Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 20, 2021

J. Peterson
Neustar Inc.
C. Wendt
Comcast

November 16, 2020

PASSporT Extension for Rich Call Data
draft-ietf-stir-passport-rcd-09

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 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 procedures which extend PASSporT objects 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 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 can not 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 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 origination of 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] 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.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 "reason" parameter intended for description of the intent or reason for a particular call. A new 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.

In addition to the type of RCD that can be signed, there are three modes of use of the signing of Rich Call Data (RCD). The first and simplest mode is exclusively for when all RCD content is directly

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 includes a URI identifying external resources. In this mode, a "rcdi" integrity claim MUST be included. This integrity claim is defined later 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 an extension to both the first and second modes and incorporates the ability to include the digest of the integrity claim as a required value, using JWT Constraints as defined in [RFC8226], in the certificate used to create the PASSporT digital signature. This mode allows for 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 policy around the content and potential review or pre-determination of allowed RCD content.

More generally, either of the claims defined in this or future specifications content can be protected by the authoritative certificate creators by inclusion in the [RFC8226] defined certificate's JWT Constraints.

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 the specific use of rich call 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 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.

5.1.4. "rcdi" RCD integrity Claim

The "rcdi" claim is an optional claim that SHOULD be included if the application requires integrity to be applied to the content of the "rcd" claim and if included MUST be included only once 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-H8BRh8j48O9oYatfu5AZzq6A9RINQZngK7T62em8MUt1FLm52"

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 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 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 at the end of the "rcd" serialized 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 including URLs contained in resources referenced by other URLs. When or if these nested URLs occur in the contents referred to by a parent URL, the insertion of the Base64 encoded contents should be included for all child URLs before moving to any subsequent parent URL.

Once the input serialized 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"
```

5.1.6. 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 Claim Constraints as defined in [RFC8226] Section 8.

The certificate JWT Claims 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.

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.

5.2. 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"
```

5.2.1. JWT Constraint for "cdn" claim

The integrity of the "crn" claim can optionally be protected by the authoritative certificate creator using JWT Constraints in the certificate.

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 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-H8BRh8j48O9oYatfu5AZzq6A9R6dQZngK7T62em8MUt1FLm52"
}
```

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/jb.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/jb.json"}
   "rcdi":"sha256-H8BRh8j48O9oYatfu5AZzq6A9R6dQZngK7T62em8MUt1FLm"
   }
```

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 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.

7.3. Compact form of the "crn" PASSporT claim

Compact form of a "crn" PASSporT claim shall be re-constructed using the "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 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

A third-party PASSporT, which contains such an "iss" element, 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 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. As stated in the previous section, the use of "iss" MUST reflect the Organization (O) field 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.

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, and Eric Burger 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.

16. References

16.1. Normative References

[I-D.ietf-sipcore-callinfo-rcd]
Wendt, C. and J. Peterson, "SIP Call-Info Parameters for Rich Call Data", draft-ietf-sipcore-callinfo-rcd-00 (work in progress), November 2020.

[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.

[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>.

[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

STIR
Internet-Draft
Intended status: Standards Track
Expires: May 6, 2021

M. Dolly
AT&T
C. Wendt
Comcast

November 02, 2020

Assertion Values for a Resource Priority Header Claim and a SIP Priority Header Claim in Support of Emergency Services Networks
draft-ietf-stir-rph-emergency-services-04

Abstract

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

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 6, 2021.

Table of Contents

1. Introduction

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

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

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

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

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

2. Terminology

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

3. New Assertion Values for "rph" claim

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

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

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

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

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

```
{
  "orig":{"tn":"12155551212"},
  "dest":{"uri":["urn:service:sos"]},
  "iat":1443208345,
  "rph":{"auth":["esnet.1"]}
}
```

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

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

```
{
  "orig":{"tn":"12155551213"},
  "dest":{"tn":["12155551212"]},
  "iat":1443208345,
  "rph":{"auth":["esnet.0"]}
}
```

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

4. The SIP Priority header "sph" claim

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

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

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

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

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

```
{
  "orig":{"tn":"12155551213"},
  "dest":{"tn":["12155551212"]},
  "iat":1443208345,
  "rph":{"auth":["esnet.0"]},
  "sph":"psap-callback"
}
```

