JWT Claim Constraints as defined in [RFC8226] Section 8. It should be recognized that the "rcdi" set of digests is intended to be unique for only a specific combination of "rcd" content and URI referenced external content, and therefore provides a robust integrity mechanism for an authentication service being performed by a non-authoritative party. This would often be associated with the use of delegate certificates [I-D.ietf-stir-cert-delegation] for the signing of calls by the calling party directly as an example, even though the "authorized party" is not necessarily the subject of a STIR certificate.

For the case that there should always be both "rcd" and "rcdi" values included in the "rcd" PASSporT, the certificate JWT Claims Constraint MUST include both of the following:

- * a "mustInclude" for the "rcd" claim, which simply constrains the fact that an "rcd" must be included if there is a "rcdi"
- * a "mustInclude" for the "rcdi" claim and a "permittedValues" equal to the created "rcdi" claim value string.

Note that optionally the "rcd" claims may be included in the "permittedValues" however it is recognized that this may be redundant with the "rcdi" permittedValues because the "rcdi" digest will imply the content of the "rcd" claims themselves.

The "permittedValues" for the "rcdi" claims may contain multiple entries, to support the case where the certificate holder is authorized to use different sets of rich call data.

8. PASSporT "crn" claim - Call Reason Definition and Usage

This specification defines a new JSON Web Token claim for "crn", Call Reason, the value of which is a single string or object that contains information as defined in [I-D.ietf-sipcore-callinfo-rcd] corresponding to the "reason" parameter for the Call-Info header. This claim is optional.

Example "crn" claim with "rcd":

```
"rcd": { "nam": "James Bond",  
        "jcl": "https://example.org/james_bond.json"},  
"crn" : "For your ears only"
```

8.1. JWT Constraint for "crn" claim

The integrity of the "crn" claim can optionally be protected by the authoritative certificate creator using JWT Constraints in the certificate. If the intent of the issuer of the certificate is to always including a call reason, a "mustInclude" for the "crn" claim indicates that a "crn" claim must be present. If the issuer of the certificate wants to constrain the contents of "crn", then it may set "permittedValues" for "crn" in the certificate.

9. Rich Call Data Claims Usage Rules

Either or both the "rcd" or "crn" claims may appear in any PASSporT claims object as optional elements. The creator of a PASSporT MAY also add a "ppt" value of "rcd" to the header of a PASSporT as well, in which case the PASSporT claims MUST contain either a "rcd" or "crn" claim, and any entities verifying the PASSporT object are required to understand the "ppt" extension in order to process the PASSporT in question. An example PASSporT header with the "ppt" included is shown as follows:

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

The PASSporT claims object contains the "rcd" key with its corresponding value. The value of "rcd" is an array of JSON objects, of which one, the "nam" object, is mandatory. The key syntax of "nam" follows the display-name ABNF given in [RFC3261].

After the header and claims PASSporT objects have been constructed, their signature is generated normally per the guidance in [RFC8225].

9.1. Verification rules

A PASSporT that uses claims defined in this specification, in order to have a successful verification outcome, MUST conform to the following:

- * abide by all rules set forth in the proper construction of the claims
- * abide by JWT Claims Constraint rules defined in [RFC8226] Section 8 or extended in [I-D.ietf-stir-enhance-rfc8226] if present in the certificate used to sign the PASSporT
- * pass integrity verification using "rcdi" if present.

Consistent with the verification rules of PASSporTs more generally [RFC8225], if any of the above criteria is not met, the PASSporT verification should be considered a failed verification for all claims in the PASSporT.

In some middle box scenarios, a relying party may not have the need to validate content that is referenced by URIs (e.g. only wanting to validate base PASSporT info like "orig" and "dest" or other "rcd" info like "nam" or "apn"). In these scenarios, this procedure while not considered a full verification, can be performed without verifying the full integrity checks of URI referenced content.

9.2. Example "rcd" PASSporTs

An example of a "nam" only PASSporT claims object is shown next (with line breaks for readability only).

```
{  "orig":{"tn":"12025551000"},
   "dest":{"tn":["12025551001"]},
   "iat":1443208345,
   "rcd":{"nam":"James Bond"} }
```

An example of a "nam" and "apn" only PASSporT claims object is shown next (with line breaks for readability only).

```
{  "orig":{"tn":"12025551000"},
   "dest":{"tn":["12155551001"]},
   "iat":1443208345,
   "rcd":{"
     "apn":"12025559990",
     "nam":"Her Majesty's Secret Service" } }
```

An example of a "nam" only PASSporT claims object with an "rcdi" claim is shown next (with line breaks for readability only).

```
{  "orig":{"tn":"12025551000"},
   "dest":{"tn":["12025551001"]},
   "iat":1443208345,
   "rcd":{"nam":"James Bond"},
   "rcdi":{"/nam": "sha256-uDtvpG1xNw+MK0XE0h+2UNQ94MQJ5d2ftgmHxsjKeMw"}
```

An example of a "rcd" claims object that includes the "jcd" and also contains a URI which requires the inclusion of an "rcdi" claim.

```
{
  "orig": { "tn": "12025551000"},
  "dest": { "tn": ["12155551001"]},
  "iat": 1443208345,
  "rcd": {
    "nam": "Q Branch Spy Gadgets",
    "jcd": ["vcard",
      [ ["version", {}, "text", "4.0"],
        ["fn", {}, "text", "Q Branch"],
        ["org", {}, "text", "MI6;Q Branch Spy Gadgets"],
        ["photo", {}, "uri", "https://example.com/photos/q-256x256.png"],
        ["logo", {}, "uri", "https://example.com/logos/mi6-256x256.jpg"],
        ["logo", {}, "uri", "https://example.com/logos/mi6-64x64.jpg"]
      ] ]
    },
  "crn": "Rendezvous for Little Nellie",
  "rcdi": {
    "/nam": "sha256-sM275lTgzCte+LHOKHtU4SxG8shl0o6OS4ot8IJQImY",
    "/jcd": "sha256-7kdCBZqH0nqMSPsmABvsKlHPhZEStgjojhdsJGRr3rk",
    "/jcd/1/3/3": "sha256-RojgWwU6xUtI4q82+kHPyHm1JKbm7+663bMvzymhk14",
    "/jcd/1/4/3": "sha256-jL4f47fF82LuwcrOrSyckA4SWr1ElfARHkW6kYo1JdI",
    "/jcd/1/5/3": "sha256-GKNxxqlLRarbyBNh7hc/4lbZAdK6B0kMRf1AMRWPkSo"
  }
}
```

In an example PASSporT, where a jCard is linked via HTTPS URL using "jcl", a jCard file served at a particular URL.

