

Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: August 25, 2021

J. Peterson  
Neustar  
February 21, 2021

STIR Certificate Delegation  
draft-ietf-stir-cert-delegation-04

Abstract

The Secure Telephone Identity Revisited (STIR) certificate profile provides a way to attest authority over telephone numbers and related identifiers for the purpose of preventing telephone number spoofing. This specification details how that authority can be delegated from a parent certificate to a subordinate certificate. This supports a number of use cases, including those where service providers grant credentials to enterprises or other customers capable of signing calls with STIR.

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 August 25, 2021.

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. Motivation . . . . .	3
4. Delegation of STIR Certificates . . . . .	4
4.1. Scope of Delegation . . . . .	5
5. Authentication Services Signing with Delegate Certificates .	6
6. Verification Service Behavior for Delegate Certificate Signatures . . . . .	7
7. Acquiring Multiple Certificates in STIR . . . . .	7
8. Certification Authorities and Service Providers . . . . .	8
8.1. ACME and Delegation . . . . .	9
8.2. Handling Multiple Certificates . . . . .	9
9. Alternative Solutions . . . . .	10
10. IANA Considerations . . . . .	10
11. Privacy Considerations . . . . .	10
12. Security Considerations . . . . .	11
13. Acknowledgments . . . . .	11
14. References . . . . .	12
14.1. Normative References . . . . .	12
14.2. Informative References . . . . .	13
Author's Address . . . . .	14

## 1. Introduction

The STIR problem statement [RFC7340] reviews the difficulties facing the telephone network that are enabled by impersonation, including various forms of robocalling, voicemail hacking, and swatting [RFC7375]. One of the most important components of a system to prevent impersonation is the implementation of credentials which identify the parties who control telephone numbers. The STIR certificates [RFC8226] specification describes a credential system based on [X.509] version 3 certificates in accordance with [RFC5280] for that purpose. Those credentials can then be used by STIR authentication services [RFC8224] to sign PASSporT objects [RFC8225] carried in SIP [RFC3261] requests.

[RFC8226] specifies an extension to X.509 that defines a Telephony Number (TN) Authorization List that may be included by certification authorities (CAs) in certificates. This extension provides additional information that relying parties can use when validating transactions with the certificate. When a SIP request, for example, arrives at a terminating administrative domain, the calling number

attested by the SIP request can be compared to the TN Authorization List of the certificate that signed the PASSporT to determine if the caller is authorized to use that calling number.

Initial deployment of [RFC8226] has focused on the use of Service Provider Codes (SPCs) to attest the scope of authority of a certificate. Typically, these codes are internal telephone network identifiers such as the Operating Company Numbers (OCNs) assigned to carriers in the United States. However, these network identifiers are effectively unavailable to non-carrier entities, and this has raised questions about how such entities might best participate in STIR, when needed. Additionally, a carrier may sometimes operate numbers that are formally assigned to another carrier. [RFC8226] gave an overview of a certificate enrollment model based on "delegation," whereby the holder of a certificate might allocate a subset of that certificate's authority to another party. This specification details how delegation of authority works for STIR certificates.

## 2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

This specification also uses the terms:

delegation: the concept of STIR certificate delegation and its terms are defined in [RFC8226].

legitimate spoofing: the practice of selecting an alternative presentation number for a telephone caller legitimately.

## 3. Motivation

The most pressing need for delegation in STIR arises in a set of use cases where callers want to use a particular calling number, but for whatever reason, their outbound calls will not pass through the authentication service of the service provider that controls that numbering resource.

One example would be an enterprise that places outbound calls through a set of service providers, for each call choosing a provider based on a least-cost routing algorithm or similar local policy. The enterprise was assigned a calling number by a particular service

provider, but some calls originating from that number will go out through other service providers.

A user might also roam from their usual service provider to a different network or administrative domain, for various reasons. Most "legitimate spoofing" examples are of this form: where a user wants to be able to use the main call-back number for their business as a calling party number, even when the user is away from the business.

These sorts of use cases could be addressed if the carrier who controls the numbering resource were able to delegate a credential that could be used to sign calls regardless of which network or administrative domain handles the outbound routing for the call. In the absence of something like a delegation mechanism, outbound carriers may be forced to sign calls with credentials that do not cover the originating number in question. Unfortunately, that practice would be difficult to distinguish from malicious spoofing, and if it becomes widespread, it could erode trust in STIR overall.

#### 4. Delegation of STIR Certificates

STIR delegate certificates are certificates containing a TNAuthList object that have been signed with the private key of a parent certificate that itself contains a TNAuthList object (either by-value or by-reference, see Section 4.1). The parent certificate needs to contain a basic constraints extension with the [RFC5280] cA boolean set to "true", indicating that the subject can sign certificates. Every STIR delegate certificate identifies its parent certificate with a standard [RFC5280] Authority Key Identifier extension.

The authority bestowed on the holder of the delegate certificate by the parent certificate is recorded in the delegate certificate's TNAuthList. Because STIR certificates use the TNAuthList object rather than the Subject Name for indicating the scope of their authority, traditional [RFC5280] name constraints are not directly applicable to STIR. In a manner similar to the RPKI [RFC6480] "encompassing" semantics, each delegate certificate MUST have a TNAuthList scope that is equal to or a subset of its parent certificate's scope: it must be "encompassed." For example, a parent certificate with a TNAuthList that attested authority for the numbering range +1-212-555-1000 through 1999 could issue a certificate to one delegate attesting authority for the range +1-212-555-1500 through 1599, and to another delegate a certificate for the individual number +1-212-555-1824.

Delegate certificates MAY also contain a basic constraints extension with the cA boolean set to "true", indicating that they can sign

subordinate certificates for further delegates. As only end-entity certificates can actually sign PASSporTs, the holder of a STIR certificate with a "true" cA boolean may create a separate end-entity certificate either with an identical TNAuthList to its parent, or with a subset of the parents authority, that would be used to sign PASSporTs.

#### 4.1. Scope of Delegation

The TNAuthList of a STIR certificate may contain one or more SPCs, or one or more telephone number ranges, or even a mix of SPCs and telephone number ranges. When delegating from a STIR certificate, a child certificate may inherit from its parent either or both of the above, and this specification explicitly permits SPC-only parent certificates to delegate individual telephone numbers or ranges to a child certificate, as this will be necessary in some operating environments. Depending on the sort of numbering resources that a delegate has been assigned, various syntaxes can be used to capture the delegated resource.

Some non-carrier entities may be assigned large and complex allocations of telephone numbers, which may be only partially contiguous or entirely disparate. Allocations may also change frequently, in minor or significant ways. These resources may be so complex, dynamic, or extensive that listing them in a certificate is prohibitively difficult. Section 10.1 of [RFC8226] describes one potential way to address this, including the TNAuthList (specified in [RFC8226]) in the certificate by-reference rather than by value, where a URL in the certificate points to a secure, dynamically-updated list of the telephone numbers in the scope of authority of a certificate. For entities that are carriers in all but name, another alternative is the allocation of an SPC; this yields much the same property, as the SPC is effectively a pointer to an external database which dynamically tracks the numbers associated with the SPC. Either of these approaches may make sense for a given deployment. Certification path construction as detailed below treats by-reference TNAuthLists in a certificate as if it had been included by-value.

Other non-carrier entities may have straightforward telephone number assignments, such as enterprises receiving a set of thousand blocks from a carrier that may be kept for years or decades. Particular freephone numbers may also have a long-term association with an enterprise and its brand. For these sorts of assignments, assigning an SPC may seem like overkill, and using the TN ranges of the TNAuthList (by-value) is sufficient.

Whichever approach is taken to representing the delegated resource, there are fundamental trade-offs regarding when and where in the

architecture a delegation is validated: that is, when the delegated TNAuthList is checked to be "encompassed" by the TNAuthList of its parent. This might be performed at the time the delegate certificate is issued, or at the time that a verification service receives an inbound call, or potentially both. It is generally desirable to offload as much of this as possible to the certification process, as verification occurs during call setup and thus additional network dips could lead to perceptible delay, whereas certification happens outside of call processing as a largely administrative function. Ideally, if a delegate certificate can supply a by-value TN range, then a verification service could ascertain that an attested calling party number is within the scope of the provided certificate without requiring any additional transactions with a service. In practice, verification services may already incorporate network queries into their processing (for example, to dereference the "x5u" field of a PASSporT) that could piggyback any additional information needed by the verification service.

Note that the permission semantics of the [RFC8226] TNAuthList are additive: that is, the scope of a certificate is the superset of all of the SPCs and telephone number ranges enumerated in the TNAuthList. As SPCs themselves are effectively pointers to a set of telephone number ranges, and a telephone number may belong to more than one SPC, this may introduce some redundancy to the set of telephone numbers specified as the scope of a certificate. The presence of one or more SPCs and one or more sets of telephone number ranges are similarly treated additively, even if the telephone number ranges turn out to be redundant to the scope of an SPC.

## 5. Authentication Services Signing with Delegate Certificates

Authentication service behavior varies from [RFC8224] as follows, although the same checks are performed by the authentication service when comparing the calling party number attested in call signaling with the scope of the authority of the signing certificate. Authentication services SHOULD NOT use a delegate certificate without validating that its scope of authority is encompassed by that of its parent certificate, and if that certificate has its own parent, the entire certification path SHOULD be validated.

This delegation architecture does not require that a non-carrier entity act as its own authentication service. That function may be performed by any authentication service that holds the private key corresponding to the delegate certificate, including one run by an outbound service provider, a third party in an enterprise's outbound call path, or in the SIP User Agent itself.

Note that authentication services creating a PASSporT for a call signed with a delegate certificate MUST provide an "x5u" link corresponding to the entire certification path, rather than just the delegate certificate used to sign the call, as described in Section 7.

## 6. Verification Service Behavior for Delegate Certificate Signatures

The responsibility of a verification service validating PASSporTs signed with delegate certificates, while largely following baseline [RFC8224] and [RFC8225], requires some additional procedures. When the verification service dereferences the "x5u" parameter, it will acquire a certificate list rather than a single certificate. It MUST then validate all of the credentials in the list, identifying the parent certificate for each delegate through its Authority Key Identifier extension.

While ordinarily, relying parties have significant latitude in certification path construction when validating a certification path, STIR assumes a more rigid hierarchical subordination model, rather than one where relying parties may want to derive their own certification path to particular trust anchors. If the certificates acquired from the "x5u" element of a PASSporT do not lead to an anchor that the verification service trusts, it treats the validation no differently than it would when a non-delegated certificate was issued by an untrusted root; in SIP, it MAY return a 437 "Unsupported Credential" response if the call should be failed for lack of a valid Identity header.

