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

C. Wendt
Comcast
J. Peterson
Neustar Inc.

February 22, 2021

PASSporT Extension for Rich Call Data
draft-ietf-stir-passport-rcd-10

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 users. This framework is intended to 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 pick up the phone. 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.

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, 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 an end user to assist a called party in determining whether to accept or trust incoming communications. This includes the name of the person 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 will be extending 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

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in [RFC2119] and [RFC6919].

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 [RFC8224] and 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 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. The second category is a set of RCD that is defined as part of the jCard definitions or extensions to that data. [I-D.ietf-sipcore-callinfo-rcd] describes the optional use of jCard in Call-Info header field as RCD with the "jcard" Call-Info purpose token. Either or both of these two types of data can be incorporated into a "rcd" claim defined in this document.

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

Both of these mechanisms, integrity digests and JWT Claims Constraints, can be used together or separately depending on the intended purpose. The first category of purpose is whether the rich call data conveyed by the RCD passport is pass-by-value or passed-by-reference; i.e., is the information contained in the passport claims and therefor 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, for example, "photo" or "logo" properties that aren't directly encoded into the JSON of the jCard) and when the signer is authoritative over the content. In this mode, integrity protection is not required and the set of claims is simply protected by the signature of the standard PASSporT [RFC8225] and SIP identity header [RFC8224] procedures. The second mode is an extension of the first where the signer is authoritative and a "rcd" claim contents include a URI identifying external resources. In this mode, an RCD Integrity or "rcdi" claim MUST be included. This integrity claim is defined later in this document and provides a digest of the "rcd" claim content so that, particularly for the case where there are URI references in the RCD, the content of that RCD can be comprehensively validated that it was received as intended by the signer of the PASSporT.

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

5. PASSporT Claims

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 and MUST be included as part of the "rcd" claim value JSON object. If there is no string associated with a display name, the claim value SHOULD then be an empty string.

5.1.2. "jcd" key

The "jcd" key value is defined to contain a value of 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" is optional. If included, this key MUST only be included once in the "rcd" JSON object and SHOULD NOT be included if there is a "jcl" key included. The "jcd" and "jcl" keys should be mutually exclusive.

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

5.1.3. "jcl" key

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

5.2. "rcdi" RCD Integrity Claim

The "rcdi" claim is claim that MUST be included for the second and fourth modes described in integrity overview section of this document. If this claim is present it MUST be only included once with a corresponding single "rcd" claim. The value of the "rcdi" key pair 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 will 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 will reference 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, in particular for the specific case of the use of "jcl". JSON pointer syntax is the key value that specifies exactly the part of JSON that should be used to generate the digest which will be the resulting string that makes up the value for the corresponding key. Detailed procedures are provided below, but an example "rcdi" is provided here:

```
"rcdi" : {
  "/jcd": "sha256-H8BRh8j48O9oAZzq6A9RINQZngK7T62em8MUt1FLm52",
  "/jcd/1/2/3": "sha256-AZzq6A9RINQZngK7T62em8MUt1FLm52H8BRh8j48O9o"
}
```

The values of each key pair are a digest combined with a string that defines the crypto algorithm used to generate the digest. For RCD, implementations MUST support the following hash algorithms, "SHA256", "SHA384", or "SHA512". The SHA-256, SHA-384, and SHA-512 are part of the SHA-2 set of cryptographic hash functions defined by the 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 MUST be represented in the text by "sha256", "sha384", or "sha512". The character following the algorithm string MUST be a minus character, "-". The subsequent characters MUST be the base64 encoded digest of a canonicalized and concatenated string 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.

5.2.1. Creation of the "rcd" element digests

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

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

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

As example, for the following "rcd" claim:

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

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

```
"rcdi": {
  "/jcd": "sha256-30SFLGHL40498527",
  "/jcd/1/3/3": "sha256-12938918VNJDSNCJ",
  "/jcd/1/4/3": "sha256-VNJDSNCJ12938918",
  "/jcd/1/5/3": "sha256-4049852730SFLGHL"
  }
}
```

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

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

```
"rcd": {
  "nam": "Q Branch Spy Gadgets",
  "jcl": "https://example.com/qbranch.json"
},
"rcdi": {
  "/jcl": "sha256-30SFLGHL40498527",
  "/jcl/1/3/3": "sha256-12938918VNJDSNCJ",
  "/jcl/1/4/3": "sha256-VNJDSNCJ12938918",
  "/jcl/1/5/3": "sha256-4049852730SFLGHL"
}
```

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

In order to facilitate proper verification of the digest 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, it should verify 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 will either refer to an element that is a part or whole of a JSON object string or to a string that is a URI referencing an external resource.

2. For a JSON formatted string, serialize the element JSON to remove all white space and line breaks. The procedures of this deterministic JSON serialization are defined in [RFC8225], Section 9. The resulting string is used to create the digest.