An example jCard JSON file is shown as follows:

```

https://example.com/qbranch.json:
["vcard",
 [ ["version", {}, "text", "4.0"],
   ["fn", {}, "text", "Q Branch"],
   ["org", {}, "text", "MI6;Q Branch Spy Gadgets"],
   ["photo", {}, "uri", "https://example.com/photos/q-256x256.png"],
   ["logo", {}, "uri", "https://example.com/logos/mi6-256x256.jpg"],
   ["logo", {}, "uri", "https://example.com/logos/mi6-64x64.jpg"]
 ]
]

```

If that jCard is hosted at the example address of "https://example.com/qbranch.json", the corresponding PASSporT claims object would be as follows:

```

{
  "orig": {"tn": "12025551000"},
  "dest": {"tn": ["12155551001"]},
  "iat": 1443208345,
  "rcd": {
    "nam": "Q Branch Spy Gadgets",
    "jcl": "https://example.com/qbranch.json"
  },
  "crn": "Rendezvous for Little Nellie",
  "rcdi": {
    "/nam": "sha256-Gb010kj7Z9+plqbOkN32H+YX0Yav3fbioSk7DxQdGZU",
    "/jcl": "sha256-Gb010kj7Z9+plqbOkN32H+YX0Yav3fbioSk7DxQdGZU",
    "/jcl/1/3/3": "sha256-RojgWwU6xUtI4q82+kHPyHm1JKbm7+663bMvzymhk14",
    "/jcl/1/4/3": "sha256-jL4f47fF82LuwcrOrSyckA4SWr1ElfARHkW6kYo1JdI",
    "/jcl/1/5/3": "sha256-GKNxxqlLRarbyBNh7hc/4lbZAdK6B0kMRf1AMRWPkSo"
  }
}

```

10. Compact form of "rcd" PASSporT

10.1. Compact form of the "rcd" PASSporT claim

Compact form of an "rcd" PASSporT claim has some restrictions but mainly follows standard PASSporT compact form procedures. For re-construction of the "nam" claim the string for the display-name in the From header field. For re-construction of the "jcl", the Call-Info header as with purpose "jcard" defined in [I-D.ietf-sipcore-callinfo-rcd] MUST be used. "jcd" claim MAY NOT be used as part of compact form.

10.2. Compact form of the "rcdi" PASSporT claim

Compact form of an "rcdi" PASSporT claim is not supported, so if "rcdi" is required compact form MUST NOT be used.

10.3. Compact form of the "crn" PASSporT claim

Compact form of a "crn" PASSporT claim shall be re-constructed using the "call-reason" parameter of a Call-Info header as defined by [I-D.ietf-sipcore-callinfo-rcd].

11. Further Information Associated with Callers

Beyond naming information and the information that can be contained in a jCard [RFC7095] object, there may be additional human-readable information about the calling party that should be rendered to the end user in order to help the called party decide whether or not to pick up the phone. This is not limited to information about the caller, but includes information about the call itself, which may derive from analytics that determine based on call patterns or similar data if the call is likely to be one the called party wants to receive. Such data could include:

- * information related to the location of the caller, or
- * any organizations or institutions that the caller is associated with, or even categories of institutions (is this a government agency, or a bank, or what have you), or
- * hyperlinks to images, such as logos or pictures of faces, or to similar external profile information, or
- * information processed by an application before rendering it to a user, like social networking data that shows that an unknown caller is a friend-of-a-friend, or reputation scores derived from crowdsourcing, or confidence scores based on broader analytics about the caller and callee.

All of these data elements would benefit from the secure attestations provided by the STIR and PASSporT frameworks. A new IANA registry has been defined to hold potential values of the "rcd" array; see Section 17.3. Specific extensions to the "rcd" PASSporT claim are left for future specification.

There is a few ways RCD can be extended in the future, jCard is an extensible object and the key/values in the RCD claim object can also be extended. General guidance for future extensibility that were followed by the authors is that jCard generally should refer to data

that references the caller as an individual or entity, where other claims, such as "crn" refer to data regarding the specific call. There may be other considerations discovered in the future, but this logical grouping of data to the extent possible should be followed for future extensibility.

12. Third-Party Uses

While rich data about the call can be provided by an originating authentication service, an intermediary in the call path could also acquire rich call data by querying a third-party service. Such a service effectively acts as a STIR Authentication Service, generating its own PASSporT, and that PASSporT could be attached to a SIP call by either the originating or terminating side. This third-party PASSporT attests information about the calling number, rather than the call or caller itself, and as such its RCD MUST NOT be used when a call lacks a first-party PASSporT that assures verification services that the calling party number is not spoofed. It is intended to be used in cases when the originating side does not supply a display-name for the caller, so instead some entity in the call path invokes a third-party service to provide rich caller data for a call.