## 7. Acquiring Multiple Certificates in STIR

PASSporT [RFC8225] uses the "x5u" element to convey the URL where verification services can acquire the certificate used to sign a PASSporT. This value is mirrored by the "info" parameter of the Identity header when a PASSporT is conveyed via SIP. Commonly, this is an HTTPS URI.

When a STIR delegate certificate is used to sign a PASSporT, the "x5u" element in the PASSporT will contain a URI indicating where a certificate list is available. While baseline JSON Web Signature (JWS) also supports an "x5c" element specifically for certificate chains, in operational practice, certification paths are already being delivered in the STIR environment via the "x5u" element, so this specification RECOMMENDS implementations contain to use "x5u"; "x5c" is OPTIONAL for environments where it is known to be supported. That list will be a concatenation of PEM-encoded certificates of the type "application/pem-certificate-chain" defined in [RFC8555]. The certificate path [RFC5280] ordering MUST be ordered from the signer

to the trust anchor. The list begins with the certificate used to sign the PASSporT, followed by its parent, and then any subsequent grandparents, great-grandparents, and so on. The key identifier in the Authority Key Identifier extension in the first certificate MUST appear in the Subject Key Identifier extension in the second certificate. The key identifier pairing MUST match in this way throughout the entire chain of certificates. Note that ACME [RFC8555] requires the first element in a pem-certificate-chain to be an end-entity certificate.

## 8. Certification Authorities and Service Providers

Once a telephone service provider has received a CA certificate attesting their numbering resources, they may delegate resources from it as they see fit. Note that the allocation to a service provider of a certificate with a basic constraints extension with the `ca` boolean set to "true" does not require that a service provider act as a certification authority itself; serving as a certification authority is a function requiring specialized expertise and infrastructure. Certification authorities are for example responsible for maintain certificate revocation lists and related functions, as well as publishing certification practice statements. A third-party certification authority, including the same one that issued the service provider its parent certificate, could act as the CA that issues delegate certificates for the service provider, if the necessary business relationships permit it. A service provider might in this case act as a Token Authority (see Section 8.1) granting its customers permissions to receive certificates from the CA.

Note that if the same CA that issued the parent certificate is also issuing a delegate certificate, it may be possible to shorten the certification path, which reduces the work required of verification services. The trade-off here is that if the CA simply issued a non-delegate certificate (whose parent is the CA's trust anchor) with the proper `TNAuthList` value, relying parties might not be able to ascertain which service provider owned those telephone numbers, information which might be used to make an authorization decision on the terminating side. However, some additional object in the certificate outside of the `TNAuthList` could preserve that information; this is a potential area for future work, and longer certification paths are the only mechanism currently defined.

All CAs must detail in their practices and policies a requirement to validate that the "encompassing" of a delegate certificate by its parent. Note that this requires that CAs have access to the necessary industry databases to ascertain whether, for example, a particular telephone number is encompassed by an SPC. Alternatively, a CA may acquire an Authority Token (see Section 8.1) that affirms



that a delegation is in the proper scope. Exactly what operational practices this entails may vary in different national telephone administrations, and are thus left to the CP/CPS [RFC3647].

### 8.1. ACME and Delegation

STIR deployments commonly use ACME [RFC8555] for certificate acquisition, and it is anticipated that delegate certificates as well will be acquired through an ACME interface. An entity can acquire a certificate from a particular CA by requesting an Authority Token [I-D.ietf-acme-authority-token] from the parent with the desired TNAuthList [I-D.ietf-acme-authority-token-tnauthlist] object. Note that if the client intends to do further subdelegation of its own, it should request a token with the "ca" Authority Token flag set.

The entity then presents that Authority Token to a CA to acquire a STIR delegate certificate. ACME returns an "application/pem-certificate-chain" object, and that object would be suitable for publishing as an HTTPS resource for retrieval with the PASSport "x5u" mechanism as discussed in Section 7. If the CSR presented to the ACME server is for a certificate with the ca boolean set to "true", then the ACME server makes a policy decision to determine whether or not it is appropriate to issue that certificate to the requesting entity. That policy decision will be reflected by the "ca" flag in the Authority Token.

Service providers that want the capability to rapidly age out delegated certificates can rely on the ACME STAR [I-D.ietf-acme-star] mechanism to automate the process of short-term certificate expiry.

### 8.2. Handling Multiple Certificates

In some deployments, non-carrier entities may receive telephone numbers from several different carriers. This could lead to enterprises needing to maintain a sort of STIR keyring, with different certificates delegated to them from different providers, potentially issued by different CAs, which they choose between when signing a call. This could be the case regardless of which syntax is used in the TNAuthList to represent the scope of the delegation (see Section 4.1). As noted in Section 8, if the parent certs use the same CA, it may be possible to shorten the certification path.

For non-carrier entities handling a small number of certificates, this is probably not a significant burden. For cases where it becomes burdensome, a few potential approaches exist. A delegate certificate could be cross-certified with another delegate certificate via an Authority Information Access field containing the URL of a Certificate Authority Issuer, so that a signer would only

need to sign with a single certificate to inherit the privileges of the other certificate(s) it has cross-certified with. In very complex delegation cases, it might make more sense to establish a bridge CA that cross-certifies with all of the certificates held by the enterprise, rather than requiring a mesh of cross-certification between a large number of certificates. Again, this bridge CA function would likely be performed by some existing CA in the STIR ecosystem. These procedures would however complicate the fairly straightforward certification path reconstruction approach described in Section 7 and would require further specification.

## 9. Alternative Solutions

At the time this specification was written, STIR was only starting to see deployment. In some future environment, the policies that govern CAs may not permit them to issue intermediate certificates with a TNAuthList object and a cA boolean set to "true" in the basic constraints certificate extension [RFC5280]. Similar problems in the web PKI space motivated the development of TLS subcerts [I-D.ietf-tls-subcerts], which substitutes a signed "delegated credential" token for a certificate for such environments. A comparable mechanism could be developed for the STIR space, allowing STIR certificates to sign a data object which contains effectively the same data as the delegate certificate specified here, including a public key that could sign PASSporTs. The TLS subcerts system has furthermore exploring leveraging ACME to issue short-lived certificates for temporary delegation as a means of obviating the need for revocation. Specification of a mechanism similar to TLS subcerts for STIR is future work, and will be undertaken only if the market require it.

## 10. IANA Considerations

This document contains no actions for the IANA.

## 11. Privacy Considerations

Any STIR certificate that identifies a narrow range of telephone numbers potentially exposes information about the entities that are placing calls. As such a telephone number range is necessarily a superset of the calling party number that is openly signaled during call setup, the privacy risks associated with this mechanism are not substantially greater than baseline STIR. See [RFC8224] for guidance on the use of anonymization mechanisms in STIR.

## 12. Security Considerations

This document is entirely about security. As delegation can allow signing in scenarios where unauthenticated "legitimate" spoofing would otherwise be used, it is hoped that delegation will improve the overall security of the STIR ecosystem. For further information on certificate security and practices, see [RFC5280], in particular its Security Considerations. Also see the Security Considerations of [RFC8226] for general guidance on the implications of the use of certificates in STIR, and [RFC7375] for the STIR threat model.

Much of the security of delegation depends on the implementation of the encompassing semantics described in Section 4. When delegating from an SPC-based TNAuthList to a set of telephone number ranges, understanding the encompassing semantics may require access to industry databases that track the numbering assets of service providers associated with a given SPC. In some operating environments, such databases might not exist. How encompassing is policed is therefore a matter outside the scope of this document, and specific to operational profiles of STIR.

The use of by-reference TNAuthLists as described in Section 4 entails that the TNAuthList associated with a certificate can change over time; see the security considerations of [RFC3986] for more on the implications of this property. It is considered a useful feature here due to the potential dynamism of large lists of telephone numbers, but this dynamism entails that a relying party might once accept that a particular telephone number is associated with a certificate, but later reject it for the same certificate as the dynamic list changes. Also that note if the HTTPS service housing the by-reference telephone number list is improperly secured, that too can lead to vulnerabilities. Ultimately, the CA that issued a delegated certificate populates the URL in the AIA field, and is responsible for making a secure selection. Service providers acting as CAs are directed to the cautionary words about running a CA in Section 8 regarding the obligations this entails for certificate revocation and so on.

## 13. Acknowledgments

We would like to thank Ines Robles, Richard Barnes, Chris Wendt, Dave Hancock, Russ Housley, Benjamin Kaduk, and Sean Turner for key input on this document.

## 14. References

### 14.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <<https://www.rfc-editor.org/info/rfc3986>>.
- [RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <<https://www.rfc-editor.org/info/rfc5280>>.
- [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>>.
- [RFC8555] Barnes, R., Hoffman-Andrews, J., McCarney, D., and J. Kasten, "Automatic Certificate Management Environment (ACME)", RFC 8555, DOI 10.17487/RFC8555, March 2019, <<https://www.rfc-editor.org/info/rfc8555>>.

## 14.2. Informative References

- [I-D.ietf-acme-authority-token]  
Peterson, J., Barnes, M., Hancock, D., and C. Wendt, "ACME Challenges Using an Authority Token", draft-ietf-acme-authority-token-05 (work in progress), March 2020.
- [I-D.ietf-acme-authority-token-tnauthlist]  
Wendt, C., Hancock, D., Barnes, M., and J. Peterson, "TNAuthList profile of ACME Authority Token", draft-ietf-acme-authority-token-tnauthlist-06 (work in progress), March 2020.
- [I-D.ietf-acme-star]  
Sheffer, Y., Lopez, D., Dios, O., Pastor, A., and T. Fossati, "Support for Short-Term, Automatically-Renewed (STAR) Certificates in Automated Certificate Management Environment (ACME)", draft-ietf-acme-star-11 (work in progress), October 2019.
- [I-D.ietf-tls-subcerts]  
Barnes, R., Iyengar, S., Sullivan, N., and E. Rescorla, "Delegated Credentials for TLS", draft-ietf-tls-subcerts-10 (work in progress), January 2021.
- [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>>.
- [RFC3647] Chokhani, S., Ford, W., Sabett, R., Merrill, C., and S. Wu, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", RFC 3647, DOI 10.17487/RFC3647, November 2003, <<https://www.rfc-editor.org/info/rfc3647>>.
- [RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480, February 2012, <<https://www.rfc-editor.org/info/rfc6480>>.
- [RFC7340] Peterson, J., Schulzrinne, H., and H. Tschofenig, "Secure Telephone Identity Problem Statement and Requirements", RFC 7340, DOI 10.17487/RFC7340, September 2014, <<https://www.rfc-editor.org/info/rfc7340>>.