3. For any URI referenced content, the content can either be a string as in jCard JSON objects or binary content. For example, image and audio files contain binary content. If the content is binary format it should be Base64 encoded to create a string, otherwise the direct string content of the file is used to create the digest.

5.2.2. JWT Claim Constraint for "rcd" claims only

For the third mode described in the integrity overview section of this document, where only JWT Claim Constraint for "rcd" claims, without an "rcdi" claim, is required, the procedure should be, when creating the certificate to include a constraint on inclusion of the "rcd" claim as well as the contents of that claim.

The certificate JWT Claims Constraint MUST include the following:

- a "mustInclude" for the "rcd" claim and a "permittedValues" equal to the created "rcd" claim value string.

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

5.2.3. JWT Claim Constraint for "rcd" and "rcdi" claims

For the fourth mode described in the integrity overview section of this document, if the signing of an "rcdi" claim is required to be protected by the authoritative certificate creator using JWT Constraints in the certificate, the procedure which is intended to constrain the signer to construct the "rcd" and "rcdi" claims and reference external content via URI in a pre-determined way. Once both the contents of the "rcd" claim and any linked content is certified and the construction of the "rcdi" claim is complete, the "rcdi" claim is linked to the STIR certificate associated with the signature in the PASSporT via JWT Claim Constraints as defined in [RFC8226] Section 8. It should be recognized that the "rcdi" set of digests is intended to be unique for only a specific combination of "rcd" content and URI referenced external content.

The certificate JWT Claims Constraint MUST include both of the following:

- a "mustInclude" for the "rcd" claim, which simply constrains the fact that an "rcd" should be included if there is a "rcdi"

- a "mustInclude" for the "rcdi" claim and a "permittedValues" equal to the created "rcdi" claim value string.

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

5.3. PASSporT "crn" claim - Call Reason

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 contains information as defined in [I-D.ietf-sipcore-callinfo-rcd] corresponding to the "reason" parameter for the Call-Info header. This claim is optional.

Example "crn" claim with "rcd":

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

5.3.1. 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 this protection is used, a "mustInclude" for the "rcdi" claim and a "permittedValues" equal to the "crn" claim value string SHOULD be included.

6. "rcd" and "crn" Claims Usage

Either the "rcd" or "crn" claim may appear in any PASSporT claims object as an optional element. The creator of a PASSporT MAY also add a "ppt" value of "rcd" to the header of a PASSporT as well, in which case the PASSporT claims MUST contain either a "rcd" or "crn" claim, and any entities verifying the PASSporT object will be required to understand the "ppt" extension in order to process the PASSporT in question. A PASSporT header with the "ppt" included will look as follows:

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

The PASSporT claims object will then contain 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].

6.1. 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" only PASSporT claims object with an "rcdi" claim is shown next (with line breaks for readability only).

```
{  "orig":{"tn":"12025551000"},
   "dest":{"tn":["12025551001"]},
   "iat":1443208345,
   "rcd":{"nam":"James Bond"},
   "rcdi":{"/nam": "sha256-918VNJD12938SNCJ"}
}
```

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

```
{
  "orig": { "tn": "12025551000"},
  "dest": { "tn": ["12155551001"]},
  "iat": 1443208345,
  "rcd": {
    "nam": "Q Branch Spy Gadgets",
    "jcd": ["vcard",
    [ ["version",{},"text","4.0"],
      ["fn",{},"text","Q Branch"],
      ["org",{},"text","MI6;Q Branch Spy Gadgets"],
      ["photo",{},"uri","https://example.com/photos/q-256x256.png"],
      ["logo",{},"uri","https://example.com/logos/mi6-256x256.jpg"],
      ["logo",{},"uri","https://example.com/logos/mi6-64x64.jpg"]
    ] ]
  },
  "crn": "Rendezvous for Little Nellie",
  "rcdi": {
    "/nam": "sha256-918VNJD12938SNCJ",
    "/jcd": "sha256-VNJDSNCJ12938918",
    "/jcd/1/3/3": "sha256-12938918VNJDSNCJ",
    "/jcd/1/4/3": "sha256-VNJDSNCJ12938918",
    "/jcd/1/5/3": "sha256-4049852730SFLGHL"
  }
}
```

In an example PASSporT where a jCard is linked via HTTPS URL and "jcl" a jCard file served at a particular URL will be created.