In telephone operations today, a third-party information service is commonly queried with the calling party's number in order to learn the name of the calling party, and potentially other helpful information could also be passed over that interface. The value of using a PASSporT to convey this information from third parties lies largely in the preservation of the third party's signature over the data, and the potential for the PASSporT to be conveyed from intermediaries to endpoint devices. Effectively, these use cases form a sub-case of out-of-band [I-D.ietf-stir-oob] use cases. The manner in which third-party services are discovered is outside the scope of this document.

An intermediary use case might look as follows: a SIP INVITE carries a display name in its From header field value and an initial PASSporT object without the "rcd" claim. When a terminating verification service implemented at a SIP proxy server receives this request, and determines that the signature is valid, it might query a third-party service that maps telephone numbers to calling party names. Upon receiving the PASSporT in a response from that third-party service, the terminating side could add a new Identity header field to the request for the "rcd" PASSporT object provided by the third-party service. It would then forward the INVITE to the terminating user agent. If the display name in the "rcd" PASSporT object matches the display name in the INVITE, then the name would presumably be rendered to the end user by the terminating user agent.

A very similar flow could be followed by an intermediary closer to the origination of the call. Presumably such a service could be implemented at an originating network in order to decouple the systems that sign for calling party numbers from the systems that provide rich data about calls.

In an alternative use case, the terminating user agent might query a third-party service. In this case, no new Identity header field would be generated, though the terminating user agent might receive a PASSporT object in return from the third-party service, and use the "rcd" field in the object as a calling name to render to users while alerting.

While in the traditional telephone network, the business relationship between calling customers and their telephone service providers is the ultimate root of information about a calling party's name, some other forms of data like crowdsourced reputation scores might derive from third parties. When those elements are present, they MUST be in a third-party "rcd" PASSporT using "iss" claim described in the next section.

12.1. Signing as a Third Party

A third-party PASSporT contains an "iss" element to distinguish its PASSporTs from first-party PASSporTs. Third-party "rcd" PASSporTs are signed with credentials that do not have authority over the identity that appears in the "orig" element of the PASSporT claims. The presence of "iss" signifies that a different category of credential is being used to sign a PASSporT than the [RFC8226] certificates used to sign STIR calls; it is instead a certificate that identifies the source of the "rcd" data. How those credentials are issued and managed is outside the scope of this specification; the value of "iss" however MUST reflect the Subject of the certificate used to sign a third-party PASSporT. The explicit mechanism for reflecting the subject field of the certificate is out of scope of this document and left to the certificate governance policies that define how to map the "iss" value in the PASSporT to the subject field in the certificate. Relying parties in STIR have always been left to make their own authorization decisions about whether to trust the signers of PASSporTs, and in the third-party case, where an entity has explicitly queried a service to acquire the PASSporT object, it may be some external trust or business relationship that induces the relying party to trust a PASSporT.

An example of a Third Party issued PASSporT claims object is as follows.

```
{  "orig":{"tn":"12025551000"},
  "dest":{"tn":["12025551001"]},
  "iat":1443208345,
  "iss":"Zorin Industries",
  "rcd":{"nam":"James St. John Smythe"} }
```

13. Levels of Assurance

As "rcd" can be provided by either first or third parties, relying parties could benefit from an additional claim that indicates the relationship of the attesting party to the caller. Even in first party cases, this admits of some complexity: the Communications Service Provider (CSP) to which a number was assigned might in turn delegate the number to a reseller, who would then sell the number to an enterprise, in which case the CSP might have little insight into the caller's name. In third party cases, a caller's name could derive from any number of data sources, on a spectrum between public data scraped from web searches to a direct business relationship to the caller. As multiple PASSporTs can be associated with the same call, potentially a verification service could receive attestations of the caller name from multiple sources, which have different levels of granularity or accuracy. Therefore, third-party PASSporTs that carry "rcd" data MUST also carry an indication of the relationship of the generator of the PASSporT to the caller in the form of the "iss" claim. As stated in the previous section, the use of "iss" MUST reflect the subject field of the certificate used to sign a third-party PASSporT to represent that relationship.

14. Using "rcd" in SIP

This section specifies SIP-specific usage for the "rcd" claim in PASSporT, and in the SIP Identity header field value. Other using protocols of PASSporT may define their own usages for the "rcd" claim.

14.1. Authentication Service Behavior

An authentication service creating a PASSporT containing a "rcd" claim MAY include a "ppt" for "rcd" or not. Third-party authentication services following the behavior in Section 12.1 MUST include a "ppt" of "rcd". If "ppt" does contain a "rcd", then any SIP authentication services MUST add a "ppt" parameter to the Identity header containing that PASSporT with a value of "rcd". The resulting Identity header might look as follows:


```
Identity: sv5CTo05KqpSmtHt3dcEiO/1CWTSZtnG3iV+1nmurLXV/HmtYNS7Ltrg9
  dlxkWzoeU7d7OV8HweTTDobV3itTmgPwCFjaEmMyEI3d7SyN21yNDo2ER/Ovgt
  w0Lu5csIppPqOgluXndzHbG7mR6Rl9BnUhHufVRbp51Mn3w0gfUs=;
  info=<https://biloxi.example.org/biloxi.cer>;alg=ES256;
  ppt="rcd"
```

This specification assumes that by default, a SIP authentication service derives the value of "rcd", specifically only for the "nam" key value, from the display-name component of the From header field value of the request, alternatively for some calls this may come from the P-Asserted-ID header. It is however a matter of authentication service policy to decide how it populates the value of "nam" key, which MAY also derive from other fields in the request, from customer profile data, or from access to external services. If the authentication service generates a "rcd" claim containing "nam" with a value that is not equivalent to the From header field display-name value, it MUST use the full form of the PASSporT object in SIP.