- [RFC7375] Peterson, J., "Secure Telephone Identity Threat Model", RFC 7375, DOI 10.17487/RFC7375, October 2014, <<https://www.rfc-editor.org/info/rfc7375>>.
- [X.509] ITU-T Recommendation X.509 (10/2012) | ISO/IEC 9594-8, "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks", 2012.

Author's Address

Jon Peterson  
Neustar, Inc.

Email: [jon.peterson@team.neustar](mailto:jon.peterson@team.neustar)

Network Working Group  
Internet-Draft  
Updates: 8226 (if approved)  
Intended status: Standards Track  
Expires: 27 January 2022

R. Housley  
Vigil Security  
26 July 2021

Enhanced JWT Claim Constraints for STIR Certificates  
draft-ietf-stir-enhance-rfc8226-05

Abstract

RFC 8226 specifies the use of certificates for Secure Telephone Identity Credentials, and these certificates are often called "STIR Certificates". RFC 8226 provides a certificate extension to constrain the JSON Web Token (JWT) claims that can be included in the Personal Assertion Token (PASSporT) as defined in RFC 8225. If the PASSporT signer includes a JWT claim outside the constraint boundaries, then the PASSporT recipient will reject the entire PASSporT. This document updates RFC 8226; it provides all of the capabilities available in the original certificate extension as well as an additional way to constrain the allowable JWT claims. The enhanced extension can also provide a list of claims that are not allowed to be included in the PASSporT.

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 27 January 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. Enhanced JWT Claim Constraints Syntax . . . . .	3
4. Usage Examples . . . . .	5
5. Certificate Extension Example . . . . .	5
6. Guidance to Certification Authorities . . . . .	7
7. IANA Considerations . . . . .	7
8. Security Considerations . . . . .	7
9. Acknowledgements . . . . .	8
10. References . . . . .	8
10.1. Normative References . . . . .	8
10.2. Informative References . . . . .	9
Appendix A. ASN.1 Module . . . . .	10
Author's Address . . . . .	11

## 1. Introduction

The use of certificates [RFC5280] in establishing authority over telephone numbers is described in [RFC8226]. These certificates are often called "STIR Certificates". STIR certificates are an important element of the overall system that prevents the impersonation of telephone numbers on the Internet.

Section 8 of [RFC8226] provides a certificate extension to constrain the JSON Web Token (JWT) claims that can be included in the Personal Assertion Token (PASSporT) [RFC8225]. If the PASSporT signer includes a JWT claim outside the constraint boundaries, then the PASSporT recipient will reject the entire PASSporT.

This document defines an enhanced JWTClaimConstraints certificate extension, which provides all of the capabilities available in the original certificate extension as well as an additional way to constrain the allowable JWT claims. That is, the enhanced extension can provide a list of claims that are not allowed to be included in the PASSporT.



The Enhanced JWT Claim Constraints certificate extension is needed to limit the authority when a parent STIR certificate delegates to a subordinate STIR certificate. For example, [I-D.ietf-stir-cert-delegation] describes the situation where service providers issue a STIR certificate to enterprises or other customers to sign PASSporTs, and the Enhanced JWT Claim Constraints certificate extension can be used to prevent specific claims from being included in PASSporTs and accepted as valid by the PASSporT recipient.

The JWT Claim Constraints certificate extension defined in [RFC8226] provides a list of claims that must be included in a valid PASSporT as well as a list of permitted values for selected claims. The Enhanced JWT Claim Constraints certificate extension defined in this document includes those capabilities and adds a list of claims that must not be included in a valid PASSporT.

## 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. Enhanced JWT Claim Constraints Syntax

The Enhanced JWT Claim Constraints certificate extension is non-critical, applicable only to end-entity certificates, and defined with ASN.1 [X.680]. The syntax of the JWT claims in a PASSporT is specified in [RFC8225].

The Enhanced JWT Claim Constraints certificate extension is optional, but when present, it constrains the JWT claims that authentication services may include in the PASSporT objects they sign. Constraints are applied by certificate issuers and enforced by recipients when validating PASSporT claims as follows:

1. `mustInclude` indicates JWT claims that MUST appear in the PASSporT in addition to the `iat`, `orig`, and `dest` claims. The baseline PASSporT claims ("`iat`", "`orig`", and "`dest`") are considered to be required by [RFC8225], and these claims SHOULD NOT be part of the `mustInclude` list. If `mustInclude` is absent, the `iat`, `orig`, and `dest` claims MUST appear in the PASSporT.
2. `permittedValues` indicates that if the claim name is present, the claim MUST exactly match one of the listed values.

3. mustExclude indicates JWT claims that MUST NOT appear in the PASSporT. The baseline PASSporT claims ("iat", "orig", and "dest") are always permitted, and these claims MUST NOT be part of the mustExclude list. If one of these baseline PASSporT claims appears in the mustExclude list, then the certificate MUST be treated as if the extension was not present.

Following the precedent in [RFC8226], JWT Claim Names MUST be ASCII strings, which are also known as strings using the International Alphabet No. 5 [ISO646].

The Enhanced JWT Claim Constraints certificate extension is identified by the following object identifier (OID):

```
id-pe-eJWTClaimConstraints OBJECT IDENTIFIER ::= { id-pe 33 }
```

The Enhanced JWT Claim Constraints certificate extension has the following syntax:

```
EnhancedJWTClaimConstraints ::= SEQUENCE {
    mustInclude [0] JWTClaimNames OPTIONAL,
    -- The listed claim names MUST appear in the PASSporT
    -- in addition to iat, orig, and dest. If absent, iat, orig,
    -- and dest MUST appear in the PASSporT.
    permittedValues [1] JWTClaimValuesList OPTIONAL,
    -- If the claim name is present, the claim MUST contain one
    -- of the listed values.
    mustExclude [2] JWTClaimNames OPTIONAL }
    -- The listed claim names MUST NOT appear in the PASSporT.
( WITH COMPONENTS { ..., mustInclude PRESENT } |
  WITH COMPONENTS { ..., permittedValues PRESENT } |
  WITH COMPONENTS { ..., mustExclude PRESENT } )

JWTClaimValuesList ::= SEQUENCE SIZE (1..MAX) OF JWTClaimValues

JWTClaimValues ::= SEQUENCE {
    claim JWTClaimName,
    values SEQUENCE SIZE (1..MAX) OF UTF8String }

JWTClaimNames ::= SEQUENCE SIZE (1..MAX) OF JWTClaimName

JWTClaimName ::= IA5String
```

#### 4. Usage Examples

Consider these usage examples with a PASSporT claim called "confidence" with values "low", "medium", and "high". These examples illustrate the constraints that are imposed by mustInclude, permittedValues, and mustExclude:

- \* If a CA issues a certificate to an authentication service that includes an Enhanced JWT Claim Constraints certificate extension that contains the mustInclude JWTClaimName "confidence", then an authentication service is required to include the "confidence" claim in all PASSporTs it generates and signs. A verification service will treat as invalid any PASSporT it receives without a "confidence" PASSporT claim.
- \* If a CA issues a certificate to an authentication service that includes an Enhanced JWT Claim Constraints certificate extension that contains the permittedValues JWTClaimName "confidence" and a permitted "high" value, then a verification service will treat as invalid any PASSporT it receives with a PASSporT "confidence" claim with a value other than "high". However, a verification service will not treat as invalid a PASSporT it receives without a PASSporT "confidence" claim at all, unless "confidence" also appears in mustInclude.
- \* If a CA issues a certificate to an authentication service that includes an Enhanced JWT Claim Constraints certificate extension that contains the mustExclude JWTClaimName "confidence", then a verification service will treat as invalid any PASSporT it receives with a PASSporT "confidence" claim regardless of the claim value.

#### 5. Certificate Extension Example

A certificate containing an example of the EnhancedJWTClaimConstraints certificate extension is provided in Figure 1. The certificate is provided in the format described in [RFC7468]. The example of the EnhancedJWTClaimConstraints extension from the certificate is shown in Figure 2. The example imposes four constraints:

1. The "confidence" claim must be present in the PASSporT.
2. The "confidence" claim must have a value of "high" or "medium".
3. The "priority" claim must not be present in the PASSporT.

NOTE: This certificate in Figure 1 will need to be corrected once IANA assigns the object identifier for the certificate extension.

```

-----BEGIN CERTIFICATE-----
MIICpzCCAk2gAwIBAgIUH7Zd3rQ5AsvOlzLnzUHhrVhDSlswCgYIKoZIzj0EAwIw
KTELMAkGA1UEBhMCVVMxGjAYBgNVBAMMEUJPRlVTIFNlQUtFTiBST09UMB4XDTIx
MDcxNTIxNTIxNVVoXDTIyMDcxNTIxNTIxNVowbDELMAkGA1UEBhMCVVMxCzAJBgNV
BAGMA1ZBMRAwDgYDVQQHDAdlZXJuZG9uMR4wHAYDVQQKDBVChb2dlcyBFcGFtcGxl
IFRlbGVjb20xDTALBgNVBASMBFZvSVAXDzANBgNVBAMMB1NIQUtFTjBZMBMGByqG
SM49AgEGCCqGSM49AwEHA0IABNR6C6nBWRA/fXTglV03aXkXy8hx9oBttVLhsTZl
IYVRBao4OZhVf/Xv1a3xLsZ6KfdhuylSeAKuCoSbVGojYDGjggEOMIIBCjAMBgNV
HRMBAf8EAjAAMA4GA1UdDwEB/wQEAwIHgDAdBgNVHQ4EFgQUUDlG3dxHyZKL/FZfS
PI7rpueRbswHwYDVR0jBBgwFoAUlToKtrQeFrwwyXpMj1qu3TQEeoEwQgYJYIZI
AYb4QgENBDUWM1RoaXMgY2VydgGmaWNhdGUgY2Fubm90IGJlIHRYdXN0ZWQgZm9y
IGFueSBwdXJwb3NlLjAwBggrBgEFBQcCBGgQKMAigBhYEMTIzNDBOBggrBgEFBQcB
IQRCEMECgDjAMFgppjb25maWRlbnNlOjSAwHjAcFgppjb25maWRlbnNlMA4MBGhpZ2gM
Bml1ZGllbWlbaIMMAoWCHByaW9yaXR5MAoGCCqGSM49BAMCA0gAMEUCIQCbNR4QKlum
+0vq2CElB1/W3avYeREsPi/7RKHffL+5eQIgarHot+X9Rl7SoyNBq5X5JyEMx0SQ
hRLkCY3Zoz2OCNQ=
-----END CERTIFICATE-----

```

Figure 1. Example Certificate.

```

0 64: SEQUENCE {
2 14:   [0] {
4 12:     SEQUENCE {
6 10:       IA5String 'confidence'
      :     }
      :   }
18 32:   [1] {
20 30:     SEQUENCE {
22 28:       SEQUENCE {
24 10:         IA5String 'confidence'
36 14:         SEQUENCE {
38 4:           UTF8String 'high'
44 6:           UTF8String 'medium'
      :         }
      :       }
      :     }
      :   }
52 12:   [2] {
54 10:     SEQUENCE {
56 8:       IA5String 'priority'
      :     }
      :   }
      : }

```

Figure 2. Example EnhancedJWTClaimConstraints extension.

