Workgroup: Network Working Group
Internet-Draft:
draft-ietf-stir-passport-rcd-26
Published: 5 June 2023
Intended Status: Standards Track
Expires: 7 December 2023
Authors: C. Wendt
Somos Inc.
J. Peterson
Neustar Inc.

PASSporT Extension for Rich Call Data

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 and is also enhanced with a integrity mechanism that is designed to protect the authoring and transport of this information for different authoritative use-cases.

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 7 December 2023.

Table of Contents

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. This document extends the use of JWT and PASSporT in the overall STIR framework by defining a PASSporT extension and the associated STIR procedures to protect additional caller and call related information. This is additional information beyond the calling party originating identity (e.g. telephone number or SIP URI) that is intended to be rendered to assist a called party in determining whether to accept or trust incoming communications. This includes information such as the name of the person or entity on one side of a communications session, for example, 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 to a call and whom is calling.

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 determine a name from the calling party number by consulting a local address book or an external database. SIP, for example, 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. In this document, we utilize the STIR framework to more generally extend the assertion of an extensible set of identity information not limited to but including calling name.

This document extends PASSporT to provide cryptographic protection for the "display-name" field of SIP requests, or similar name fields in other protocols, 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. In addition, Section 12 describes use-cases that enable external third-party authorities to convey rich information associated with a calling number via a "rcd" PASSporT while clearly identifying the third-party as the source of the Rich Call Data information. 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

This document defines Rich Call Data (RCD) which is a PASSporT extension [RFC8225] that defines an extensible claim for asserting information about the call beyond the telephone number. This includes information such as more detailed information about the calling party or calling number being presented or the purpose of the call. There are many use-cases that will be described in this document around the entities responsible for the signing and integrity of this information, whether it is the entity that originates a call, a service provider acting on behalf of a caller or use-cases where third-party services may be authoritative over the rich call data on behalf of the caller. In general, PASSporT [RFC8225] has been defined to be a communications protocol independent technology, but it's initial usage as detailed in [RFC8224] is with the SIP protocol [RFC3261]. There are many SIP specific references and definitions in this document, but future specifications may extend the usage of RCD PASSporTs and claims to other protocol specific usage and definitions.

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-Identity [RFC3325], or an icon associated with the caller. 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 a string 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 are policy and restrictions around what data elements are 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 enforces the policies 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 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 [W3C-SubresourceIntegrity]. 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 compute the signature in 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 in the PASSporT claims is pass-by-value or pass-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 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 or "rcd" claims 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 URI refs	Includes URI refs
Auth	1: No integrity req	2: RCD 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 URIs referencing external content 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 modes 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, in particular when delegating signing authority for PASSporT, to enable a mechanism for allowing agreed 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 referenced external content using URIs.

5. PASSporT Claim "rcd" Definition and Usage

5.1. PASSporT "rcd" Claim

This document 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 match the display-name component of the From header field value of a SIP request [RFC3261] or alternatively from the P-Asserted-Identity header field value [RFC3325], or a similar field in other PASSporT using protocols. This key MUST be included once as part of the "rcd" claim value JSON object. The key syntax of "nam" MUST follow the display-name ABNF given in [RFC3261]. 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 match 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 or "rcd" claims 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 or "rcd" claims. 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 HTTPS URL reference to an image resource 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://wwww.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 HTTPS URL 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. The jCard is defined in this specification as an extensible object format used to contain RCD information about the call initiator. This object is intended to directly match the Call-Info header field value defined in [I-D.ietf-sipcore-callinfo-rcd] with a type of "jcard" where the format of the jCard and properties used should follow the normative usage and formatting rules and procedures in that document. 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. Either a "jcd" or "jcl" MAY appear in the "rcd" claim, but not both.

The jCard object value for "jcd" MUST be a jCard JSON object that MAY have URI referenced content, but that URI referenced content MUST 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 "rcd" claims, using Call-Info as protocol with the addition of an identity header carrying the PASSPorT is not required. The identity header carrying a PASSporT with "rcd" claim including a "jcd" value can be used as the primary and only transport of the RCD information.

5.1.5. "jcl" key

The "jcl" key value is an HTTPS URL that refers to a jCard [RFC7095] JSON object on a web server. The web server MUST use the MIME media type for JSON text as application/json with a default encoding of UTF-8 [RFC8259]. This link may correspond to 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. The "jcd" or "jcl" keys MAY only appear once in the "rcd" claim but MUST be mutually exclusive.