14.2. Verification Service Behavior

[RFC8224] Section 6.2 Step 5 requires that specifications defining "ppt" values describe any additional verifier behavior. The behavior specified for the "ppt" values of "rcd" is as follows. If the PASSporT is in compact form, then the verification service SHOULD extract the display-name from the From header field value, if any, and use that as the value for the "nam" key when it recomputes the header and claims of the PASSporT object. Additionally, if there exists a Call-Info header field as defined in [I-D.ietf-sipcore-callinfo-rcd], the "jcard" value can be derived to determine the "jcd" key when it recomputes the header and claims of the PASSporT object. If the signature validates over the recomputed object, then the verification should be considered successful.

However, if the PASSporT is in full form with a "ppt" value of "rcd", then the verification service MUST extract the value associated with the "rcd" "nam" key in the object. If the signature validates, then the verification service can use the value of the "rcd" "nam" key as the display name of calling party, which would in turn be rendered to alerted users or otherwise leveraged in accordance with local policy. This allows SIP networks that convey the display name through a field other than the From header field to interoperate with this specification. Similarly, the "jcd" or linked "jcl" jcard information and "crn" can be optionally, based on local policy for devices that support it, used to populate a Call-Info header field following the format of [I-D.ietf-sipcore-callinfo-rcd].

The third-party "rcd" PASSporT cases presents some new challenges, as an attacker could attempt to cut-and-paste such a third-party PASSporT into a SIP request in an effort to get the terminating user agent to render the display name or confidence values it contains to a call that should have no such assurance. A third-party "rcd" PASSporT provides no assurance that the calling party number has not been spoofed: if it is carried in a SIP request, for example, then some other PASSporT in another Identity header field value would have to carry a PASSporT attesting that. A verification service MUST determine that the calling party number shown in the "orig" of the "rcd" PASSporT corresponds to the calling party number of the call it has received, and that the "iat" field of the "rcd" PASSporT is within the date interval that the verification service would ordinarily accept for a PASSporT.

Verification services may alter their authorization policies for the credentials accepted to sign PASSporTs when third parties generate PASSporT objects, per Section 12.1. This may include accepting a valid signature over a PASSporT even if it is signed with a credential that does not attest authority over the identity in the "orig" claim of the PASSporT, provided that the verification service has some other reason to trust the signer. No further guidance on verification service authorization policy is given here.

The behavior of a SIP UAS upon receiving an INVITE containing a PASSporT object with a "rcd" claim largely remains a matter of implementation policy. In most cases, implementations would render this calling party name information to the user while alerting. Any user interface additions to express confidence in the veracity of this information are outside the scope of this specification.

15. Using "rcd" as additional claims to other PASSporT extensions

Rich Call Data, including calling name information, for example, is often data that is additive data to the personal communications information defined in the core PASSporT data required to support the security properties defined in [RFC8225]. For cases where the entity that is originating the personal communications and additionally is supporting the authentication service and also is the authority of the Rich Call Data, rather than creating multiple identity headers with multiple PASSporT extensions or defining multiple combinations and permutations of PASSporT extension definitions, the authentication service can alternatively directly add the "rcd" claims to the PASSporT it is creating, whether it is constructed with a PASSporT extension or not.

Note: There is one very important caveat to this capability, because generally if there is URI referenced content in an "rcd" PASSporT there is often the requirement to use "rcdi" and JWT Claims Constraints. So, it is important for the user of this specification to recognize that the certificates used must include the necessary JWT Claims Constraints for proper integrity and security of the values in the "rcd" claim incorporated into PASSporTs that are not "rcd".

15.1. Procedures for applying "rcd" as claims only

For a given PASSporT using some other extension than "rcd", the Authentication Service MAY additionally include the "rcd" claim as defined in this document. This would result in a set of claims that correspond to the original intended extension with the addition of the "rcd" claim.

The Verification service that receives the PASSporT, if it supports this specification and chooses to, should interpret the "rcd" claim as simply just an additional claim intended to deliver and/or validate delivered Rich Call Data.

15.2. Example for applying "rcd" as claims only

In the case of [RFC8588] which is the PASSporT extension supporting the SHAKEN specification [ATIS-1000074], a common case for an Authentication service to co-exist in a CSP network along with the authority over the calling name used for the call. Rather than require two identity headers, the CSP Authentication Service can apply both the SHAKEN PASSporT claims and extension and simply add the "rcd" required claims defined in this document.

For example, the PASSporT claims for the "shaken" PASSporT with "rcd" claims would be as follows:

```
Protected Header
{
  "alg":"ES256",
  "typ":"passport",
  ppt:shaken,
  "x5u":"https://cert.example.org/passport.cer"
}
Payload
{
  attest:A,
  "dest":{"tn":["12025551001"]},
  "iat":1443208345,
  "orig":{"tn":"12025551000"},
  origid:123e4567-e89b-12d3-a456-426655440000,
  "rcd":{"nam":"James Bond"}
}
```

A Verification Service that supports "rcd" and "shaken" PASSport extensions is able to receive the above PASSport and interpret both the "shaken" claims as well as the "rcd" defined claim.

If the Verification Service only understands the "shaken" extension claims but doesn't support "rcd", the "rcd" is ignored and disregarded.

16. Acknowledgements

We would like to thank David Hancock, Robert Sparks, Russ Housley, Eric Burger, Alec Fenichel, Ben Campbell, Jack Rickard for helpful suggestions, review, and comments.

17. IANA Considerations

17.1. JSON Web Token Claim

This specification requests that the IANA add three new claims to the JSON Web Token Claims registry as defined in [RFC7519].

Claim Name: "rcd"

Claim Description: Rich Call Data Information

Change Controller: IESG

Specification Document(s): [RFCThis]

Claim Name: "rcdi"

Claim Description: Rich Call Data Integrity Information

Change Controller: IESG

Specification Document(s): [RFCThis]

Claim Name: "crn"

Claim Description: Call Reason

Change Controller: IESG

Specification Document(s): [RFCThis]

17.2. PASSporT Types

This specification requests that the IANA add a new entry to the PASSporT Types registry for the type "rcd" which is specified in [RFCThis].