An example jCard JSON file is shown as follows:

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

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

```
{
  "orig": {"tn": "12025551000"},
  "dest": {"tn": ["12155551001"]},
  "iat": 1443208345,
  "rcd": {
    "nam": "Q Branch Spy Gadgets",
    "jcl": "https://example.com/qbranch.json"
  },
  "crn": "Rendezvous for Little Nellie",
  "rcdi": {
    "/nam": "sha256-918VNJD12938SNCJ",
    "/jcl": "sha256-VNJDSNCJ12938918",
    "/jcl/1/3/3": "sha256-12938918VNJDSNCJ",
    "/jcl/1/4/3": "sha256-VNJDSNCJ12938918",
    "/jcl/1/5/3": "sha256-4049852730SFLGHL"
  }
}
```

7. Compact form of "rcd" PASSporT

7.1. Compact form of the "rcd" PASSporT claim

Compact form of an "rcd" PASSporT claim has some restrictions but mainly follows standard PASSporT compact form procedures. For re-construction of the "nam" claim the string for the display-name in the From header field. For re-construction of the "jcl", the Call-Info header as with purpose "jcard" defined in

[I-D.ietf-sipcore-callinfo-rcd] MUST be used. "jcd" claim MAY NOT be used as part of compact form.

7.2. Compact form of the "rcdi" PASSporT claim

Compact form of an "rcdi" PASSPorT claim is not supported, so if "rcdi" is required compact form should not be used.

7.3. 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].

8. 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 that will be 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 14.3. Specific extensions to the "rcd" PASSporT claim are left for future specification.

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. It is more likely that when those elements are present, they will be in a third-party "rcd" PASSporT.

9. Third-Party Uses

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

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

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

display name in the INVITE, then the name would presumably be rendered to the end user by the terminating user agent.

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

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

9.1. 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 will necessarily be 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 Name field of the certificate used to sign a third-party PASSporT. 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":"Example, Inc.",
   "rcd":{"nam":"James Bond"} }
```

10. 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, PASSporTs that carry "rcd" data SHOULD also carry an indication of the relationship of the generator of the PASSporT to the caller. As stated in the previous section, the use of "iss" MUST reflect the Subject Name of the certificate used to sign a third-party PASSporT to represent that relationship.

11. 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.

11.1. Authentication Service Behavior

An authentication service creating a PASSporT containing a "rcd" claim MAY include a "ppt" for "rcd" or not. Third-party authentication services following the behavior in Section 9.1 MUST include a "ppt" of "rcd". If "ppt" does contain a "rcd", then any SIP authentication services MUST add a "ppt" parameter to the Identity header containing that PASSporT with a value of "rcd". The resulting Identity header might look as follows:

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

This specification assumes that by default, a SIP authentication service will derive 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 "rcd" and "nam" key, which MAY also derive from other fields in the request, from customer profile data, or from access to external services. If the authentication service generates a PASSporT object containing "rcd" 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.

11.2. 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. Optionally, 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 will allow 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 9.1. This may include accepting a valid signature over a PASSporT even if it is signed with a credential that does not attest authority over the identity in the "orig" claim of the PASSporT, provided that the verification service has some other reason to trust the signer. No further guidance on verification service authorization policy is given here.

The behavior of a SIP UAS upon receiving an INVITE containing a PASSporT object with a "rcd" claim will largely remain 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.

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

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

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

12.1. 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.

12.2. Example for applying "rcd" as claims only

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

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

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

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

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

13. Acknowledgements

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

14. IANA Considerations

14.1. 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]

14.2. 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].

14.3. 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 three values, "nam", "jcd", and "jcl", which are specified in [RFCThis].

15. Security Considerations

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.

15.1. The use of JWT Claim Constraints in delegate certificates to exclude unauthorized Claims

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

16. References

16.1. Normative References

[I-D.housley-stir-enhance-rfc8226]
Housley, R., "Enhanced JWT Claim Constraints for STIR Certificates", draft-housley-stir-enhance-rfc8226-00 (work in progress), January 2021.

[I-D.ietf-sipcore-callinfo-rcd]
Wendt, C. and J. Peterson, "SIP Call-Info Parameters for Rich Call Data", draft-ietf-sipcore-callinfo-rcd-01 (work in progress), November 2020.

[I-D.ietf-stir-cert-delegation]
Peterson, J., "STIR Certificate Delegation", draft-ietf-stir-cert-delegation-03 (work in progress), July 2020.

[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>.

[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>.

[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>.

[RFC6919] Barnes, R., Kent, S., and E. Rescorla, "Further Key Words for Use in RFCs to Indicate Requirement Levels", RFC 6919, DOI 10.17487/RFC6919, April 2013, <https://www.rfc-editor.org/info/rfc6919>.

[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>.

[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>.

16.2. Informative References

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

[I-D.ietf-stir-oob] Rescorla, E. and J. Peterson, "STIR Out-of-Band Architecture and Use Cases", draft-ietf-stir-oob-07 (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>.

Authors' Addresses

Chris Wendt
Comcast
Comcast Technology Center
Philadelphia, PA 19103
USA

Email: chris-ietf@chriswendt.net

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

Email: jon.peterson@neustar.biz