Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 7, 2020

J. Peterson
Neustar Inc.
C. Wendt
Comcast

November 04, 2019

PASSporT Extension for Rich Call Data
draft-ietf-stir-passport-rcd-05

Abstract

This document extends PASSporT, a token for conveying cryptographically-signed call information about personal communications, to include rich data that can be transmitted and subsequently rendered to users, extending identifying information beyond human-readable display name comparable to the "Caller ID" function common on the telephone network. The 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 an integrity mechanism to optionally protect the handling of this information between authoritative and non-authoritative parties authoring 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 people 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 mechanisms which extends PASSporT to carry 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 a 'display-name' in the From header field value from the originating to terminating side, though it is an unsecured field that is not commonly trusted. The same is true of information in the Call-Info header field.

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 that may be 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 from an entity that is associated with the originated with the call. Either the caller themselves if they are authoritative, or a service provider, or a third-party service may be authoritative over the rich call data on behalf of the caller or service provider representing 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] and typically is the calling name that is a textual description of the caller. The second data is a set of RCD that is defined as part of the jCard definitions or extensions to that data. [I.D.wendt-sipcore-callinfo-rcd-00] describes the use of jCard 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.

In addition to the type of RCD that can be signed, there are three normative modes of use of the signing of Rich Call Data (RCD). The first and simplest mode is exclusively for when RCD content is direcly included as part of the claims (i.e. no URIs are included in the content). In this mode the set of claims is signed via standard PASSporT [RFC8225] and SIP identity header [RFC8224] procedures. The second mode is an extension of the first where a "rcd" claim is included and the content MAY or MAY NOT include URI external resources. In this mode, a "rcdi" integrity claim MUST be included. This integrity claim is defined in this document and provides a digest of the content so that, particularly for the case where there is 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 mode is yet another addition to both the first and second modes and incorporates the ability to include the digest of the integrity claim as a required value in the certificate used to create the PASSporT digital signature. This mode allows for cases where there is a different authoritative entity over

the content of the RCD, separate from the signer of the PASSporT itself allowing the ability to have policy around the content and potential review or pre-determination of allowed RCD content.

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 or whatever potential policy either via regulatory rules, a customer service agreements, or an enterprise brand consistency there may be the desire to pre-certify the specific use of rich data. This document defines a mechanism that allows for an 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.

The integrity mechanism is a process of generating a sufficiently strong cryptographic digest for both the "rcd" claim contents (e.g. "nam" and "jcd") 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"). This mechanism is inspired and based on the W3C Subresource Integrity specification (http://www.w3.org/TR/SRI/). This mechanism additionally defines the ability to constrain the digest and RCD integrity mechanism to be mandatory without modification using JWT Constraints defined in [RFC8226].

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 a similar field in other PASSporT using protocols. This key MUST be included once and MUST be included as 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 and may derive from the Call-Info header field value defined in [I.D.wendt-sipcore-callinfo-rcd] with a type of "jcard". As also defined in [I.D.wendt-sipcore-callinfo-rcd], format of the jCard and properties used should follow the normative usage and formating 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.

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. This link is intended to and may derive from the Call-Info header field value defined in [I.D.wendt-sipcore-callinfo-rcd] with a type of "jcard". As also defined in [I.D.wendt-sipcore-callinfo-rcd], format of the jCard and properties used should follow the normative usage and formating rules and procedures. The "jcl" key 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 "jcd" key included. The "jcd" and "jcl" keys should be mutually exclusive.

5.1.4. "rcdi" RCD integrity Claim

The "rcdi" claim is an optional claim that if the application requires integrity applied to the content of the "rcd" claim SHOULD be included with a corresponding "rcd" claim. The value of the "rcdi" key pair should contain a string that is defined as follows.

The first part of the string should define 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 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 "rcd" claim and the URLs contained in the claim. The details of the creation of this string are defined in the next section.

Example:
"rcdi" : "sha256-H8BRh8j48O9oYatfu5AZzq6A9RINQZngK7T62em8MUt1FLm52t+eX6xO"

5.1.5. Creation of the "rcd" digest

In order to facilitate proper verification of the digest and whether the "rcd" content was 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 constraint 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 the digest. Third, when the "rcd" data is verified at the Verification Service, it MUST verify the digest by constructing the "rcd" input digest string.

The procedures for the creation of the "rcd" input digest string is as follows.

1. Arrange the keys in the "rcd" claim value to be in lexicographic order.

2. Serialize the resulting "rcd" claim value JSON object to remove all white space and line breaks. The procedures of this deterministic JSON serialization is defined in [RFC8225], Section 9.

3. Identify, in order of where they appear in the serialized string, all of the URLs referencing external resource files.

4. Construct the "rcd" input string by first inserting the serialized "rcd" claim value.

5. If there is at least one URL identified, insert a semicolon character in the "rcd" input string.

6. Follow the semicolon with the Base64 encoded contents of resource file referenced by the first URL.

7. Repeat steps 5 and 6 for any additionally identified corresponding URLs.

Once the input digest string has been created, use this string to create the base64 encoded digest output that can be inserted into the "rcdi" claim as discussed in the last section.

Example "rcd" claim with URL:
```
"rcd": { "nam" : "James Bond",
         "jcl" : "https://example.org/james_bond.json"
       }
```

Example "rcd" input digest string (with line breaks for readability):
```
{"nam":"James Bond","jcl":"https://example.org/james_bond.json"};
ONG##*NCCCDJK123...KLJASlkJlkjsadlf2e3
```

Example "rcdi" claim:
```
"rcdi":"sha256-u5AZzq6A9RINQZngK7T62em8M"
```

5.2. JWT Constraint for "rcdi" claim

Once both the contents of the "rcd" claim is certified and the construction of the "rcdi" claim is complete, the "rcdi" digest is linked to the STIR certificate associated with the signature in the PASSporT via JWT Constraints as defined in [RFC8226] Section 8.