17.3. PASSporT RCD Types

This document requests that the IANA create a new registry for PASSporT RCD types. Registration of new PASSporT RCD types shall be under the Specification Required policy.

This registry is to be initially populated with four values, "nam", "apn", "jcd", and "jcl", which are specified in [RFCThis].

18. Security Considerations

Whether its identities, alternate identities, images, logos, physical addresses, all of the information contained in a RCD PASSporT must follow some form of vetting in which the authoritative entity or user of the information being signed MUST follow an applicable policy of the eco-system using RCD. This can be of many forms, depending on the setup and constraints of the eco-system so is therefore out-of-scope of this document. However, the general chain of trust that signers of RCD PASSporT are either directly authoritative or have been delegated authority through certificates using JWT Claim Constraints and integrity mechanisms defined in this and related documents is critical to maintain the integrity of the eco-system utilizing this and other STIR related specifications.

Revealing information such as the name, location, and affiliation of a person necessarily entails certain privacy risks. Baseline PASSporT has no particular confidentiality requirement, as the information it signs over in a using protocol like SIP is all

information that SIP carries in the clear anyway. Transport-level security can hide those SIP fields from eavesdroppers, and the same confidentiality mechanisms would protect any PASSporT(s) carried in SIP.

Since computation of "rcdi" digests for URIs requires the loading of referenced content, it would be best practice to validate that content at the creation of the "rcdi" or corresponding JWT claim constraint value by checking for content that may cause issues for verification services or that doesn't follow the behavior defined in this document, e.g. unreasonably sized data, the inclusion of recursive URI references, etc. Along the same lines, the verification service should also use precautionary best practices to avoid attacks when accessing URI linked content.

18.1. The use of JWT Claim Constraints in delegate certificates to exclude unauthorized claims

While this can apply to any PASSporT that is signed with a STIR Delegate Certificates [I-D.ietf-stir-cert-delegation], it is important to note that when constraining PASSporTs to include specific claims or contents of claims, it is also important to consider potential attacks by non-authorized signers that may include other potential PASSporT claims that weren't originally vetted by the authorized entity providing the delegate certificate. The use of JWT claims constraints as defined in [I-D.ietf-stir-enhance-rfc8226] for preventing the ability to include claims beyond the claims defined in this document may need to be considered.

Certificate issuers SHOULD NOT include an entry in mustExclude for the "rcdi" claim for a certificate that will be used with the PASSporT Extension for Rich Call Data defined in this document. Excluding this claim would prevent the integrity protection mechanism from working properly.

19. References

19.1. Normative References

[I-D.ietf-sipcore-callinfo-rcd]
Wendt, C. and J. Peterson, "SIP Call-Info Parameters for Rich Call Data", Work in Progress, Internet-Draft, draft-ietf-sipcore-callinfo-rcd-02, 22 February 2021, <<https://www.ietf.org/archive/id/draft-ietf-sipcore-callinfo-rcd-02.txt>>.

- [I-D.ietf-stir-cert-delegation]
Peterson, J., "Secure Telephone Identity Revisited (STIR) Certificate Delegation", Work in Progress, Internet-Draft, draft-ietf-stir-cert-delegation-04, 22 February 2021, <<https://www.ietf.org/archive/id/draft-ietf-stir-cert-delegation-04.txt>>.
- [I-D.ietf-stir-enhance-rfc8226]
Housley, R., "Enhanced JSON Web Token (JWT) Claim Constraints for Secure Telephone Identity Revisited (STIR) Certificates", Work in Progress, Internet-Draft, draft-ietf-stir-enhance-rfc8226-05, 26 July 2021, <<https://www.ietf.org/archive/id/draft-ietf-stir-enhance-rfc8226-05.txt>>.
- [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>>.
- [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>>.
- [RFC4627] Crockford, D., "The application/json Media Type for JavaScript Object Notation (JSON)", RFC 4627, DOI 10.17487/RFC4627, July 2006, <<https://www.rfc-editor.org/info/rfc4627>>.
- [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>>.
- [RFC6901] Bryan, P., Ed., Zyp, K., and M. Nottingham, Ed., "JavaScript Object Notation (JSON) Pointer", RFC 6901, DOI 10.17487/RFC6901, April 2013, <<https://www.rfc-editor.org/info/rfc6901>>.

- [RFC7095] Kewisch, P., "jCard: The JSON Format for vCard", RFC 7095, DOI 10.17487/RFC7095, January 2014, <<https://www.rfc-editor.org/info/rfc7095>>.
- [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>>.
- [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>>.
- [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>>.
- [RFC8588] Wendt, C. and M. Barnes, "Personal Assertion Token (PaSSporT) Extension for Signature-based Handling of Asserted information using toKENs (SHAKEN)", RFC 8588, DOI 10.17487/RFC8588, May 2019, <<https://www.rfc-editor.org/info/rfc8588>>.

19.2. Informative References

- [ATIS-1000074]
ATIS/SIP Forum NNI Task Group, "Signature-based Handling of Asserted information using toKENs (SHAKEN)" <https://access.atis.org/apps/group_public/download.php/32237/ATIS-1000074.pdf>, January 2017.

[I-D.ietf-stir-oob]

Rescorla, E. and J. Peterson, "Secure Telephone Identity
Revisited (STIR) Out-of-Band Architecture and Use Cases",
Work in Progress, Internet-Draft, draft-ietf-stir-oob-07,
9 March 2020, <<https://www.ietf.org/archive/id/draft-ietf-stir-oob-07.txt>>.