## 6. Guidance to Certification Authorities

The EnhancedJWTClaimConstraints extension specified in this document and the JWTClaimConstraints extension specified in [RFC8226] MUST NOT both appear in the same certificate.

If the situation calls for mustExclude constraints, then the EnhancedJWTClaimConstraints extension is the only extension that can express the constraints.

On the other hand, if the situation does not call for mustExclude constraints, then either the EnhancedJWTClaimConstraints extension or the JWTClaimConstraints extension can express the constraints. Until such time as support for the EnhancedJWTClaimConstraints extension becomes widely implemented, the use of the JWTClaimConstraints extension may be more likely to be supported. This guess is based on the presumption that the first specified extension will be implemented more widely in the next few years.

## 7. IANA Considerations

This document makes use of object identifiers for the Enhanced JWT Claim Constraints certificate extension defined in Section 3 and the ASN.1 module identifier defined in Appendix A. Therefore, IANA has made the following assignments within the SMI Numbers Registry.

For the Enhanced JWT Claim Constraints certificate extension in the "SMI Security for PKIX Certificate Extension" (1.3.6.1.5.5.7.1) registry:

```
33 id-pe-eJWTClaimConstraints
```

For the ASN.1 module identifier in the "SMI Security for PKIX Module Identifier" (1.3.6.1.5.5.7.0) registry:

```
101 id-mod-eJWTClaimConstraints-2021
```

## 8. Security Considerations

For further information on certificate security and practices, see [RFC5280], especially the Security Considerations section.

Since non-critical certificate extension are ignored by implementations that do not recognize the extension object identifier (OID), constraints on PASSporT validation will only be applied by relying parties that recognize the EnhancedJWTClaimConstraints extension.

The Enhanced JWT Claim Constraints certificate extension can be used by certificate issuers to provide limits on the acceptable PASSports that can be accepted by verification services. Enforcement of these limits depends upon proper implementation by the verification services. The digital signature on the PASSportT data structure will be valid even if the limits are violated.

Use of the Enhanced JWT Claim Constraints certificate extension permittedValues constraint is most useful when the claim definition allows a specified set of values. In this way, all of the values that are not listed in the JWTClaimValuesList are prohibited in a valid PASSport.

Certificate issuers must take care when imposing constraints on the PASSport claims and the claim values that can successfully validated; some combinations can prevent any PASSport from being successfully validated by the certificate. For example, an entry in mustInclude and an entry in mustExclude for the same claim will prevent successful validation on any PASSport.

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 [I-D.ietf-stir-passport-rcd]. Excluding this claim would prevent the integrity protection mechanism from working properly.

Certificate issuers must take care when performing certificate renewal [RFC4949] to include exactly the same Enhanced JWT Claim Constraints certificate extension in the new certificate as the old one. Renewal usually takes place before the old certificate expires, so there is a period of time where both the new certificate and the old certificate are valid. If different constraints appear in the two certificates with the same public key, some PASSports might be valid when one certificate is used and invalid when the other one is used.

## 9. Acknowledgements

Many thanks to Chris Wendt for his insight into the need for the for the Enhanced JWT Claim Constraints certificate extension.

Thanks to Ben Campbell, Theresa Enghardt, Ben Kaduk, Erik Kline, Eric Vyncke, and Rob Wilton for their thoughtful review and comments. The document is much better as a result of their efforts.

## 10. References

### 10.1. 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>>.
- [RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <<https://www.rfc-editor.org/info/rfc5280>>.
- [RFC5912] Hoffman, P. and J. Schaad, "New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)", RFC 5912, DOI 10.17487/RFC5912, June 2010, <<https://www.rfc-editor.org/info/rfc5912>>.
- [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>>.
- [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>>.
- [X.680] International Telecommunication Union, "Information Technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation", ISO/IEC 8824-1, August 2021.

## 10.2. Informative References

- [I-D.ietf-stir-cert-delegation]  
Peterson, J., "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-passport-rcd]  
Wendt, C. and J. Peterson, "PASSporT Extension for Rich Call Data", Work in Progress, Internet-Draft, draft-ietf-stir-passport-rcd-12, 12 July 2021, <<https://www.ietf.org/archive/id/draft-ietf-stir-passport-rcd-12.txt>>.

- [ISO646] International Organization for Standardization, "Information processing - ISO 7-bit coded character set for information interchange", ISO/IEC 646:1991, December 1991.
- [RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <<https://www.rfc-editor.org/info/rfc4949>>.
- [RFC7468] Josefsson, S. and S. Leonard, "Textual Encodings of PKIX, PKCS, and CMS Structures", RFC 7468, DOI 10.17487/RFC7468, April 2015, <<https://www.rfc-editor.org/info/rfc7468>>.

## Appendix A. ASN.1 Module

This appendix provides the ASN.1 [X.680] definitions for the Enhanced JWT Claim Constraints certificate extension. The module defined in this appendix are compatible with the ASN.1 specifications published in 2015.

This ASN.1 module imports ASN.1 from [RFC5912].

<CODE BEGINS>

EnhancedJWTClaimConstraints-2021

```
{ iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) id-mod(0)
  id-mod-eJWTClaimConstraints-2021(101) }
```

DEFINITIONS EXPLICIT TAGS ::= BEGIN

IMPORTS

id-pe

FROM PKIX1Explicit-2009 -- From RFC 5912

```
{ iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) id-mod(0)
  id-mod-pkix1-explicit-02(51) }
```

EXTENSION

FROM PKIX-CommonTypes-2009 -- From RFC 5912

```
{ iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) id-mod(0)
  id-mod-pkixCommon-02(57) } ;
```

-- Enhanced JWT Claim Constraints Certificate Extension

```
ext-eJWTClaimConstraints EXTENSION ::= {
  SYNTAX EnhancedJWTClaimConstraints
```



```
IDENTIFIED BY id-pe-eJWTClaimConstraints }

id-pe-eJWTClaimConstraints OBJECT IDENTIFIER ::= { id-pe 33 }

EnhancedJWTClaimConstraints ::= SEQUENCE {
    mustInclude [0] JWTClaimNames OPTIONAL,
        -- The listed claim names MUST appear in the PASSport
        -- in addition to iat, orig, and dest.  If absent, iat, orig,
        -- and dest MUST appear in the PASSport.
    permittedValues [1] JWTClaimValuesList OPTIONAL,
        -- If the claim name is present, the claim MUST contain one
        -- of the listed values.
    mustExclude [2] JWTClaimNames OPTIONAL }
    -- The listed claim names MUST NOT appear in the PASSport.
( WITH COMPONENTS { ..., mustInclude PRESENT } |
  WITH COMPONENTS { ..., permittedValues PRESENT } |
  WITH COMPONENTS { ..., mustExclude PRESENT } )

JWTClaimValuesList ::= SEQUENCE SIZE (1..MAX) OF JWTClaimValues

JWTClaimValues ::= SEQUENCE {
    claim JWTClaimName,
    values SEQUENCE SIZE (1..MAX) OF UTF8String }

JWTClaimNames ::= SEQUENCE SIZE (1..MAX) OF JWTClaimName

JWTClaimName ::= IA5String

END
<CODE ENDS>
```

## Author's Address

Russ Housley  
Vigil Security, LLC  
516 Dranesville Road  
Herndon, VA, 20170  
United States of America  
  
Email: housley@vigilsec.com

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

C. Wendt  
Somos Inc.  
J. Peterson  
Neustar Inc.  
24 April 2022

PASSport Extension for Rich Call Data  
draft-ietf-stir-passport-rcd-17

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 26 October 2022.

## Copyright Notice

Copyright (c) 2022 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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised 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 . . . . .	7
5.1.3. "icn" key . . . . .	8
5.1.4. "jcd" key . . . . .	9
5.1.5. "jcl" key . . . . .	9
6. "rcdi" RCD Integrity Claim Definition and Usage . . . . .	10
6.1. Creation of the "rcd" element digests . . . . .	11
6.1.1. "nam" and "apn" elements . . . . .	12
6.1.2. "icn" elements . . . . .	12
6.1.3. "jcd" elements . . . . .	12
6.1.4. "jcl" elements . . . . .	14
6.2. JWT Claim Constraints for "rcd" claims only . . . . .	15
7. JWT Claim Constraints usage for "rcd" and "rcdi" claims . . . . .	15
8. PASSporT "crn" claim - Call Reason Definition and Usage . . . . .	16
8.1. JWT Constraint for "crn" claim . . . . .	16
9. Rich Call Data Claims Usage Rules . . . . .	17
9.1. "rcd" PASSporT Verification . . . . .	17
9.2. "rcdi" Integrity Verification . . . . .	18
9.3. Example "rcd" PASSporTs . . . . .	18
10. Compact form of "rcd" PASSporT . . . . .	20
10.1. Compact form of the "rcd" PASSporT claim . . . . .	20
10.2. Compact form of the "rcdi" PASSporT claim . . . . .	21
10.3. Compact form of the "crn" PASSporT claim . . . . .	21
11. Further Information Associated with Callers . . . . .	21
12. Third-Party Uses . . . . .	22

12.1. Signing as a Third Party . . . . .	23
13. Levels of Assurance . . . . .	24
14. Using "rcd" in SIP . . . . .	24
14.1. Authentication Service Behavior . . . . .	24
14.2. Verification Service Behavior . . . . .	25
15. Using "rcd" and "rcdi" as additional claims to other PASSporT extensions . . . . .	26
15.1. Procedures for applying "rcd" as claims only . . . . .	27
15.2. Example for applying "rcd" as claims only . . . . .	27
16. Acknowledgements . . . . .	28
17. IANA Considerations . . . . .	28
17.1. JSON Web Token Claim . . . . .	28
17.2. PASSporT Types . . . . .	29
17.3. PASSporT RCD Types . . . . .	29
18. Security Considerations . . . . .	29
18.1. The use of JWT Claim Constraints in delegate certificates to exclude unauthorized claims . . . . .	30
19. References . . . . .	30
19.1. Normative References . . . . .	30
19.2. Informative References . . . . .	32
Authors' Addresses . . . . .	32

## 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 an "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 each resource referenced by a URI within a claim value (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 [RFC9118]. 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 an "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 [RFC9060] 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. "icn" key

The "icn" key value is an optional URI reference to an image that can be used to pictorially represent the originator of personal communications. This icon key value should be used as a base or default method of associating an image with a calling party.