5. Order of Claim Keys

The order of the claim keys MUST follow the rules of [RFC8225] Section 9; the claim keys MUST appear in lexicographic order. Therefore, the claim keys discussed in this document appear in the PASSporT Payload in the following order,

- dest
- iat
- orig
- rph

- sph

6. Compact Form of PASSporT

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

7. Acknowledgements

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

8. IANA Considerations

8.1. JSON Web Token claims

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

Claim Name: "sph"

Claim Description: SIP Priority header field

Change Controller: IESG

Specification Document(s): [RFCThis]

9. Security Considerations

The security considerations discussed in [RFC8224], Section 12, are applicable here.

10. References

10.1. Normative References

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

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

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

[RFC7090] Schulzrinne, H., Tschofenig, H., Holmberg, C., and M. Patel, "Public Safety Answering Point (PSAP) Callback", RFC 7090, DOI 10.17487/RFC7090, April 2014, <https://www.rfc-editor.org/info/rfc7090>.

[RFC7135] Polk, J., "Registering a SIP Resource Priority Header Field Namespace for Local Emergency Communications", RFC 7135, DOI 10.17487/RFC7135, May 2014, <https://www.rfc-editor.org/info/rfc7135>.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <https://www.rfc-editor.org/info/rfc7519>.

[RFC8224] Peterson, J., Jennings, C., Rescorla, E., and C. Wendt, "Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 8224, DOI 10.17487/RFC8224, February 2018, <https://www.rfc-editor.org/info/rfc8224>.

[RFC8225] Wendt, C. and J. Peterson, "PASSporT: Personal Assertion Token", RFC 8225, DOI 10.17487/RFC8225, February 2018, <https://www.rfc-editor.org/info/rfc8225>.

[RFC8443] Singh, R., Dolly, M., Das, S., and A. Nguyen, "Personal Assertion Token (PASSporT) Extension for Resource Priority Authorization", RFC 8443, DOI 10.17487/RFC8443, August 2018, <https://www.rfc-editor.org/info/rfc8443>.

10.2. Informative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

Authors' Addresses

Martin Dolly
AT&T

Email: md3135@att.com

Chris Wendt
Comcast
Comcast Technology Center
Philadelphia, PA 19103
USA

Email: chris-ietf@chriswendt.net

Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 6, 2021

J. Peterson
Neustar

November 2, 2020

Out-of-Band STIR for Service Providers
draft-ietf-stir-servprovider-oob-00

Abstract

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

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 6, 2021.

Table of Contents

1. Introduction

STIR [RFC8224] provides a cryptographic assurance of the identity of calling parties in order to prevent impersonation, which is a key enabler of unwanted robocalls, swatting, vishing, voicemail hacking, and similar attacks (see [RFC7340]). The STIR out-of-band [I-D.ietf-stir-oob] framework enables the delivery of PASSporT [RFC8225] objects through a Call Placement Service (CPS), rather than carrying them within a signaling protocol such as SIP. Out-of-band conveyance is valuable when end-to-end SIP delivery of calls is partly or entirely unavailable due to network border policies, calls routinely transitting a gateway to the PSTN, or similar circumstances.

While out-of-band STIR can be implemented as an open Internet service, it then requires complex security measures to enable the CPS function without allowing the CPS to collect data about the parties placing calls. This specification describes CPS implementations that act specifically on behalf of service providers who will be processing the calls that STIR secures, and who thus will learn about the parties to communication independently, so an alternative security architecture becomes possible.

Environments that might support this flavor of STIR out-of-band include carriers, large enterprises, call centers, or any Internet service that aggregates on behalf of a large number of telephone endpoints.

2. Terminology

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

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

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

The process of locating a destination CPS and submitting a PASSporT requires Internet connectivity between the call originator and the CPS. If the CPS is deployed in the terminating service provider network, that network connectivity could be leveraged to initiate a SIP session, during which in-band STIR could be used. The applicability of this architecture is therefore to those cases where, for whatever reason, SIP calls cannot reliably be placed end-to-end, but an HTTP transaction can reliably be sent to the destination network from the out-of-band authentication service (OOB-AS) in the caller's network. It is hoped that as IP connectivity between telephone providers increases, there will be less need for an out-of-band mechanism, but it can serve as a fallback mechanism in cases where service providers cannot predict whether end-to-end delivery of SIP calls will occur.