Authors' Addresses

Chris Wendt
Comcast
Comcast Technology Center
Philadelphia, PA 19103,
United States of America

Email: chris-ietf@chriswendt.net

Jon Peterson
Neustar Inc.
1800 Sutter St Suite 570
Concord, CA 94520,
United States of America

Email: jon.peterson@neustar.biz

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 13, 2022

J. Peterson
Neustar
C. Wendt
Comcast
July 12, 2021

Connected Identity for STIR
draft-peterson-stir-rfc4916-update-04

Abstract

The SIP Identity header 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 January 13, 2022.

Copyright Notice

Copyright (c) 2021 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents

(<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	2
2. Terminology	4
3. Connected Identity Problem Statement for STIR	4
4. Connected Identity in Provisional Dialogs	5
5. Connected Identity in Mid-Dialog and Dialog-Terminating Requests	6
6. Interaction with Divert PASSporT	7
7. Authorization Policy for Callers	7
8. Pre-Association with Destinations	8
9. Connected Identity and Conferencing	9
10. Examples	9
11. Updates to RFC4916	9
12. Acknowledgments	9
13. IANA Considerations	9
14. Security Considerations	10
15. References	10
15.1. Informative References	10
15.2. Informative References	11
Authors' Addresses	12

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 of a session. Users review information about the calling party, for example, to determine whether to accept communications initiated by a 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 automata 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 [RFC7340]). 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, but in certain network environments, 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 identity in the backwards direction of a call is here 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, for various backwards-compatibility reasons. 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 signable 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 updates [RFC4916] to reflect the changes to the SIP Identity header 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].

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. 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 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 unceremoniously dumped on a PSTN gateway, they might be sent to a default intermediary that makes forwarding decisions based on a local flat file, various mechanisms like private ENUM [RFC6116] might be consulted, 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 to 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 ("short-stopping") that rely on intermediary networks making it appear as if a call has terminated to one side, while maintaining that the call is still active to the other, 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, just like dialog-forming requests, then another impersonation vector leading to fraud in the telephone network could be shut down.

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.

4. Connected Identity in 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 the use of the UPDATE method to send the connected identity in the backwards direction after the UAS had received and responded to a PRACK [RFC3262] from the UAC, which would in turn have been triggered by a provisional lxx response sent earlier by the UAC. [RFC4916] permits the From header field of the UPDATE to change the address of record of the recipient: if the original INVITE had been sent with a To header field value of "sip:bob@example.com", the UAS in its UPDATE could set the From header field value to "sip:carol@example.com." For STIR, this is a very important property, as Carol might not even possess a credential that can legitimately sign for Bob.

Per [RFC3262], UAC's that require connected identity MUST thus send a Require header field with the option tag 100rel in INVITES in addition to an Identity header field value containing a PASSporT. UAS's that support this mechanism will first send a Require header field with the option tag 100rel in lxx class responses to INVITES that they receive, along with the necessary RSeq header field. The UAC will send a PRACK when it receives the reliable lxx response from the UAS; the UAS, upon receiving a PRACK, responds with a 200 OK. At this point, the terminating UA is free to send an UPDATE [RFC3311] request in the backwards direction to the originating UA. This update will contain an Identity header, with a PASSporT that signs for the connected identity in its "orig" claim, which typically corresponds to the From header field value of the UPDATE request. If the PASSporT is valid, the originating UA will respond with an OK, and may perform any behaviors associated with the updated identity (see Section 7). Even if connected identity is not required by the originator of an INVITE request, it can still be solicited if available by sending the 100rel option tag in a Supported header field when sending an INVITE with an Identity header, which will trigger the preceding flow if the UAS supports connected identity.

Usually, the updated Identity reflects a changed to the From header field value. But in many operating environments, the From header field value does not contain the identity of the caller that has been asserted by the network, which is instead conveyed by the P-Asserted-Identity header field [RFC3325]. The contents of PAID are not used for dialog matching, and so in environments where PAID is used, it can be altered more dynamically. However, in order for the connected identity and a PASSporT to be conveyed in the backwards direction, a provisional dialog still needs to be established, and an UPDATE sent: in this case, it will be the UPDATE that contains the connected identity in its P-Asserted-Identity header field value, and that value will be signed by the PASSporT in its "orig" claim.

5. 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, MUST contain Identity headers with valid PASSporTs based on the current To/From header field values for the dialog. This 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 [I-D.peterson-stir-messaging]). This specification thus does not mandate 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 with an Identity header containing a PASSporT, any CANCEL request received for the dialog initiated by that INVITE must also contain an Identity header 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. It is however REQUIRED by this specification that if a UAC sends a CANCEL for its own PASSporT-protected INVITE request, that it include an Identity header with a valid PASSporT in the CANCEL. UAS policy will have to determine the instances where it will accept unsigned CANCEL requests for a dialog initiated with a signed INVITE.

6. Interaction with Divert PASSporT

Many of the use cases that motivate connected identity involve retargeting: when a call acquires a new target (in its Request-URI) during transit, the terminating side needs a way to express to the originating side which destination the INVITE reached. 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 specified in [RFC8946], the only way those diversion PASSporTs will be seen by the calling party is if redirection is used (SIP 3XX responses) instead of retargeting; while some network policies may want to conceal service logic from the originating party, sending redirections in the backwards direction is the only current 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 per Section 4 the terminating side sends an UPDATE with an Identity header containing a PASSporT for its current From (or PAID) header field value, it MAY include in Identity header field values any "div" PASSporTs it received in the INVITE that initiated this provisional dialog. These "div" PASSporTs will 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. Note however that "div" is not universally supported, and thus calls may be retargeted with generating a "div" PASSporT, so sending those PASSporTs in the backwards direction cannot be mandated. Also note that this will potentially reveal service logic to the called party.

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--and 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 will not prescribe any user experience associated with placing a call, it assumes that callers might have some way to set an authorization posture that will result in the right thing happening when the connected identity is not expected. This is analogous to a situation where SRTP negotiation fails because the keys exchanged at the media layer do not match 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, that would cause their user agent to send the INVITE with a Require for 100rel. Similarly, 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 party.