When being used for SIP [RFC3261] this claim key value used to protect the call-info header field with a purpose parameter value of "icon" as described in Section 20.9 [RFC3261]. Example as follows:

```
Call-Info: <http://www.example.com/alice/photo.jpg>;  
  purpose=icon
```

Note that [I-D.ietf-sipcore-callinfo-rcd] extends the specific usage of "icon" in SIP in the context of the larger rich call data framework with specific guidance on referencing images and image types, sizes and formats.

It should be also noted that with jCard, as described in the following "jcd" and "jcl" key value sections and in [I-D.ietf-sipcore-callinfo-rcd], there are alternative ways of including photos and logos as URI references. The "icn" key should be then considered a base or default image and jCard usage should be considered for profiles and extensions that provide more direct guidance on the usage of specific defined usage of what each image type represents for the proper rendering to end users.

#### 5.1.4. "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 an "rcd" PASSport, other future specifications and protocols are encouraged to be adapted for use of "jcd" (or similarly "jcl" below) key beyond SIP and Call-Info.

#### 5.1.5. "jcl" key

The "jcl" key value is defined to contain a URI 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 the integrity overview Section 4 of this document. If this claim is present it MUST be included only 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" : {  
  "/jcl": "sha256-7kdCBZqH0nqMSPsmABvsKlHPhZESTgjojhdSJGRr3rk",  
  "/jcl/1/2/3": "sha256-jL4f47fF82LuwcrOrSyckA4SWr1ElfARHkW6kYo1JdI"  
}
```

The values of each key/value pair consists of a digest across either the direct values or indirectly referenced resources, 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", "icn", "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 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 a value that is a part or the whole of a JSON object or to a string that is a URI referencing an external resource.
2. For a JSON value, serialize the 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 is the input for the hash function.
3. For any URI referenced content, the bytes of the body of the HTTP response is the input for the hash function.

#### 6.1.1. "nam" and "apn" elements

In the case of "nam" and "apn", the only allowed value is a string. For both of these key values an "rcdi" JSON pointer or integrity digest is optional because the direct value is protected by the signature and can be constrained directly with JWTClaimConstraints. If used, the JSON key value referenced by the JSON pointer is the string includes the quotes, so quotes MUST be included to compute the digest.

#### 6.1.2. "icn" elements

In the case of "icn", the only allowed value is a URI value that references an image file. If the URI references externally linked content there would need to be a JSON pointer and digest entry for the content in that linked resource. In order to reference the "icn" value for a digest, the JSON pointer string would be "/icn" and the digest string would be created using the image file data following the rules of JSON pointer. Even though this is probably not the typical case, an "rcdi" JSON pointer or integrity digest is optional if the image value is directly included via a data URI. However, even though the direct value can be protected by the signature and can be constrained directly with JWTClaimConstraints, since the length of the image data is likely much larger than the integrity digest, this specification would recommend the use of the "rcdi" JSON pointer and integrity digest as the constraint value in JWTClaimConstraints over the image data.

#### 6.1.3. "jcd" elements

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": {
  "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"]
    ]
  ],
  "nam": "Q Branch Spy Gadgets"
}

```

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-tbxXX9mRY2dtss3vNdNkNkt9hrV9N1LqGST2hDlw97I",
  "/jcd/1/3/3": "sha256-RojgWwU6xUtI4q82+kHPyHm1JKbm7+663bMvzymhk14",
  "/jcd/1/4/3": "sha256-jL4f47fF82LuwcrOrSyckA4SWr1ElfARHkW6kYo1JdI",
  "/jcd/1/5/3": "sha256-GKNxxqlLRarbyBNh7hc/4lbZAdK6B0kMRf1AMRWPkSo"
}

```

The use of a JSON pointer and integrity digest for the "jcd" claim key and value is optional. The "jcd" value is the directly included jCard array and can be protected by the signature and can be constrained directly with JWTClaimConstraints. However, for data length reasons (as with "icn" above) or more importantly for potential privacy and/or security considerations with a publically accessible certificate this specification would recommend the use of the "rcdi" JSON pointer and integrity digest as the constraint value in JWTClaimConstraints over the jCard data.

It is important to remember the array indexes for JSON Pointer are dependent on the order of the elements in the jCard. The use of digest for the "/jcd" corresponding to the entire jCard array string can be included as a redundant mechanism to avoid any possibility of substitution, insertion attacks, or other potential techniques 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.

#### 6.1.4. "jcl" elements

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": {
  "jcl": "https://example.com/qbranch.json",
  "nam": "Q Branch Spy Gadgets"
},
"rcdi": {
  "/jcl": "sha256-Gb010kj7Z9+plqbOkN32H+YX0Yav3fbioSk7DxQdGZU",
  "/jcl/1/3/3": "sha256-RojgWwU6xUtI4q82+kHPyHm1JKbm7+663bMvzymhkl4",
  "/jcl/1/4/3": "sha256-jL4f47fF82LuwcrOrSyckA4SWr1ElfARHkW6kYo1JdI",
  "/jcl/1/5/3": "sha256-GKNxxqlLRarbyBNh7hc/4lbZAdK6B0kMRf1AMRWPkSo"
}
```

The following is the example contents of resource pointed to by <https://example.com/qbranch.json> used to calculate the above digest for "/jcl"

```
[ "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" ]
  ]
]
```

## 6.2. JWT Claim Constraints for "rcd" claims only

For the third mode described in the integrity overview Section 4 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 4 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 objective 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 extension 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 [RFC9060] 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 extension MUST include both of the following:

- \* a "mustInclude" for the "rcd" claim, which simply constrains the fact that an "rcd" must be included



- \* 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 (or "rcd" claims more generally) 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 can contain information as defined in [I-D.ietf-sipcore-callinfo-rcd] corresponding to the "call-reason" parameter for the Call-Info header. This claim is optional.

Example "crn" claim with "rcd":

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

As also noted in [I-D.ietf-sipcore-callinfo-rcd] this claim is included as corresponding to "call-reason" Call-Info parameter, but there is an alternative suggested way to include call-reason which is to use the "cif" claim with a "call-reason" key value, as defined below in this document.

### 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 an "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. "rcd" PASSporT Verification

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

- \* have a valid signature
- \* 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 [RFC9118] if present in the certificate used to sign the PASSporT

Consistent with the verification rules of PASSporTs more generally [RFC8225], if any of the above criteria is not met, relying parties MUST NOT use any of the claims in the PASSporT.

## 9.2. "rcdi" Integrity Verification

If the "rcdi" claim exists, any party that dereferences a URI (i.e. downloading content for display to users) from the "rcd" claim MUST perform integrity validation of the content against the corresponding digest. Consequently, if URIs with contents covered by integrity digests are passed to another entity, the corresponding integrity digest MUST also be included, for example by passing the PASSporT. Entities that pass on the content without the URI do not have to pass on the corresponding integrity digest. An entity that does not otherwise need to dereference a URI from the "rcd" claim would be discouraged from unnecessarily dereferencing the URI solely to perform integrity verification.

If there is any issue with completing the integrity verification procedures for externally referenced content, including HTTP or HTTPS errors, the referenced content MUST be considered not verified. This SHOULD NOT however impact the result of base PASSporT verification for claims content that is directly included in the claims of the PASSporT.

## 9.3. 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 an "rcd" claims object that includes the "jcd" and also contains URI references to content which requires the inclusion of an "rcdi" claim and corresponding digests.

```

{
  "crn": "Rendezvous for Little Nellie",
  "orig": { "tn": "12025551000"},
  "dest": { "tn": ["12155551001"]},
  "iat": 1443208345,
  "rcd": {
    "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"]
      ] ],
    "nam": "Q Branch Spy Gadgets"
  },
  "rcdi": {
    "/jcd/1/3/3": "sha256-RojgWwU6xUtI4q82+kHPyHm1JKbm7+663bMvzymhkl4",
    "/jcd/1/4/3": "sha256-jL4f47fF82LuwcrOrSyckA4SWrlElfARHkW6kYo1JdI",
    "/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 hosted at the example web address of <https://example.com/qbranch.json> is shown as follows:

```

["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"]
  ]
]

```

For the above referenced jCard, the corresponding PASSporT claims object would be as follows:

```
{
  "crn": "Rendezvous for Little Nellie",
  "orig": {"tn": "12025551000"},
  "dest": {"tn": ["12155551001"]},
  "iat": 1443208345,
  "rcd": {
    "nam": "Q Branch Spy Gadgets",
    "jcl": "https://example.com/qbranch.json"
  },
  "rcdi": {
    "/jcl": "sha256-qCn4pEH6BJu7zXndLFuAP6DwlTv5fRmJlAFkqftwnCs",
    "/jcl/1/3/3": "sha256-RojgWwU6xUtI4q82+kHPyHm1JKbm7+663bMvzymhk14",
    "/jcl/1/4/3": "sha256-jL4f47fF82LuwcrOrSyckA4SWrlElfARHkW6kYo1JdI",
    "/jcl/1/5/3": "sha256-GKNxxq1LRarbyBNh7hc/41bZAdK6B0kMRf1AMRWPkSo"
  }
}
```

An example "rcd" PASSporT that uses "nam" and "icn" keys with "rcdi" for calling name and referenced icon image content:

```
{
  "crn": "Rendezvous for Little Nellie",
  "orig": {"tn": "12025551000"},
  "dest": {"tn": ["12155551001"]},
  "iat": 1443208345,
  "rcd": {
    "nam": "Q Branch Spy Gadgets",
    "icn": "https://example.com/photos/q-256x256.png"
  },
  "rcdi": {
    "/nam": "sha256-sM275lTgzCte+LHOKHtU4SxG8shl0o6OS4ot8IJQImY",
    "/icn": "sha256-RojgWwU6xUtI4q82+kHPyHm1JKbm7+663bMvzymhk14"
  }
}
```

## 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 that will be enumerated below, 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. "jcl" and "jcd" MAY NOT be used with compact form due to integrity rules and URI reference rules in this specification leading to too restrictive of a set of constraints. Future specifications may revisit this to propose a consistent and comprehensive way of addressing integrity and security of information.

## 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 [RFC8816] 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 an "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 an "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 an "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 an "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" and "rcdi" as additional claims to other PASSporT extensions

Rich Call Data, including calling name information, as a common example, is often data that is additive 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 originating the personal communications is supporting the authentication service for the calling identity and is the authority of the Rich Call Data, rather than creating multiple Identity header fields cooresponding to multiple PASSporT extensions, the authentication service can alternatively directly add the "rcd" claim to a PASSporT that authenticates the calling identity.

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 should 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.v002], 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" PASSporT extension claims and doesn't support "rcd" PASSporT extension, then the "rcd" claim is used during PASSporT signature validation but is otherwise ignored and disregarded.

## 16. Acknowledgements

We would like to thank David Hancock, Robert Sparks, Russ Housley, Eric Burger, Alec Fenichel, Ben Campbell, Jack Rickard, Jordan Simpson 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.

The use of JWTClaimConstraints, a mechanism defined in [RFC8226] and extended in [RFC9118] to constrain any of the RCD information in the public certificate by including that information in the certificate, depending on the availability in the deployment of the PKI system, may present a privacy issue. The use of "rcdi" claim and digests for representing JWT claim contents may be a recommended way of preventing the exposure of that information through the certificates which are often publically accessible and available.

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 [RFC9060], 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 [RFC9118] 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-04, 7 March 2022,  
<<https://www.ietf.org/archive/id/draft-ietf-sipcore-callinfo-rcd-04.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>>.
- [RFC9060] Peterson, J., "Secure Telephone Identity Revisited (STIR) Certificate Delegation", RFC 9060, DOI 10.17487/RFC9060, September 2021, <<https://www.rfc-editor.org/info/rfc9060>>.
- [RFC9118] Housley, R., "Enhanced JSON Web Token (JWT) Claim Constraints for Secure Telephone Identity Revisited (STIR) Certificates", RFC 9118, DOI 10.17487/RFC9118, August 2021, <<https://www.rfc-editor.org/info/rfc9118>>.

## 19.2. Informative References

- [ATIS-1000074.v002]  
ATIS/SIP Forum NNI Task Group, "Signature-based Handling of Asserted information using toKENS (SHAKEN) <[https://access.atis.org/apps/group\\_public/download.php/62391/ATIS-1000074.v002.pdf](https://access.atis.org/apps/group_public/download.php/62391/ATIS-1000074.v002.pdf)>", November 2021.
- [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>>.

## Authors' Addresses

Chris Wendt  
Somos Inc.  
Email: [chris-ietf@chriswendt.net](mailto:chris-ietf@chriswendt.net)

Jon Peterson  
Neustar Inc.  
Email: [jon.peterson@neustar.biz](mailto:jon.peterson@neustar.biz)

STIR  
Internet-Draft  
Intended status: Standards Track  
Expires: September 12, 2021

M. Dolly  
AT&T  
C. Wendt  
Comcast  
March 11, 2021

Assertion Values for a Resource Priority Header Claim and a SIP Priority  
Header Claim in Support of Emergency Services Networks  
draft-ietf-stir-rph-emergency-services-07

Abstract

This document adds new assertion values for a Resource Priority Header ("rph") claim and a new SIP Priority Header claim ("sph") for protection of the "psap-callback" value as part of the "rph" PASSporT extension, in support of the security of Emergency Services Networks for emergency call origination and callback.

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 September 12, 2021.

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. New Assertion Values for "rph" claim . . . . .	3
4. The SIP Priority header "sph" claim . . . . .	4
5. Order of Claim Keys . . . . .	5
6. Compact Form of PASSporT . . . . .	6
7. Acknowledgements . . . . .	6
8. IANA Considerations . . . . .	6
8.1. JSON Web Token claims . . . . .	6
9. Security Considerations . . . . .	6
10. References . . . . .	6
10.1. Normative References . . . . .	6
10.2. Informative References . . . . .	7
Authors' Addresses . . . . .	8

## 1. Introduction

Personal Assertion Token (PASSporT) Extension for Resource Priority Authorization [RFC8443] extended the Personal Assertion Token (PASSporT) specification defined in [RFC8225] to allow the inclusion of cryptographically signed assertions of authorization for the values populated in the Session Initiation Protocol (SIP) "Resource-Priority" header field [RFC4412]. [I-D.rosen-stir-emergency-calls] introduces the need and justification for the protection of both the SIP "Resource-Priority" and "Priority" header fields, used for categorizing the priority use of the call in the telephone network, specifically for emergency calls.

Compromise of the SIP "Resource-Priority" or "Priority" header fields could lead to misuse of network resources (i.e., during congestion scenarios), impacting the application services supported using the SIP "Resource-Priority" header field and the handling of Public Safety Answering Point (PSAP) callbacks.

[RFC8225] allows extensions by which an authority on the originating side verifying the authorization of a particular communication for the SIP "Resource-Priority" header field or the SIP "Priority" header field can use PASSporT claims to cryptographically sign the information associated with either the SIP "Resource-Priority" or "Priority" header field and convey assertion of those values by the signing party authorization. A signed SIP "Resource-Priority" or "Priority" header field will allow a receiving entity (including entities located in different network domains/boundaries) to verify

the validity of assertions to act on the information with confidence that the information has not been spoofed or compromised.

This document adds new "auth" array key values for a Resource Priority Header ("rph") claim defined in [RFC8443], in support of Emergency Services Networks for emergency call origination and callback. This document additionally defines a new PASSporT claim, "sph", including protection of the SIP Priority header field for the indication of an emergency service call-back assigned the value "psap-callback" as defined in [RFC7090]. The use of the newly defined claim and key values corresponding to the SIP 'Resource-Priority' and 'Priority' header fields for emergency services is introduced in [I-D.rosen-stir-emergency-calls] but otherwise out-of-scope of this document. In addition, the PASSporT claims and values defined in this document are intended for use in environments where there are means to verify that the signer of the SIP 'Resource-Priority' and 'Priority' header fields is authoritative.

## 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. New Assertion Values for "rph" claim

This specification defines the ability to sign the SIP Resource-Priority Header field namespace for local emergency communications defined in [RFC7135] and represented by the string "esnet.x" where x is the priority-level allowed in the esnet namespace. As of the writing of this specification the priority-level is between 0 and 4, inclusive, but may be extended by future specifications.

Similar to the values defined by [RFC8443] for the "auth" JSON object key inside the "rph" claim, the string "esnet.x" with the appropriate value should be used when resource priority is required for local emergency communications corresponding and exactly matching the SIP Resource-Priority header field representing the namespace invoked in the call.

When using "esnet.x" as the "auth" assertion value in emergency service destined calls, the "orig" claim of the PASSporT MUST represent the calling party number that initiates the call to emergency services. The "dest" claim MUST either be a country or region specific dial string (e.g., "911" for North America or "112" GSM defined string used in Europe and other countries) or

"urn:service:sos" as defined in [RFC5031], representing the emergency services destination of the call.

The following is an example of an "rph" claim for SIP 'Resource-Priority' header field with an "esnet.1" assertion:

```
{
  "dest":{"uri":["urn:service:sos"]},
  "iat":1615471428,
  "orig":{"tn":"12155551212"},
  "rph":{"auth":["esnet.1"]}
}
```

For emergency services callbacks, the "orig" claim of the "rph" PASSporT MUST represent the Public Safety Answering Point (PSAP) telephone number. The "dest" claim MUST be the telephone number representing the original calling party of the emergency service call that is being called back.

The following is an example of an "rph" claim for SIP 'Resource-Priority' header field with a "esnet.0" assertion:

```
{
  "dest":{"tn":["12155551212"]},
  "iat":1615471428,
  "orig":{"tn":"12155551213"},
  "rph":{"auth":["esnet.0"]}
}
```

After the header and claims PASSporT objects have been constructed, their signature is generated normally per the guidance in [RFC8225] using the full form of PASSporT. The credentials (i.e., Certificate) used to create the signature must have authority over the namespace of the "rph" claim, and there is only one authority per claim. The authority MUST use its credentials associated with the specific service supported by the resource priority namespace in the claim. If r-values are added or dropped by the intermediaries along the path, the intermediaries must generate a new "rph" identity header and sign the claim with their own authority.

#### 4. The SIP Priority header "sph" claim

As defined in [RFC7090] the SIP Priority header field may be set to the value "psap-callback" for emergency services callback calls. Because some SIP networks may act on this value and provide priority or other special routing based on this value, it is important to protect and validate the authoritative use associated with it.

Therefore, we define a new claim key as part of the "rph" PASSporT, "sph". This is an optional claim that MUST only be used only with an "auth" claim with an "esnet.x" value indicating an authorized emergency callback call and corresponding to a SIP Priority header field with the value "psap-callback".

The value of the "sph" claim key should only be "psap-callback" which MUST match the SIP Priority header field value for authorized emergency services callbacks. If the value is anything other than "psap-callback", the PASSporT validation MUST be considered a failure case.

Note: Because the intended use of this specification is only for emergency services, there is also an explicit assumption that the signer of the "rph" PASSporT can authoritatively represent both the content of the Resource Priority Header field and Priority Header field information associated specifically with a emergency services callback case where both could exist. This document is not intended to be a general mechanism for protecting SIP Priority Header fields, this could be accomplished as part of future work with a new PASSporT extension or new claim added to either an existing PASSporT or PASSporT extension usage.

The following is an example of an "sph" claim for SIP 'Priority' header field with the value "psap-callback":