4. Advertising a CPS

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

list of available CPS providers, say. In more pluralist environments, some mechanism is needed to discover the CPS associated with the target of a call.

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

The format of a service provider CPS advertisement is a simple JSON object containing one or more pairs of TNAuthList values pointing to the URIs of CPSs, e.g. { "1234":"https://cps.example.com" }. TNAuthList values can be either Service Provider Codes (SPCs) or telephone numbers or number ranges. CPS URIs MUST be HTTPS URIs. [More TBD].

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

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

5. Submitting a PASSporT

Submitting a PASSporT to a CPS as specified in the STIR out-of-band framework [I-D.ietf-stir-oob] requires security measures which are intended to prevent the CPS from learning the identity of the caller (or callee), to the degree possible. In this service provider case, however, the CPS is operated by the service provider of the callee

(or an entity operating on their behalf), and as such the information that appears in the PASSporT is redundant with call signaling that the terminating party will receive anyway. Therefore, the service provider out-of-band framework does not attempt to conceal the identity of the originating or terminating party from the CPS.

An out-of-band authentication service (OOB-AS) forms a secure connection with the target CPS. This may happen at the time a call is being placed, or it may be a persistent connection, if there is a significant volume of traffic sent over this interface. The OOB-AS SHOULD authenticate itself to the CPS using its STIR credential [RFC8226]the same one it would use to sign calls via mutual TLS; this helps mitigate the risk of flooding that more open OOB implementations may face. Furthermore, use of mutual TLS prevents attackers from replaying captured PASSporTs to the CPS. A CPS makes its own policy decision as to whether it will accept calls from a particular OOB-AS, and at what volumes.

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

6. PASSporT Retrieval

The STIR out-of-band framework [I-D.ietf-stir-oob] proposes two means that called parties can acquire PASSporTs out-of-band: through a retrieval interface, or through a subscription interface. In the service provider context, where many calls occur simultaneously, an out-of-band capable verification service may therefore operate in one of two modes: it can either pull PASSporTs from the CPS after calls arrive, or receive push notifications from the CPS for incoming calls.

If a CPS serves only one service provider, then all PASSporTs submitted to the CPS are made available to the OOB-VS of that provider; indeed, the CPS and OOB-VS may be colocated or effectively operated as a consolidated system. In a multi-provider environment, the STIR credential of the terminating domain can be used by the CPS

to determine the range of TNAuthLists for which an OOB-VS is entitled to receive PASSporTs; this may be through a mechanism like mutual TLS, or through using the STIR credential to sign a token that is submitted to the CPS by the retrieving OOB-VS. Note that a CPS will need to inspect the "dest" element of a PASSporT to determine which OOB-VS should receive the PASSporT in this case. [TBD: Which sub/not protocol to use for the case where the CPS and OOB-VS are not composed in a single function?]

Pulling of PASSporTs from the CPS will follow the basic REST flow described in [I-D.ietf-stir-oob] Section 9. In the push interface case, exactly how a CPS determines which PASSporTs to send to an out-of-band verification service is a matter of implementation. An OOB-VS could for example subscribe to a range of telephone numbers, which will be directed to that OOB-VS by the CPS (provided the OOB-VS is authorized to receive them by the CPS).

In the pull model, a terminating service provider contacts the CPS via its OOB-VS after having received a call in cases when the call signaling does not itself carry a STIR signature. In the push model, a PASSporT might be sent to the OOB-VS either before or after unsigned call signaling has been received by the terminating domain. Domains using the push model may therefore need to adopt a model where call signaling is held momentarily in order to await the potential arrival of a PASSporT at the OOB-VS. The exact timing of this, and its interaction with the substitution attack described in [I-D.ietf-stir-oob] Section 7.4, will be the covered by future versions of this specification.

7. Gateways

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

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

8. Acknowledgments

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

9. IANA Considerations

This memo includes no request to IANA.

10. Security Considerations

TBD.