Ultimately, authorization policy for called parties is difficult to set, as calls can end up at unexpected places for legitimate reasons. Some work has been done to make sure that secure diversion works with STIR, as described in Section 6.

8. 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.

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 and 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, provide an opportunity to form a pre-association with the 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 [RFC3375], in which an INVITE is sent with no SDP. Similar media-less dialogs have been proposed for certain automata per [RFC5552]. In the STIR context, a media-less dialog is established by sending an INVITE with an

Identity header but no SDP. STIR-aware UAS's 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 and then an UPDATE 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.

[More TBD. In some environments, that may require the use of mechanisms defined by [RFC8816].]

9. Connected Identity and Conferencing

The establishment of connected identity when there are more than two parties in a session will depend on the conferencing mechanism used.

[More TBD.]

10. Examples

[TBD: Revise RFC4916 examples to show new Identity header present in UPDATE and in a backwards-direction BYE.]

11. Updates to RFC4916

[TBD - ways that UPDATES in the backwards direction can carry additional information in support of the above]

In general, the guidance of RFC4916 remains valid for RFC8224.

The deprecation of the Identity-Info header has a number of implications for RFC4916; all of the protocol examples need to be updated to reflect that.

12. Acknowledgments

We would like to thank YOU for your contributions to this specification.

13. IANA Considerations

This memo includes no request to IANA.

14. Security Considerations

TBD.

15. References

15.1. Informative 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>>.
- [RFC3375] Hollenbeck, S., "Generic Registry-Registrar Protocol Requirements", RFC 3375, DOI 10.17487/RFC3375, September 2002, <<https://www.rfc-editor.org/info/rfc3375>>.
- [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>>.
- [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>>.

- [RFC7159] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", RFC 7159, DOI 10.17487/RFC7159, March 2014, <<https://www.rfc-editor.org/info/rfc7159>>.
- [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>>.
- [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>>.
- [RFC8396] Peterson, J. and T. McGarry, "Managing, Ordering, Distributing, Exposing, and Registering Telephone Numbers (MODERN): Problem Statement, Use Cases, and Framework", RFC 8396, DOI 10.17487/RFC8396, July 2018, <<https://www.rfc-editor.org/info/rfc8396>>.
- [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>>.
- [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>>.

15.2. Informative References

- [I-D.peterson-stir-messaging]
Peterson, J. and C. Wendt, "Messaging Use Cases and Extensions for STIR", draft-peterson-stir-messaging-01 (work in progress), February 2021.

- [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>>.

Authors' Addresses

Jon Peterson
Neustar, Inc.
1800 Sutter St Suite 570
Concord, CA 94520
US

Email: jon.peterson@team.neustar

Chris Wendt
Comcast
One Comcast Center
Philadelphia, PA 19103
USA

Email: chris-ietf@chriswendt.net

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 26 April 2022

C. Wendt
Comcast
23 October 2021

Identity Header Error Handling
draft-wendt-stir-identity-header-errors-handling-03

Abstract

This document extends STIR and the Authenticated Identity Management in the Session Initiation Protocol (SIP) error handling procedures to include the mapping of verification failure reasons to STIR defined 4xx codes so the failure reason of an Identity header field can be conveyed to the upstream authentication service when local policy dictates that the call should continue in the presence of a verification failure. This document also defines procedures that enable a failure reason to be mapped to a specific Identity header for scenarios that use multiple Identity header fields where some may have errors and others may not and the handling of those situations is defined.

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 26 April 2022.

Copyright Notice

Copyright (c) 2021 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document.

Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	2
2. Terminology	3
3. Reason header field protocol "STIR"	3
4. Use of provisional error responses to signal errors without terminating the call	3
5. Handling of a verification error when there are multiple Identity header fields	3
6. Handling multiple verification errors	4
7. Removal of the Reason header field by Authentication Service	5
8. IANA Considerations	5
9. Acknowledgements	5
10. Security Considerations	6
11. Normative References	6
Author's Address	6

1. Introduction

[RFC8224] in Section 6.2.2 discusses future specifications for enhancement of how errors are communicated and the handling of multiple Identity header fields. This specification provides some additional mechanisms for solutions to address these problems.

In some deployments of STIR and specifically using SIP [RFC3261] as defined by [RFC8224], one issue with the current error handling, specifically with the use of the defined 4xx error responses, is that when an error occurs with the verification of the Identity header field or the PASSporT contained in the Identity header field and a 4xx response is returned, the call is then terminated. It may be the case that the policy for handling errors dictates that calls should continue even if there is a verification error, in the case of, for example inadvertent errors, however the authentication service should still be notified of the error so that corrective action can be taken. This specification will discuss the use of the Reason header field in subsequent provisional (1xx) responses in order to accomplish this.

For the handling of multiple Identity header fields and the potential situation that some of the Identity header fields in a call may pass verification but others may have errors, this document provides a

mechanism to add an identifier so that the authentication service can identify which Identity header field is being referred to in the case of an error.

2. Terminology

The keywords "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. Reason header field protocol "STIR"

This specification defines a new Reason header field [RFC3326] protocol "STIR" for STIR applications using SIP as defined in [RFC8224]. This will differentiate current protocols, specifically "SIP" which is currently in wide industry usage, from the [RFC8224] defined error cause codes and the potential use of multiple Reason header fields defined in [RFC3326] and updated in [upcoming document TBD] allowing multiple Reason header fields with the same "STIR" protocol string. The use of multiple Reason header field is discussed in more detail later in the document.

4. Use of provisional error responses to signal errors without terminating the call

In cases where local policy dictates that a call should continue regardless of any verification errors that may have occurred, including 4XX errors described in [RFC8224] Section 6.2.2, then the verification service SHOULD NOT send the 4XX as a response, but rather include the error response code and reason phrase in a Reason header field, defined in [RFC3326], in the next provisional or final responses sent to the authentication service.