```
{
  "dest":{"tn":["12155551212"]},
  "iat":1615471428,
  "orig":{"tn":["12155551213"]},
  "rph":{"auth":["esnet.0"]},
  "sph":"psap-callback"
}
```

## 5. Order of Claim Keys

The order of the claim keys MUST follow the rules of [RFC8225] Section 9 which defines the deterministic JSON serialization used for signature generation (and validation); the claim keys MUST appear in lexicographic order. Therefore, the claim keys discussed in this document appear in the PASSporT Payload in the following order,

- o dest
- o iat
- o orig

- o rph

- o sph

## 6. Compact Form of PASSport

The use of the compact form of PASSport is not specified in this document or recommended for 'rph' PASSports.

## 7. Acknowledgements

The authors would like to thank Brian Rosen, Terry Reese, and Jon Peterson for helpful suggestions, comments, and corrections.

## 8. IANA Considerations

### 8.1. JSON Web Token claims

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

Claim Name: "sph"

Claim Description: SIP Priority header field

Change Controller: IESG

Specification Document(s): [RFCThis]

## 9. Security Considerations

The security considerations discussed in [RFC8224], [RFC8225], and [RFC8443] are applicable here.

## 10. References

### 10.1. Normative References

[RFC4412] Schulzrinne, H. and J. Polk, "Communications Resource Priority for the Session Initiation Protocol (SIP)", RFC 4412, DOI 10.17487/RFC4412, February 2006, <<https://www.rfc-editor.org/info/rfc4412>>.

[RFC5031] Schulzrinne, H., "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services", RFC 5031, DOI 10.17487/RFC5031, January 2008, <<https://www.rfc-editor.org/info/rfc5031>>.

- [RFC7090] Schulzrinne, H., Tschofenig, H., Holmberg, C., and M. Patel, "Public Safety Answering Point (PSAP) Callback", RFC 7090, DOI 10.17487/RFC7090, April 2014, <<https://www.rfc-editor.org/info/rfc7090>>.
- [RFC7135] Polk, J., "Registering a SIP Resource Priority Header Field Namespace for Local Emergency Communications", RFC 7135, DOI 10.17487/RFC7135, May 2014, <<https://www.rfc-editor.org/info/rfc7135>>.
- [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>>.
- [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>>.
- [RFC8443] Singh, R., Dolly, M., Das, S., and A. Nguyen, "Personal Assertion Token (PASSporT) Extension for Resource Priority Authorization", RFC 8443, DOI 10.17487/RFC8443, August 2018, <<https://www.rfc-editor.org/info/rfc8443>>.

## 10.2. Informative References

- [I-D.rosen-stir-emergency-calls] Rosen, B., "Non-Interactive Emergency Calls", draft-rosen-stir-emergency-calls-00 (work in progress), March 2020.
- [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>>.
- [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>>.



Authors' Addresses

Martin Dolly  
AT&T

Email: md3135@att.com

Chris Wendt  
Comcast  
Comcast Technology Center  
Philadelphia, PA 19103  
USA

Email: chris-ietf@chriswendt.net

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: 23 October 2022

J. Peterson  
Neustar  
21 April 2022

Out-of-Band STIR for Service Providers  
draft-ietf-stir-servprovider-oob-02

Abstract

The Secure Telephone Identity Revisited (STIR) framework defines means of carrying its Persona Assertion Tokens (PASSporTs) either in-band, within the headers of a SIP request, or out-of-band, through a service that stores PASSporTs for retrieval by relying parties. This specification defines a way that the out-of-band conveyance of PASSporTs can be used to support large service providers, for cases in which in-band STIR conveyance is not universally available.

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 23 October 2022.

Copyright Notice

Copyright (c) 2022 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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Terminology . . . . .	3
3. Service Provider Deployment Architecture for Out-of-Band STIR . . . . .	3
4. Advertising a CPS . . . . .	4
5. Submitting a PASSporT . . . . .	5
6. PASSporT Retrieval . . . . .	6
7. Gateways . . . . .	7
8. Acknowledgments . . . . .	7
9. IANA Considerations . . . . .	7
10. Security Considerations . . . . .	8
11. References . . . . .	8
11.1. Normative References . . . . .	8
11.2. Informative References . . . . .	9
Author's Address . . . . .	10

## 1. Introduction

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]). The STIR out-of-band [RFC8816] framework enables the delivery of PASSporT [RFC8225] objects through a Call Placement Service (CPS), rather than carrying them within a signaling protocol such as SIP. Out-of-band conveyance is valuable when end-to-end SIP delivery of calls is partly or entirely unavailable due to network border policies, calls routinely transitting a gateway to the PSTN, or similar circumstances.

While out-of-band STIR can be implemented as an open Internet service, it then requires complex security measures to enable the CPS function without allowing the CPS to collect data about the parties placing calls. This specification describes CPS implementations that act specifically on behalf of service providers who will be processing the calls that STIR secures, and who thus will learn about the parties to communication independently, so an alternative security architecture becomes possible. These functions may be crucial to the adoption of STIR in some environments, like mobile networks, where in-band transmission of STIR may not be feasible.

Environments that might support this flavor of STIR out-of-band include carriers, large enterprises, call centers, or any Internet service that aggregates on behalf of a large number of telephone endpoints. That last case may include certain classes of gateway or transit providers.

## 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. Service Provider Deployment Architecture for Out-of-Band STIR

The architecture in this specification assumes that every participating service provider is associated with one or more designated CPS instances. A service provider's CPS serves as a place where callers, or in some cases gateways, can deposit a PASSporT when attempting to place a call to a subscriber of the destination service provider; if the caller's domain supports in-band STIR, this can be done at the same time as an in-band STIR call is placed. The terminating service provider could operate the CPS themselves, or a third party could operate the CPS on the destination's behalf. This model does not assume a monolithic CPS that acts on behalf of all service providers, but nor does it prohibit multiple service providers from sharing a CPS provider. Moreover, a particular CPS can be a logically distributed entity compromised of several geographically distant entities that flood PASSporTs among themselves to support an anycast-like service.

The process of locating a destination CPS and submitting a PASSporT naturally requires Internet connectivity to the CPS. If the CPS is deployed in the terminating service provider network, any such network connectivity could instead be leveraged by a caller to initiate a SIP session, during which in-band STIR could be used

normally. The applicability of this architecture is therefore to those cases where, for whatever reason, SIP requests cannot reliably convey PASSporTs end-to-end, but an HTTP transaction can reliably be sent to the CPS from the out-of-band authentication service (OOB-AS). It is hoped that as IP connectivity between telephone providers increases, there will be less need for an out-of-band mechanism, but it can serve as a fallback mechanism in cases where service providers cannot predict whether end-to-end delivery of SIP calls will occur.

#### 4. Advertising a CPS

If more than one CPS exists for a given deployment, there will need to be some means of discovering CPSs, either administratively or programmatically. Many services providers have bilateral agreements to peer with one another, and in those environments, identifying their respective CPS's could be a simple matter of provisioning. A consortium of service providers could simply agree to choose from a list of available CPS providers, say. In more pluralist environments, some mechanism is needed to discover the CPS associated with the target of a call.

In order to allow the CPS chosen by a service provider to be discovered securely, this specification defines a CPS advertisement. Effectively, a CPS advertisement is a document which contains the URL of a CPS, as well as any information needed to determine which PASSporTs should be submitted to that CPS (e.g., Service Provider Codes (SPCs) or telephone number ranges). An advertisement may be signed with a STIR [RFC8226] credential, or another credential that is trusted by the participants in a given STIR environment. The advantage to signing with STIR certificates is that they contain a "TNAuthList" value indicating the telephone network resources that a service provider controls. This information can be matched with a TNAuthList value in the CPS advertisement to determine whether the signer has the authority to advertise a particular CPS as the proper destination for PASSporTs.

The format of a service provider CPS advertisement is a simple JSON object containing one or more pairs of TNAuthList values pointing to the URIs of CPSs, e.g. { "1234":"https://cps.example.com" }. TNAuthList values can be either Service Provider Codes (SPCs) or telephone numbers or number ranges. CPS URIs MUST be HTTPS URIs. These CPS URIs SHOULD be publicly reachable, as service providers cannot usually anticipate all of the potential callers that might want to connect with them, but in more constrained environments, they MAY be only reachable over a closed network.

CPS advertisements could be made available through existing or new databases, potentially aggregated across multiple service providers and distributed to call originators as necessary. They could be discovered during the call routing process, including through a DNS lookup. They could be shared through a distributed database among the participants in a multilateral peering arrangement.

An alternative to CPS advertisements that may be usable in some environments is adding a field to STIR [RFC8226] certificates identifying the CPS URI issued to individual service providers. As these certificates are themselves signed by a CA, and contain their own TNAUTHList, the URI would be bound securely to the proper telephone network identifiers. As STIR assumes a community of relying parties who trust these credentials, this method perhaps best mirrors the trust model required to allow a CPS to authorize PASSport submission and retrieval.

## 5. Submitting a PASSport

Submitting a PASSport to a CPS as specified in the STIR out-of-band framework [RFC8816] requires security measures which are intended to prevent the CPS from learning the identity of the caller (or callee), to the degree possible. In this service provider case, however, the CPS is operated by the service provider of the callee (or an entity operating on their behalf), and as such the information that appears in the PASSport is redundant with call signaling that the terminating party will receive anyway. Therefore, the service provider out-of-band framework does not attempt to conceal the identity of the originating or terminating party from the CPS.

An out-of-band authentication service (OOB-AS) forms a secure connection with the target CPS. This may happen at the time a call is being placed, or it may be a persistent connection, if there is a significant volume of traffic sent over this interface. The OOB-AS SHOULD authenticate itself to the CPS via mutual TLS using its STIR credential [RFC8226], the same one it would use to sign calls; this helps mitigate the risk of flooding that more open OOB implementations may face. Furthermore, use of mutual TLS prevents attackers from replaying captured PASSports to the CPS. A CPS makes its own policy decision as to whether it will accept calls from a particular OOB-AS, and at what volumes. A CPS can use this mechanism to authorize service providers who already hold STIR credentials to submit PASSports to a CPS, but alternative mechanisms would be required for any entities that do not hold a STIR credential, including gateway or transit providers who want to submit PASSports. See Section 7 below for more on their behavior.

Service provider out-of-band PASSporTs do not need to be encrypted for storage at the CPS, although use of transport-layer security to prevent eavesdropping on the connection between the CPS and OOB-ASs is REQUIRED. PASSporTs will typically be submitted to the CPS at the time they are created by an AS; if the PASSporT is also being used for in-band transit within a SIP request, the PASSporT can be submitted to the CPS before or after the SIP request is sent, at the discretion of the originating domain. An OOB-AS will use a REST interface to submit PASSporTs to the CPS as described in [RFC8816] Section 9. PASSporTs persist at the CPS for as long as is required for them to be retrieved (see the next section), but in any event for no longer than the freshness interval of the PASSporT itself (a maximum of sixty seconds).