The certificate JWT Constraint MUST include both of the following:

- a "mustInclude" for the "rcd" claim

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

6. "rcd" Usage

The "rcd" claim may appear in any PASSporT claims object as an optional element. The creator of a PASSporT MAY however add a "ppt" value of "rcd" to the header of a PASSporT as well, in which case the PASSporT claims MUST contain a "rcd" 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 obejct 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":"sha256-H8BRh8j48O9oYatfu5AZzq6A9R6dQZngK7T62em8MUt1FLm52t+eX6xO"
}
```

An example of a PASSporT claims object that includes the "jcd" which is optional, but will also include the mandatory "nam" object is shown next (with line breaks for readability only).

```
{  "orig":{"tn":"12025551000"},
   "dest":{"tn":"12155551001"},
   "iat":1443208345,
   "rcd":{"nam":"James Bond","jcd":["vcard",[["version",{},"text","4.0"],
       ["fn",{},"text", "James Bond"],
       ["n",{},"text",["Bond","James","","","Mr."]],
       ["adr",{"type":"work"},"text",
         ["","","3100 Massachusetts Avenue NW","Washington","DC","20008","USA"]
       ],
       ["email",{},"text","007@mi6-hq.com"],
       ["tel",{"type":["voice","text","cell"],"pref":"1"},"uri",
        "tel:+1-202-555-1000"],
       ["tel",{"type":["fax"]},"uri","tel:+1-202-555-1001"],
       ["bday",{},"date","19241116"],
       ["logo",{},"uri",
       "https://upload.wikimedia.org/wikipedia/en/c/c5/
Fleming007impression.jpg"
       ]]]}}
```

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:

```
["vcard",
  [
    ["version", {}, "text", "4.0"],
    ["fn", {}, "text", "James Bond"],
    ["n", {}, "text", ["Bond", "James", "", "", "Mr."]],
    ["adr", {"type":"work"}, "text",
      ["", "", "3100 Massachusetts Avenue NW", "Washington", "DC", "20008",
      "USA"]
    ],
    ["email", {}, "text", "007@mi6-hq.com"],
    ["tel", { "type": ["voice", "text", "cell"], "pref": "1" }, "uri",
      "tel:+1-202-555-1000"],
    ["tel", { "type": ["fax"] }, "uri", "tel:+1-202-555-1001"],
    ["bday", {}, "date", "19241116"]
    ["logo", {}, "uri",
    "https://upload.wikimedia.org/wikipedia/en/c/c5/Fleming007impression.jpg"]
  ]
]
```

If that jCard is hosted at the example address of "https://example.org/james_bond.json", the corresponding PASSporT claims object would be as follows (with line breaks for readability only):

```
{  "orig":{"tn":"12025551000"},
   "dest":{"tn":"12155551001"},
   "iat":1443208345,
   "rcd":{"nam":"James Bond","jcl":"https://example.org/james_bond.json"}
   }
```

If we were to add a "rcdi" integrity claim to the last example, the corresponding PASSporT claims object would be as follows (with line breaks for readability only):

```
{  "orig":{"tn":"12025551000"},
   "dest":{"tn":"12155551001"},
   "iat":1443208345,
   "rcd":{"nam":"James Bond","jcl":"https://example.org/james_bond.json"}
   "rcdi":"sha256-H8BRh8j48O9oYatfu5AZzq6A9R6dQZngK7T62em8MUt1FLm52t+eX6xO"
   }
```

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 MUST be used. For re-construction of the "jcl", the Call-Info header with purpose "jcard" 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 shall be re-constructed following the same "rcdi" defined digest procedures in this document of all of the content and referenced URI content once downloaded.

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, the terminating side or 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 original authority'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 the 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

When a third party issues a PASSporT with an "rcd" claim, the PASSporT MUST contain the "rcd" "ppt" type in its header object. It moreover MUST include an "iss" claim as defined in [RFC7519] to indicate the source of this PASSporT; that field SHOULD be populated with the subject of the credential used to sign the PASSporT.

A PASSporT with a "ppt" of "rcd" MAY be signed with credentials that do not have authority over the identity that appears in the "orig" element of the PASSporT claims. Relying parties in STIR have always been left to make their own authorization decisions about whether or not the 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. [TBD claim - take from SHAKEN?]

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/HmtyNS7Ltrg9dlxkWzo
    eU7d7OV8HweTTDobV3itTmgPwCFjaEmMyEI3d7SyN21yNDo2ER/Ovgtw0Lu5csIp
    pPqOg1uXndzHbG7mR6Rl9BnUhHufVRbp51Mn3w0gfUs="; \
    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 "rcd" 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.

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, for example, calling name information, 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.

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 Robert Sparks, Russ Housley, and Eric Burger for helpful suggestions and comments.

14. IANA Considerations

14.1. JSON Web Token Claim

This specification requests that the IANA add two 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]

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.

More TBD.

16. References

16.1. Normative References

[I-D.ietf-stir-oob]
Rescorla, E. and J. Peterson, "STIR Out-of-Band Architecture and Use Cases", draft-ietf-stir-oob-05 (work in progress), July 2019.

[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>.

[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.

[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

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

Email: jon.peterson@neustar.biz

Chris Wendt
Comcast
Comcast Technology Center
Philadelphia, PA 19103
USA

Email: chris-ietf@chriswendt.net