11. Informative References

[I-D.ietf-stir-oob]
Rescorla, E. and J. Peterson, "STIR Out-of-Band Architecture and Use Cases", draft-ietf-stir-oob-07 (work in progress), March 2020.

[I-D.ietf-stir-passport-divert]
Peterson, J., "PASSporT Extension for Diverted Calls", draft-ietf-stir-passport-divert-09 (work in progress), July 2020.

[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>.

[RFC3311] Rosenberg, J., "The Session Initiation Protocol (SIP) UPDATE Method", RFC 3311, DOI 10.17487/RFC3311, October 2002, <https://www.rfc-editor.org/info/rfc3311>.

[RFC4916] Elwell, J., "Connected Identity in the Session Initiation Protocol (SIP)", RFC 4916, DOI 10.17487/RFC4916, June 2007, <https://www.rfc-editor.org/info/rfc4916>.

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

[RFC7340] Peterson, J., Schulzrinne, H., and H. Tschofenig, "Secure Telephone Identity Problem Statement and Requirements", RFC 7340, DOI 10.17487/RFC7340, September 2014, <https://www.rfc-editor.org/info/rfc7340>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8224] Peterson, J., Jennings, C., Rescorla, E., and C. Wendt, "Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 8224, DOI 10.17487/RFC8224, February 2018, <https://www.rfc-editor.org/info/rfc8224>.

[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>.

Author's Address

Jon Peterson
Neustar, Inc.

Email: jon.peterson@neustar.biz

Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 6, 2021

J. Peterson
Neustar
C. Wendt
Comcast

November 2, 2020

Messaging Use Cases for STIR
draft-peterson-stir-messaging-00

Abstract

Secure Telephone Identity Revisited (STIR) provides a means of attesting the identity of a telephone caller via a signed token in order to prevent impersonation of a calling party number, which is a key enabler for illegal robocalling. Similar impersonation is leveraged by bad actors in the text messaging space. This document considers the applicability of STIR's Persona Assertion Token (PASSporT) and certificate issuance framework to instant text and multimedia messaging use cases, both for messages carried or negotiated by SIP, and for non-SIP messaging.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 6, 2021.

Table of Contents

1. Introduction

The STIR problem statement [RFC7340] describes widespread problems enabled by impersonation in the telephone network, including illegal robocalling, voicemail hacking, and swatting. As telephone services are increasingly migrating onto the Internet and using Voice over IP (VoIP) protocols such as SIP [RFC3261], it is necessary for these protocols to support stronger identity mechanisms to prevent impersonation. [RFC8224] defines a SIP Identity header field capable of carrying PASSporT [RFC8225] objects in SIP as a means to cryptographically attest that the originator of a telephone call is authorized to use the calling party number (or, for native SIP cases, SIP URI) associated with the originator of the call.

The problem of bulk, unsolicited commercial communications is not however limited to telephone calls. Increasingly, spammers and fraudsters are turning to messaging applications to deliver undesired content to consumers. In some respects, mitigating these unwanted messages resembles the email spam problem: textual analysis of the message contents can be used to fingerprint content that is generated by spammers, for example. However, encrypted messaging is becoming more common, and analysis of message contents may no longer be a reliably way to mitigate messaging spam in the future. And as STIR sees further deployment in the telephone network, it seems likely that the governance structures put in place for securing telephone

network resources with STIR could be repurposed to help secure the messaging ecosystem.

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

2. Terminology

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

3. Applicability to Messaging Systems

At a high level, baseline PASSporT [RFC8225] claims provide similar value to number-based messaging as they do to traditional telephone calls. A signature over the calling and called party numbers, along with a timestamp, could already help to prevent impersonation in the mobile messaging ecosystem. When it comes to protecting message contents, broadly, there are ways that the PASSporT mechanism of STIR could apply to messaging: first, a PASSporT could be used to securely negotiate a session over which messages will be exchanged; and second, in sessionless scenarios a PASSporT could be generated on a per-message basis with its own built-in message security.