## 6. PASSporT Retrieval

The STIR out-of-band framework [RFC8816] proposes two means that called parties can acquire PASSporTs out-of-band: through a retrieval interface, or through a subscription interface. In the service provider context, where many calls to or from the same number may pass through a CPS simultaneously, an out-of-band capable verification service (OOB-VS) may therefore operate in one of two modes: it can either pull PASSporTs from the CPS after calls arrive, or receive push notifications from the CPS for incoming calls.

Pulling of PASSporTs from the CPS will follow the basic REST flow described in [RFC8816] Section 9. In the pull model, a terminating service provider polls the CPS via its OOB-VS after having received a call for those cases in which the call signaling does not itself carry a PASSporT. Exactly how a CPS determines which PASSporTs an OOB-VS is eligible to receive over this interface is a matter of local policy. If a CPS serves only one service provider, then all PASSporTs submitted to the CPS are made available to the OOB-VS of that provider; indeed, the CPS and OOB-VS may be colocated or effectively operated as a consolidated system. In a multi-provider environment, the STIR credential of the terminating domain can be used by the CPS to determine the range of TNAAuthLists for which an OOB-VS is entitled to receive PASSporTs; this may be through a mechanism like mutual TLS, or through using the STIR credential to sign a token that is submitted to the CPS by the retrieving OOB-VS. Note that a multi-provider CPS will need to inspect the "dest" element of a PASSporT to determine which OOB-VS should receive the PASSporT.

In a push model, an OOB-VS could for example subscribe to a range of telephone numbers, which will be directed to that OOB-VS by the CPS (provided the OOB-VS is authorized to receive them by the CPS). PASSporT might be sent to the OOB-VS either before or after unsigned

call signaling has been received by the terminating domain. In either model, the terminating side may need to delay rendering a call verification indicator when alerting, in order to await the potential arrival of a PASSporT at the OOB-VS. The exact timing of this, and its interaction with the substitution attack described in [RFC8816] Section 7.4, is left for future work.

## 7. Gateways

In some deployment architectures, gateways might perform a function that interfaces with a CPS for the retrieval or storage of PASSporTs, especially in cases when in-band STIR service providers need to exchange secure calls with providers that can only be reached by STIR out-of-band. For example, a closed network of in-band STIR providers may send SIP INVITEs to a gateway in front of a traditional PSTN tandem that services a set of legacy service providers. In that environment, a gateway might extract a PASSporT from an in-band SIP INVITE and store it in a CPS that was established to handle requests for one or more legacy providers, who in turn consume those PASSporTs through an OOB-VS to assist in robocall mitigation and similar functions.

The simplest way to interface a gateway performing this sort of function for a service provider CPS system is to issue credentials to the gateway that allow it to act on behalf of the legacy service providers it supports: this would allow it to both add PASSporTs to the CPS acting on behalf of the legacy providers, and also to create PASSporTs for in-band STIR conveyance from the legacy-providers to terminating service providers in the closed STIR network. For example, a service provider could issue a delegate certificate [RFC9060] for this purpose.

## 8. Acknowledgments

We would like to thank Alex Fenichel for contributions to this specification.

## 9. IANA Considerations

This memo includes no request to IANA.



## 10. Security Considerations

The Security Considerations of [RFC8816] apply to those document as well, including concerns about potential denial-of-service vectors and traffic analysis. However, that specification's model focused a great deal on the privacy implications of uploading PASSporTs to a third-party web service. This draft mitigates those concerns by making the CPS one of the two parties to call setup (or an entity contractual acting on their behalf). That said, any architecture in which PASSporTs are shared with a federated or centralized CPS raises potential concerns about data collection [RFC7258].

Unlike [RFC8816], this document proposes the use of STIR certificates to authenticate transactions with a CPS as well as signatures for CPS advertisements. This presumes an environment where STIR certificates are issued by known trust anchors which are known to the CPS, potentially including gateways and similar services. Common STIR deployments use Service Provider Codes (SPCs) instead of telephone numbers ranges to identify service providers today; determining whether a given SPC entitles a service provider to access PASSporTs for a given telephone number is not trivial, but is a necessary component of this CPS architecture. If anyone with a STIR certificate is able to publish or access PASSporTs for any telephone number, the potential data collection implications are significant. As

## 11. References

### 11.1. 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>>.
- [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>>.
- [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>>.

#### 11.2. Informative References

- [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>>.
- [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>>.
- [RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <<https://www.rfc-editor.org/info/rfc7258>>.
- [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>>.
- [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>>.
- [RFC9060] Peterson, J., "Secure Telephone Identity Revisited (STIR) Certificate Delegation", RFC 9060, DOI 10.17487/RFC9060, September 2021, <<https://www.rfc-editor.org/info/rfc9060>>.

Author's Address

Jon Peterson  
Neustar, Inc.  
Email: [jon.peterson@team.neustar](mailto:jon.peterson@team.neustar)

Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: August 26, 2021

J. Peterson  
Neustar  
C. Wendt  
Comcast  
February 22, 2021

Messaging Use Cases and Extensions for STIR  
draft-peterson-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 instant text and multimedia messaging use cases, both for messages carried or negotiated by SIP, and for non-SIP messaging.

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 August 26, 2021.

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. Security Considerations . . . . .	7
8. References . . . . .	7
8.1. Normative References . . . . .	7
8.2. Informative References . . . . .	8
Authors' Addresses . . . . .	9

## 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, in some environments 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 reliably

way to mitigate messaging spam in the future. And as STIR sees further deployment in the telephone network, it seems likely that 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 the 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 "mkey" claim of PASSporT using the [RFC8862] framework. Similar practices would apply to sessions that negotiate text over RTP via [RFC4103] or similar mechanisms. For the most basic use cases, STIR for messaging should not require any further protocol enhancements.

[TBD: liase with GSMA on this]

However, current usage of baseline [RFC8224] Identity is largely confined to INVITE requests. RCS-style applications would require PASSporTs for all conversation participants. This would in turn require the implementation of STIR connected identity [I-D.peterson-stir-rfc4916-update].

### 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, which is used in some North American emergency services use cases. The interaction of STIR with MESSAGE is not as straightforward as the potential use case with MSRP. An Identity header could be added to any SIP MESSAGE request, but without some extension to the PASSporT claims, the PASSporT would offer no protection to the message content. As the bodies of SIP requests are MIME encoded, S/MIME [RFC8591] has been proposed as a means of providing integrating for MESSAGE (and some MSRP cases as well). The interaction of [RFC8226] STIR certificates with S/MIME for messaging applications would require some further explication; and potentially, PASSporT could provide its own integrity check for message contents.

Moreover, 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. This specification proposes that the STIR credentials assigned to service providers could be leveraged to sign for PASSporTs for messages that originate from telephone numbers. In order to apply PASSporT to textual or multimedia

messaging, a new claim is here 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. This helps to prevent the replay of a PASSporT for a message to putatively secure a call, or vice versa.

This specification defines a new optional JWT [RFC7519] claim "msgi" which provides a digest over the contents of a message, which may be a text message, or a more complex 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.

[TBD: Do we need algorithmic agility here?]

In order to generate the message digest, the following steps are taken:

[TBD: Canonicalization procedures. Maybe we need separate procedures for plain text (like, SMPP), rich text, and then more complex multimedia messages? Definitely a danger of scope creep. For the emergency services case, we want OASIS CAP, right? Maybe focus on that. Anything we could easily steal here?]

At the end result of the process, 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.

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 [I-D.ietf-stir-oob] 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.

[TBD: I mean, if you can deliver a PASSporT OOB, you can deliver a message OTT - there may be limits to how useful a mechanism like this would be. In any event, the precise way to do OOB for messaging would need to be sketched out here.]

#### 4. Certificates and Messaging

The [RFC8226] STIR certificate profiles defines a way to issue certificates that sign PASSporTs, which attest through their TNAuthList either a Service Provider Code (SPC), or a set of one or more telephone numbers. This specification proposes that the semantics of this certificates should suffice for signing for messages from a telephone number without further modification.

[TBD: Or should there be? Should for example certificates have to have some special authority to sign for messages instead of calls?]

#### 5. Acknowledgments

We would like to thank 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. Security Considerations

TBD.

## 8. References

### 8.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <<https://www.rfc-editor.org/info/rfc3261>>.
- [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>>.

## 8.2. Informative References

- [I-D.ietf-stir-oob] Rescorla, E. and J. Peterson, "STIR Out-of-Band Architecture and Use Cases", draft-ietf-stir-oob-07 (work in progress), March 2020.
- [I-D.ietf-stir-passport-divert] Peterson, J., "PASSport Extension for Diverted Calls", draft-ietf-stir-passport-divert-09 (work in progress), July 2020.
- [I-D.peterson-stir-rfc4916-update] Peterson, J. and C. Wendt, "Connected Identity for STIR", draft-peterson-stir-rfc4916-update-02 (work in progress), November 2020.
- [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>>.
- [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>>.
- [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>>.
- [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>>.
- [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>>.

#### Authors' Addresses

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

Email: [jon.peterson@team.neustar](mailto:jon.peterson@team.neustar)

Chris Wendt  
Comcast  
One Comcast Center  
Philadelphia, PA 19103  
USA

Email: [chris-ietf@chriswendt.net](mailto:chris-ietf@chriswendt.net)

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 1xx 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 1xx 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 1xx 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](mailto:jon.peterson@team.neustar)

Chris Wendt  
Comcast  
One Comcast Center  
Philadelphia, PA 19103  
USA

Email: [chris-ietf@chriswendt.net](mailto: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= \
"eyJhbGciOiJFbGVzIiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IiIjOiJ9.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 \
kZXN0Ijpw7InVyaSI6WyJzaXA6YWxpY2VAZXhhbXBsZS5jb20iXX0sImhhdC \
I6IjE0NDMyMDgzNDUiLCJvcmlnIjpw7InRuIjoimTIxNTU1NTEyMTIifX0.r \
q3pjTlhoRwakEGjHCnWSwUnshd0-zJ6F1VOgFWSjHBr8Qjplk-cpFYpFYs \
ojNCpTzO3QfP0lckGaS6hEck7w"
```

```
Reason: STIR ;cause=436 ; text="Bad Identity Info" ;ppt= \
"eyJhbGciOiJFUzI1NiIsInR5cCI6InBhc3Nwb3J0IiwieDV1Ii \
joiaHR0cHM6Ly9jZXXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LmNlciJ9.eyJ \
xpY2VAZXhhbXBsZS5jb20iXX0sImhhdCkZXN0Ijpw7InVyaSI6WyJzaXA6YW \
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](mailto:chris-ietf@chriswendt.net)