Example Reason header field:

Reason: STIR ;cause=436 ;text="Bad Identity Info"

5. Handling of a verification error when there are multiple Identity header fields

In cases where a SIP message includes multiple Identity header fields and one of those Identity header fields has an error, the verification service SHOULD include the error response code and reason phrase associated with the error in a Reason header field, defined in [RFC3326], in the next provisional or final responses sent to the authentication service. The reason cause in the Reason header

field SHOULD represent the error that occurred when verifying the contents of the Identity header field. The association of a Reason header field and error to a specific Identity header field is accomplished by adding a "ppt" parameter containing the PASSporT that generated the error to the Reason header field. The "ppt" parameter for the Reason header field is optional, but RECOMMENDED, in particular for cases that a SIP INVITE contains multiple Identity header fields. The PASSporT can be included in full form, or optionally in compact form, where only the signature of the PASSporT is used to identify the reported Identity header field with an error.

Example Reason header field with full form PASSporT:

```
Reason: STIR ;cause=436 ;text="Bad Identity Info" ;ppt= \
"eyJhbGciOiJFbGVzIiIsInR5cCI6InBhc3Nwb3J0IiwieDVlIiIjOiJ9.eyJ \
joiaHR0cHM6Ly9jZXXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LmNlciJ9.eyJ \
kZXN0Ijpw7InVyaSI6WyJzaXA6YWxpY2VAZXhhbXBsZS5jb20iXX0sImhhdC \
I6IjE0NDMyMDgzNDUiLCJvcmlnIjpw7InRuIjoimTIxNTU1NTEyMTIifX0.r \
q3pjTlhoRwakEGjHCnWSwUnshd0-zJ6F1VOgFWSjHBr8Qjplk-cpFYpFYs \
ojNCpTzO3QfPOLckGaS6hEck7w"
```

Example Reason header field with compact form PASSporT: ~~~~~~

```
Reason: STIR ;cause=436 ;text="Bad Identity Info" ;ppt= \
"..rq3pjTlakeGjHCnWSwUnshd0-zJ6F1VOgFWSjHBr8Qjplk-cpFYpFYs \
ojNCpTzO3QfPOLckGaS6hEck7w" ~~~~~~
```

6. Handling multiple verification errors

If there are multiple Identity header field verification errors being reported the verification service SHOULD include corresponding Reason header fields with "ppt" parameters including full or compact form of the PASSporT with cause and text parameters identifying each error. As mentioned previously, the potential use of multiple Reason header fields defined in [RFC3326] is updated in [upcoming document TBD] allowing multiple Reason header fields with the same protocol value, for this specification being "STIR".

Example Reason header fields for two identity info errors:

```
Reason: STIR ;cause=436 ;text="Bad Identity Info" ;ppt= \
"eyJhbGciOiJFUzI1NiIsInR5cCI6InBhc3Nwb3J0IiwieDV1Ii \
joiaHR0cHM6Ly9jZXXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LmNlciJ9.eyJ \
kZXN0Ijpp7InVyaSI6WyJzaXA6YWxpY2VAZXhhbXBsZS5jb20iXX0sImhhdC \
I6IjE0NDMyMDgzNDUiLCJvcmlnIjpp7InRuIjoimTIxNTU1NTEyMTIifX0.r \
q3pjTlhoRwakEGjHCnWSwUnshd0-zJ6F1VOgFWSjHBr8Qjplk-cpFYpFYs \
ojNCpTzO3QfP0lckGaS6hEck7w"
```

```
Reason: STIR ;cause=436 ; text="Bad Identity Info" ;ppt= \
"eyJhbGciOiJFUzI1NiIsInR5cCI6InBhc3Nwb3J0IiwieDV1Ii \
joiaHR0cHM6Ly9jZXXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LmNlciJ9.eyJ \
xpY2VAZXhhbXBsZS5jb20iXX0sImhhdCkZXN0Ijpp7InVyaSI6WyJzaXA6YW \
p7InRuIjoimTIxNTU1NTEyMTIifX0I6IjE0NDMyMDgzNDUiLCJvcmlnIj.r \
J6F1VOgFWSjHBr8Qjplk-cpFYpFYsq3pjTlhoRwakEGjHCnWSwUnshd0-z \
ckGaS6hEck7wojNCpTzO3QfP0l"
```

7. Removal of the Reason header field by Authentication Service

When an Authentication Service [RFC8224] receives the Reason header field with a PASSporT it generated as part of an Identity header field and the authentication of a call, it should first follow local policy to recognize and acknowledge the error (e.g. perform operational actions like logging or alarming), but then MUST remove the identified Reason header field to avoid the PASSporT information from going upstream to a UAC or UAS that may not be authorized to see claim information contained in the PASSporT for privacy or other reasons.

8. IANA Considerations

This document requests the definition of a new protocol value (and associated protocol cause) to be registered by the IANA into the "Reason Protocols" sub-registry under <http://www.iana.org/assignments/sip-parameter> as follows:

Protocol Value	Protocol Cause	Reference
STIR	Status code	RFC 8224

9. Acknowledgements

Would like to thank David Hancock for help to identify these error scenarios and Jon Peterson, Roman Shpount, and STIR working group for helpful feedback and discussion.

10. Security Considerations

TBD

11. 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>>.
- [RFC3326] Schulzrinne, H., Oran, D., and G. Camarillo, "The Reason Header Field for the Session Initiation Protocol (SIP)", RFC 3326, DOI 10.17487/RFC3326, December 2002, <<https://www.rfc-editor.org/info/rfc3326>>.
- [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>>.

Author's Address

Chris Wendt
Comcast
Comcast Technology Center
Philadelphia, PA 19103,
United States of America

Email: chris-ietf@chriswendt.net