For the first case, where SIP negotiates a session where the media will be text messages, as for example with the Message Session Relay Protocol (MSRP) [RFC4975], the usage of STIR would deviate little from [RFC8224]. An INVITE request sent with an Identity header containing a PASSporT with the proper calling and called party numbers would then negotiate an MSRP session the same way that an INVITE for a telephone call would negotiate an audio session. The same would apply to sessions that negotiate text over RTP via [RFC4103] or similar mechanisms. In these cases, STIR for messaging should not require any further protocol enhancements.

[TBD: Also consider the applicability of "mkey" to these schemes, and RFC8862? Also, any interest in MLS interaction?]

In the second case, SIP also has a method for sending messages a the body of a SIP request: the MESSAGE [RFC3428] method. The interaction

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

Moreover, the MESSAGE method is not commonly used today to carry messages for consumer devices. A variety of non-SIP protocols, both those integrated in to the traditional telephone network and those based on over-the-top applications, are responsible for most of the messaging that is sent to and from telephone numbers. This specification proposes that the STIR credentials assigned to service providers could be leveraged to sign for PASSporTs for messages that originate from telephone numbers. In order to apply PASSporT to textual or multimedia messaging, a new claim is here defined to provide a hash over message contents.

4. PASSporTs and Messaging

In order to differentiate a PASSporT for a message from a PASSporT used to secure a telephone call, this document defines a new "msg" PASSporT Type. This prevents the replay of a PASSporT for a message to putatively secure a call, or vice versa.

This specification defines a new optional JWT [RFC7519] claim "msgi" which provides a digest over the contents of a message, which may be a text message, or a more complex multimedia message. "msgi" MUST NOT appear in PASSporTs with a type other than "msg", but they are OPTIONAL in "msg" PASSporTs, as integrity for messages may be provided by some other service (e.g. [RFC8591]). Implementations of "msgi" MUST support the following hash algorithms: "SHA256", "SHA384", or "SHA512", which are defined as part of the SHA-2 set of cryptographic hash functions by the NIST.

[TBD: Do we need algorithmic agility here?]

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

[TBD: Canonicalization procedures. Maybe we need separate procedures for plain text (like, SMPP), rich text, and then more complex multimedia messages? Definitely a danger of scope creep. Anything we could easily steal here?]

At the end result of the process, the digest becomes the value of the JWT "msgi" claim, as per this example:

"msgi" :
"sha256-H8BRh8j48O9oYatfu5AZzq6A9RINQZngK7T62em8MUt1FLm52t+eX6xO"

4.1. PASSporTs Conveyance with Messaging

If the message is being conveyed in SIP, via the MESSAGE method, then the PASSporT could be conveyed in an Identity header field in that request. The authentication and verification service procedures for populating that PASSporT would follow [RFC8224], with the addition of the "msgi" claim defined in Section 4.

In cases where messages are conveyed by some protocol other than SIP, that protocol might itself have some way of conveying PASSporTs. But there will surely be cases where legacy transmission of messages will not permit an accompanying PASSporT, in which case something like out-of-band [I-D.ietf-stir-oob] conveyance would be the only way to deliver the PASSporT.

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

5. Certificates and Messaging

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

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

6. Acknowledgments

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

7. IANA Considerations

7.1. JSON Web Token Claims Registration

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

Claim Name: "msgi"

Claim Description: Message Integrity Information

Change Controller: IESG

Specification Document(s): [RFCThis]

7.2. PASSporT Type Registration

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

"msg" as defined in [RFCThis] Section 4.

8. Security Considerations

TBD.

9. Informative References

[I-D.ietf-stir-oob]
Rescorla, E. and J. Peterson, "STIR Out-of-Band Architecture and Use Cases", draft-ietf-stir-oob-07 (work in progress), March 2020.

[I-D.ietf-stir-passport-divert]
Peterson, J., "PASSporT Extension for Diverted Calls", draft-ietf-stir-passport-divert-09 (work in progress), July 2020.

[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>.

[RFC3311] Rosenberg, J., "The Session Initiation Protocol (SIP) UPDATE Method", RFC 3311, DOI 10.17487/RFC3311, October 2002, <https://www.rfc-editor.org/info/rfc3311>.