The jCard object referenced by the URI value for "jcl" MUST be a jCard JSON object that MAY have URI referenced content, but that URI referenced content MUST 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. "rcdi" and "rcd" claims MAY each appear once in a PASSporT, but if "rcdi" is included the "rcd" MUST correspondingly be present also. 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 URI referenced external 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 URI references to external content that include JSON objects themselves, for the specific case of the use of "jcl", defined in Section 6.1.4. JSON pointer syntax is the key value that documents 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-jL4f47fF82LuwcrOrSyckA4SWrlElfARHkW6kYo1JdI"
}
```

The values of each key/value pair consists of a digest across one of the following objects referenced by the JSON pointer key,

- *content inline to the referenced object
- *the content of a resource referenced by an inline URI object
- *the content of a resource specified by a URI that is in embedded in content specified by an inline URI object(e.g., jcl)

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

Note that the digest is computed on the Json representation of the string, which necessarily includes the beginning and ending double-quote characters.

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.

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 MUST be a JSON pointer and digest entry for the content in that linked resource. When creating a key/value representing "icn", the key is the JSON pointer string "/icn" and the digest value string would be created using the image file byte data referenced in the URI.

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 indices 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 indices are used to reference the URI strings.

```
"rcdi": {
  "/jcd": "sha256-7kdCBZqH0nqMSPsmABvsKlHPhZEStgjojhdSJGRr3rk",
  "/jcd/1/3/3": "sha256-RojgWwU6xUtI4q82+kHPyHm1JKbm7+663bMvzymhkl4",
  "/jcd/1/4/3": "sha256-jL4f47fF82LuwcrOrSyckA4SWrlElfARHkW6kYo1JdI",
  "/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, the use of the "rcdi" JSON pointer and integrity digest as the constraint value in JWTClaimConstraints over the jCard data is RECOMMENDED.

It is important to remember the array indices 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 indices added to the "jcl" (e.g., "/jcl/1/2/3") are treated as if the external content referenced by the 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": "sha256-7kdCBZqH0nqMSPsmABvsKlHPhZEStgjojhdSJGRr3rk",
  "/jcl/1/3/3": "sha256-RojgWwU6xUtI4q82+kHPyHm1JKbm7+663bMvzymhkl4",
  "/jcl/1/4/3": "sha256-jL4f47fF82LuwcrOrSyckA4SWrlElfARHkW6kYo1JdI",
  "/jcl/1/5/3": "sha256-GKNxxqlLRarbyBNh7hc/4lbZAdK6B0kMRf1AMRWPkSo"
}
```

The "rcdi" MUST have a "/jcl" key value and digest value to protect the referenced jCard object and each URI referenced in the referenced jCard array string MUST have a corresponding JSON pointer string key and digest value.

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

When using JWT Claim Constraints for "rcd" claims the procedure when creating the signing certificate should follow the following guidelines.

The "permittedValues" for the "rcd" claim MAY contain a single entry or optionally MAY contain multiple entries with the intent of supporting cases where the certificate holder is authorized to use different sets of rich call data corresponding to different call scenarios.

Only including "permittedValues" for "rcd", with no "mustInclude", provides the ability for the construction a valid PASSPorT that can either have no "rcd" claim within or only the set of constrained "permittedValues" values for an included "rcd" claim.

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

The use of JWT Claim Constraints with an "rcdi" claim is for cases where URI referenced content is to be protected by the authoritative certificate issuer. The objective for the use of JWT Claim Constraints for the combination of both "rcd" and "rcdi" claims is to constrain the signer to only construct the "rcd" and "rcdi" claims inside a PASSporT to contain and reference only a pre-determined set of content. Once both the contents of the "rcd" claim and any referenced content is certified by the party that is authoritative for the certificate being issued to the signer, the "rcdi" claim is constructed and linked to the STIR certificate associated with the signature in the PASSporT via JWT Claim Constraints extension as defined in [RFC8226] Section 8 and extended in [RFC9118]. 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 cases that there should always be both "rcd" and "rcdi" claims included in the 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.

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

This document defines a new JSON Web Token claim for "crn", Call Reason, the value of which is a single string 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"}
```

7.1. JWT Constraint for "crn" claim

The integrity of the "crn" claim contents can optionally be protected by the authoritative certificate issuer using JWT Constraints in the certificate. When the signer of the PASSporT intends to always include a call reason string of any value, a "mustInclude" for the "crn" claim in the JWT Claim Constraints

indicates that a "crn" claim must always be present and is RECOMMENDED to be included by the certificate issuer. If the signer of the "crn" claim wants to constrain the contents of "crn", then "permittedValues" for "crn" in JWT Claim Constraints should match the contents of the allowed strings and is RECOMMENDED to be included by the certificate issuer.