[RFC3428] Campbell, B., Ed., Rosenberg, J., Schulzrinne, H., Huitema, C., and D. Gurle, "Session Initiation Protocol (SIP) Extension for Instant Messaging", RFC 3428, DOI 10.17487/RFC3428, December 2002, <https://www.rfc-editor.org/info/rfc3428>.

[RFC4103] Hellstrom, G. and P. Jones, "RTP Payload for Text Conversation", RFC 4103, DOI 10.17487/RFC4103, June 2005, <https://www.rfc-editor.org/info/rfc4103>.

[RFC4474] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 4474, DOI 10.17487/RFC4474, August 2006, <https://www.rfc-editor.org/info/rfc4474>.

[RFC4916] Elwell, J., "Connected Identity in the Session Initiation Protocol (SIP)", RFC 4916, DOI 10.17487/RFC4916, June 2007, <https://www.rfc-editor.org/info/rfc4916>.

[RFC4975] Campbell, B., Ed., Mahy, R., Ed., and C. Jennings, Ed., "The Message Session Relay Protocol (MSRP)", RFC 4975, DOI 10.17487/RFC4975, September 2007, <https://www.rfc-editor.org/info/rfc4975>.

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

[RFC7340] Peterson, J., Schulzrinne, H., and H. Tschofenig, "Secure Telephone Identity Problem Statement and Requirements", RFC 7340, DOI 10.17487/RFC7340, September 2014, <https://www.rfc-editor.org/info/rfc7340>.

[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>.

[RFC8591] Campbell, B. and R. Housley, "SIP-Based Messaging with S/MIME", RFC 8591, DOI 10.17487/RFC8591, April 2019, <https://www.rfc-editor.org/info/rfc8591>.

Authors' Addresses

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

Email: jon.peterson@team.neustar

Chris Wendt
Comcast
One Comcast Center
Philadelphia, PA 19103
USA

Email: chris-ietf@chriswendt.net

Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 6, 2021

J. Peterson
Neustar
C. Wendt
Comcast

November 2, 2020

Connected Identity for STIR
draft-peterson-stir-rfc4916-update-02

Abstract

The SIP Identity header conveys cryptographic identity information about the originators of SIP requests. The Secure Telephone Identity Revisited (STIR) framework however provides no means for determining the identity of the called party in a traditional telephone calling scenario. This document updates prior guidance on the "connected identity" problem to reflect the changes to SIP Identity that accompanied STIR, and considers a revised problem space for connected identity as a means of detecting calls that have been retargeted to a party impersonating the intended destination, as well as spoofing of mid-dialog or dialog-terminating events by intermediaries or third parties.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 6, 2021.

Table of Contents

1. Introduction

The Session Initiation Protocol (SIP) [RFC3261] initiates sessions, and as a step in establishing sessions, it exchanges information about the parties at both ends of a session. Users review information about the calling party, for example, to determine whether to accept communications initiated by a SIP, in the same way that users of the telephone network assess "Caller ID" information before picking up calls. This information may sometimes be consumed by automata to make authorization decisions.

STIR [RFC8224] provides a cryptographic assurance of the identity of calling parties in order to prevent impersonation, which is a key enabler of unwanted robocalls, swatting, vishing, voicemail hacking, and similar attacks (see [RFC7340]). There also exists a related problem: the identity of the party who answers a call can differ from that of the initial called party for various innocuous reasons such as call forwarding, but in certain network environments it is possible for attackers to hijack the route of a called number and direct it to a resource controlled by the attacker. It can potentially be difficult to determine why a call reached a target other than the one originally intended, and whether the party ultimately reached by the call is one that the caller should trust. The property of providing identity in the backwards direction of a call is here called "connected identity."

Previous work on connected identity focused on fixing the core semantics of SIP. [RFC4916] allowed a mid-dialog request, such as an UPDATE [RFC3311], to convey identity in either direction within the context of an existing INVITE-initiated dialog. In an update to the original [RFC3261] behavior, [RFC4916] allowed that UPDATE to alter the From header field value for requests in the backwards direction: previously [RFC3261] required that the From header field values sent in requests in the backwards direction reflect the To header field value of the dialog-forming request, for various backwards-compatibility reasons. In other words, if Alice sent a dialog-forming request to Bob, then under the original [RFC3261] rules, even if Bob's SIP service forwarded that dialog-forming request to Carol, Carol would still be required to put Bob's identity in the From header field value in any mid-dialog requests in the backwards direction.

One of the original motivating use cases for [RFC4916] was the use of connected identity with the SIP Identity [RFC4474] header field. While a mid-dialog request in the backwards direction (e.g. UPDATE) can be signed with Identity like any other SIP request, forwarded requests would not be signable without the ability to change the mid-dialog From header field value: Carol, say, would not be able to furnish a key to sign for Bob's identity, if Carol wanted to sign requests in the backwards direction. Carol would however be able to sign for her own identity in the From header field value, if mid-dialog requests in the backwards direction were permitted to vary from the original To header field value.

With the obsolence of [RFC4474] by [RFC8224], this specification updates [RFC4916] to reflect the changes to the SIP Identity header and the revised problem space of STIR. It also explores some new features that would be enabled by connected identity for STIR, including the use of connected identity to prevent route hijacking and to notify callers when an expected called party has successfully been reached. This document also addresses concerns about applying [RFC4916] connected identity to STIR as given in [RFC8862].

2. Terminology

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

3. Connected Identity Problem Statement for STIR

The STIR problem statement [RFC7340] enumerates robocalling, voicemail hacking, vishing, and swatting as problems with the modern telephone network that are enabled, or abetted, by impersonation: by

the ability of a calling party to arbitrarily set the telephone number that will be rendered to end users to identify the caller.

Today, sophisticated adversaries can redirect calls on the PSTN to destinations other than the intended called party. For some call centers, like those associated with financial institutions, healthcare, and emergency services, an attacker could hope to gain valuable information about people or to prevent some classes of important services. Moreover, on the Internet, the lack of any centralized or even federated routing system for telephone numbers has resulted in deployments where the routing of calls is arbitrary: calls to telephone numbers might be unceremoniously dumped on a PSTN gateway, they might be sent to a default intermediary that makes forwarding decisions based on a local flat file, various mechanisms like private ENUM might be consulted, or routing might be determined in some other, domain specific way. In short, there are numerous attack surfaces that an adversary could explore to attempt to redirect calls to a particular number to someplace other than the intended destination.

Another motivating use case for connected identity is mid-dialog requests, including BYE. The potential for an intermediary to generate a forged BYE in the backwards direction has always been built-in to the stateful dialog management of SIP. There is a class of mobile fraud attacks ("short-stopping") that rely on intermediary networks making it appear as if a call has terminated to one side, while maintaining that the call is still active to the other, in order to create a billing discrepancy that could be pocketed by the intermediary. If BYE requests in both directions of a SIP dialog could be authenticated with STIR, just like dialog-forming requests, then another impersonation vector leading to fraud in the telephone network could be shut down.

There are however practical limits to what securing the signaling can achieve. [RFC4916] rightly observed that once a SIP call has been answered, the called party can be replaced by a different party with a different identity due to call transfer, call park and retrieval, and so on. In some cases, due to the presence of a back-to-back user agent, it can be effectively impossible for the calling party to know that this has happened. The problem statement considered for STIR focuses solely on signaling, not whether media from the connected party should be rendered to the caller when a dialog has been established. This specification does not consider further any threats that arise from a substitution of media.

4. Authorization Policy for Callers

In a traditional telephone call, the called party receives an alerting signal and can make a decision about whether or not to pick up a phone. They may have access to displayed information, like "Caller ID", to help them arrive at an authorization decision. The situation is more complicated for callers, however: callers typically expect to be connected to the proper destination and are often holding telephones in a position that would not enable them to see displayed information, if any were available for them to review--and moreover, their most direct response to a security breach would be to hang up the call they were in the middle of placing.

While this specification will not prescribe any user experience associated with placing a call, it assumes that callers might have some way to a set an authorization posture that will result in the right thing happening when the connected identity is not expected. This is analogous to a situation where SRTP negotiation fails because the keys exchanges at the media layer do not match fingerprints exchanged at the signaling layer: when a user requests confidentiality services, and they are unavailable, media should not be exchanged. Thus we assume that users have a way in their interface to require this criticality, on a per-call basis, or perhaps on a per-destination basis. Similarly, users will not always place calls where the connected identity is crucial--but when they do, they should have a way to tell their devices that the call should not be completed if it arrives at an unexpected party.