8. Rich Call Data Claims Usage Rules

The "rcd" or "crn" claims MAY appear in any PASSporT claims object as optional elements. The creator of a PASSporT MAY also add a PASSporT extension ("ppt") value, defined in [RFC8225] Section 8.1, of "rcd" to the header of a PASSporT as well, in which case the PASSporT claims MUST contain at least one or both an "rcd" or "crn" claim. Any entities verifying the PASSporT claims defined in this document are required to understand the PASSporT extension in order to process the PASSporT in question. An example PASSporT header with the PASSporT extension ("ppt") value of "rcd" 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" key and value, is mandatory.

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

8.1. "rcd" PASSporT Verification

A verifier that successfully verifies a PASSportT that contains an "rcd" claim MUST ensure the following about the PASSporT:

- *it has a valid signature per the verification procedures detailed in [RFC8225]
- *it abides by all rules set forth in the proper construction of the claims defined in Section 5 of this document
- *it abides by JWT Claims Constraint rules defined in [RFC8226] Section 8 or extended in [RFC9118] if present in the certificate used to compute the signature in the PASSporT

In addition if the "iss" claim is included in the PASSPorT, verification should follow procedures described in Section 10.2.

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.

8.2. "rcdi" Integrity Verification

When the "rcdi" claim exists, the verifier should verify the digest for each JSON pointer key. Any digest string that doesn't match a generated digest MUST be considered a failure of the verification of the content referenced by the JSON pointer.

If there is any issue with completing the integrity verification procedures for referenced external 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.

As a potential optimization of verification procedure, an entity that does not otherwise need to dereference a URI from the "rcd" claim for display to end-user is NOT RECOMMENDED to unnecessarily dereference the URI solely to perform integrity verification.

8.3. 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", "apn", and "icn" using an https URI PASSporT claims object is shown next (with line breaks for readability only). Note, in this example, there is no integrity protection over the "icn" element in the "rcd" claim.

```
{  "orig":{"tn":"12025551000"},
   "dest":{"tn":["12155551001"]},
   "iat":1443208345,
   "rcd":{
     "apn":"12025559990",
     "icn":"https://example.com/photos/quartermaster-256x256.png",
     "nam":"Her Majesty's Secret Service" } }
```

An example of a "nam", "apn", and "icn" using data URI PASSporT claims object is shown next (with line breaks for readability only). Note, in this example, the "icn" data is incorporated directly in

the "rcd" claim and therefore separate integrity protection is not required.

```
{  "orig":{"tn":"12025551000"},
   "dest":{"tn":["12155551001"]},
   "iat":1443208345,
   "rcd":{
     "apn":"12025559990",
     "icn":"
       AAACNbyblAAAAHElEQVQI12P4//8/w38GIAXDIBKE0DHxgljNBAAO9TXL0Y4OH
       wAAAABJRU5ErkJggg==",
     "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. Note, in this example, the "rcdi" claim includes integrity protection of the URI referenced content.

```
{
  "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-qCn4pEH6BJu7zXndLFuAP6DwlTv5fRmJ1AFkqftwnCs",
   "/jcl/1/3/3":"sha256-RojgWwU6xUtI4q82+kHPyHm1JKbm7+663bMvzymhkl4",
   "/jcl/1/4/3":"sha256-jL4f47fF82LuwcrOrSyckA4SWrlElfARHkW6kYo1JdI",
   "/jcl/1/5/3":"sha256-GKNxxqlLRarbyBNh7hc/4lbZAdK6B0kMRf1AMRWPkSo"
  }
}
```

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+LHOKHtU4SxG8shlOo6OS4ot8IJQImY",
    "/icn": "sha256-RojgWwU6xUtI4q82+kHPyHm1JKbm7+663bMvzymhkl4"
  }
}
```

9. Compact form of "rcd" PASSporT

9.1. Compact form of the "rcd" PASSporT claim

The specific usage of compact form of an "rcd" PASSporT claim, defined in [RFC8225] Section 7, has some restrictions that will be enumerated below, but mainly follows standard PASSporT compact form procedures. Compact form only provides the signature from the PASSporT, requiring the re-construction of the other PASSporT claims from the SIP header fields as discussed in [RFC8224] Section 4.1.