Ultimately, authorization policy for called parties is difficult to set, as calls can end up at unexpected places for legitimate reasons. Some work has been done to make sure that secure diversion works with STIR, in for example [I-D.ietf-stir-passport-divert]. Those indications can be consumed by on the terminating side by verification services to determine that a call has reached its eventual destination for the right reasons. The only way those diversion PASSporTs will be seen by the calling party is if redirection is used (SIP 3XX responses) instead of retargeting; while some network policies may want to conceal service logic from the originating party, sending redirections in the backwards direction is the only current defined way for secure indications of redirection to be revealed to the calling party. That in turn would allow the calling user agent to have a strong assurance that legitimate entities in the call path caused the request to reach a party that the caller did not anticipate.

5. Pre-Association with Destinations

Any connected identity mechanism will work best if the user knows before initiating a call that connected identity is supported by the destination side. Not every institution that a user wants to connect to securely will support STIR and connected identity out of the gate.

The user interface of modern smartphones support an address book from which users select telephone numbers to dial. Even when dialing a number manually, the interface frequently checks the address book and will display to users any provisioned name for the target of the call if one exists. Similarly, when clicking on a telephone number viewed on a web page, or similar service, smartphone often prompt users approve the access to the outbound dialer. These sorts of decision points, when the user is still interacting with the user interface, provide an opportunity to form a pre-association with the destination, and potentially even to exchange STIR PASSporTs in order to validate whether or not the expected destination can be reached securely. Again, this is probably most meaningful for contacting financial, government, or emergency services, for cases where reaching an unintended destination may have serious consequences.

Future versions of this specification will explore how the security features of destinations can be discovered before calls are set up so that calling parties can make more informed authorization decisions. This may rely on the establishment of a provisional, media-less SIP dialog which can then negotiate media when the user approves of the destination. In some environments, that may require the use of mechanisms defined by [I-D.ietf-stir-oob].

6. Examples

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

7. Updates to RFC4916

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

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

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

8. Acknowledgments

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

9. IANA Considerations

This memo includes no request to IANA.

10. Security Considerations

TBD.

11. Informative References

[I-D.ietf-modern-problem-framework]
Peterson, J. and T. McGarry, "Modern Problem Statement, Use Cases, and Framework", draft-ietf-modern-problem-framework-04 (work in progress), March 2018.

[I-D.ietf-stir-oob]
Rescorla, E. and J. Peterson, "STIR Out-of-Band Architecture and Use Cases", draft-ietf-stir-oob-07 (work in progress), March 2020.

[I-D.ietf-stir-passport-divert]
Peterson, J., "PASSporT Extension for Diverted Calls", draft-ietf-stir-passport-divert-09 (work in progress), July 2020.

[I-D.peterson-modern-teri]
Peterson, J., "An Architecture and Information Model for Telephone-Related Information (TeRI)", draft-peterson-modern-teri-04 (work in progress), March 2018.

[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>.

[RFC3311] Rosenberg, J., "The Session Initiation Protocol (SIP) UPDATE Method", RFC 3311, DOI 10.17487/RFC3311, October 2002, <https://www.rfc-editor.org/info/rfc3311>.

[RFC4474] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 4474, DOI 10.17487/RFC4474, August 2006, <https://www.rfc-editor.org/info/rfc4474>.

[RFC4916] Elwell, J., "Connected Identity in the Session Initiation Protocol (SIP)", RFC 4916, DOI 10.17487/RFC4916, June 2007, <https://www.rfc-editor.org/info/rfc4916>.

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

[RFC7340] Peterson, J., Schulzrinne, H., and H. Tschofenig, "Secure Telephone Identity Problem Statement and Requirements", RFC 7340, DOI 10.17487/RFC7340, September 2014, <https://www.rfc-editor.org/info/rfc7340>.

[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>.

Authors' Addresses

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

Email: jon.peterson@team.neustar

Chris Wendt
Comcast
One Comcast Center
Philadelphia, PA 19103
USA

Email: chris-ietf@chriswendt.net