The re-construction of the "nam" claim, if using SIP protocol, should use the display-name string in the From header field. For other protocols, if there is a display name field that exists, the string should be used, otherwise the string should be an empty string, e.g., "". "jcl" and "jcd" MUST NOT be used with compact form due to integrity rules and URI reference rules in this document 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 and to provide specific guidance for other protocol usage.

9.2. Compact form of the "rcdi" PASSporT claim

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

9.3. 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].

10. 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 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 using SIP protocol for this example: 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 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 PASSporT object matches, or is string equivelent to, 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.

10.1. 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 document; 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"} }
```

10.2. Verification using Third Party RCD

The third-party "rcd" PASSporT cases must be considered in the verification service, 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. Following the rules of [RFC8225] and in particular if there is multiple identity headers, for example with the case of the inclusion of an "rcd" and "shaken" PASSporTs from two different signing providers, 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. It is possible that if there is multiple identity headers

are present, only the verified identity information should be considered when presenting call information to an end user.

Verification services may alter their authorization policies for the credentials accepted to sign PASSporTs when third parties generate PASSporT objects, per Section 10.1. 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.

11. Levels of Assurance

As "rcd" can be provided by either first party providers that are directly authorized to sign PASSporTs in the STIR eco-system or third party providers that are indirectly or delegated authority to sign PASSporTs. Relying parties could benefit from an additional claim that indicates the identification, in the form of a uniquely identifiable name, of the attesting party to the caller. Even in first party cases, 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 be determined 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 are RECOMMENDED to also carry an indication of the identity of the generator of the PASSporT in the form of the 'iss' claim.

12. Use of "rcd" PASSporTs in SIP

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

12.1. Authentication Service Behavior for SIP protocol

An authentication service creating a PASSporT containing an "rcd" claim MAY include a PASSporT extension ("ppt" value) of "rcd" or not. Third-party authentication services following the behavior in Section 10.1 MUST include a PASSporT extension value of "rcd". If PASSporT extension does contain an "rcd", then any SIP authentication services MUST add a PASSporT extension "ppt"

parameter to the Identity header field containing that PASSporT with a value of "rcd". The resulting Identity header field might look as follows:

```
Identity: sv5CTo05KqpSmtHt3dcEiO/1CWTSZtnG3iV+1nmurLXV/HmtyNS7Ltrg9
      dlxkWzoeU7d7OV8HweTTDobV3itTmgPwCFjaEmMyEI3d7SyN21yNDo2ER/Ovgt
      w0Lu5csIppPqOg1uXndzHbG7mR6Rl9BnUhHufVRbp51Mn3w0gfUs=;
      info=<https://biloxi.example.org/biloxi.cer>;alg=ES256;
      ppt="rcd"
```

This document assumes that by default when using the SIP protocol, an authentication service determines 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 match or be determined by 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 string equivalent to the From header field display-name value, it MUST use the full form of the PASSporT object in SIP.

In addition, {I-D.ietf-sipcore-callinfo-rcd}} defines a Call-Info header field that MAY be used as a source of RCD information that an authentication services uses to construct the appropriate PASSporT RCD claim types used.

Note also that, as a best practice, the accuracy and legitimacy of Rich Call Data information that is included in the claims is RECOMMENDED to follow a trust framework that is out of scope of this document. As with telephone numbers for the STIR framework the authentication of Rich Call Data should follow some type of vetting process by an entity that is authoritative over determining the accuracy and legitimacy of that information. This includes the mechanisms for how and from whom that information is received by the authentication service. For example, the general use of Call-Info via SIP as a trusted source of RCD information on the authentication side is NOT RECOMMENDED.

12.2. Verification Service Behavior for SIP protocol

[RFC8224] Section 6.2 Step 5 requires that future specifications defining PASSporT extension ("ppt") values describe any additional verifier behavior specific to the SIP protocol. The general verification proceedures defined in Section 8.1 should be followed, but the following paragraphs describe some of the specifics needed to implement a verification service using the SIP protocol.

If the PASSporT is in compact form, then the verification service MUST extract the display-name from the From header field value, if any, and MUST use that as the string 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" JSON object value MUST be used to construct the "jcd" key value when it recomputes the header and claims of the PASSporT object. If the signature validates over the recomputed object, then the verification is considered successful.

If the PASSporT is in full form with a PASSporT extension value of "rcd", then the verification service MUST extract the value associated with the "rcd" claim "nam" key in the object. If the PASSporT signature is verified successfully then the verification service MUST additionally compare the string value of the "rcd" claim "nam" key value with the From header field value or the preferred value. The preferred value depends on local policy of the SIP network technique that conveys the display name string through a field other than the From header field to interoperate with this specification (e.g. P-Asserted-Identity) as discussed in [RFC8224]. Similarly, "jcd" or "jcl" jcard information, "icn", "apn", or "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]. If future defined PASSporT RCD claims types are present, they should follow similar defined proceedures and policies.

The behavior of a SIP UAS upon receiving an INVITE or other type of session initiation request 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.

13. Using "rcd", "rcdi", "crn" 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 corresponding to multiple PASSporT extensions, the authentication service can alternatively directly

add the "rcd" claim to a PASSporT that authenticates the calling identity.

13.1. Procedures for applying RCD claims as claims only

For a given PASSporT using some other extension than "rcd", the Authentication Service MAY additionally include the "rcd" defined in {#rcd_define}, "rcdi" defined in {#rcdi_define}, and "crn" defined in {#crn_define} claims. 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.

13.2. Example for applying RCD claims 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 understands and supports claims defined in the "rcd" and "shaken" PASSporT extensions is able to receive the

above PASSporT and interpret both the "shaken" claims as well as the "rcd" defined claims.

If the Verification Service only understands the "shaken" PASSporT extension claims and doesn't support "rcd" PASSporT extension or claims, then the "rcd" claim, in this example, is used during PASSporT signature validation but is otherwise ignored and disregarded.

14. 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 16.3. 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.

15. 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.

16. IANA Considerations

16.1. JSON Web Token Claim

This document 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]

16.2. Personal Assertion Token (PASSporT) Extensions

This document requests that the IANA add a new entry to the Personal Assertion Token (PASSporT) Extensions registry for the type "rcd" which is specified in [RFCThis].

16.3. PASSporT RCD Claim Types

This document requests that the IANA create a new registry for PASSporT RCD claim types. This new registry should be added to the "Personal Assertion Token (PASSporT)" group. Registration of new

PASSporT RCD claim types shall be under the Specification Required policy.

This registry is to be initially populated with five claim name values, "nam", "apn", "icn", "jcd", and "jcl", which are specified in [RFCThis]. This is a two column registry with column1 = "Name" and column2 = "Reference Document". Any new registrations should consist of only of the name and the reference document. There is an obligation for expert review, where the designated expert should validate that the proposed new PASSporT RCD claim type has a scope that doesn't potentially conflict or overlap with the usage or interpretation of the other existing types in the registry.

17. Security Considerations

The process of signing information contained in a "rcd" PASSporT, whether the identities, identifiers, alternate identities or identifiers, images, logos, physical addresses, or otherwise should follow some vetting process in which an authoritative entity should follow an appropriate consistent policy defined and governed by the eco-system using RCD and the STIR framework. This can be of many forms, depending on the setup and constraints of the policy requirements of the eco-system and 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 in many current base communications protocols, for example SIP, is information that carried 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 dereferencing and download of any RCD URI linked resources as part of verification either in-network or on device could provide some level of information about calling patterns, so this should be considered when making these resources available.

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 is RECOMMENDED for the prevention of 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.

As general guidance, the use of URLs and URIs that reference potentially dangerous or intentionally harmful content should be considered in implimenting this specification. [RFC3986] Section 7 contains good additional guidance to consider when communicating or dereferencing URLs and URIs.

17.1. 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.

18. References

18.1. 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-06, 3 June 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-sipcore-callinfo-rcd-06>.

[IANA-COSE-ALG] "COSE Algorithms <https://www.iana.org/assignments/cose/cose.xhtml>", n.d..

[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>.

[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>.

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

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

[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>.

[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>.

[RFC8259] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", STD 90, RFC 8259, DOI 10.17487/RFC8259, December 2017, <https://www.rfc-editor.org/info/rfc8259>.

[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>.

18.2. 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>", November 2021.

[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>.

[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>.

[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>.

[W3C-SubresourceIntegrity]
W3C, "Subresource Integrity <https://www.w3.org/TR/SRI/>", 23 June 2016.

Authors' Addresses

Chris Wendt
Somos Inc.

Email: chris-ietf@chriswendt.net

Jon Peterson
Neustar Inc.

Email: jon.peterson@neustar.biz