Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 14, 2017

J. Peterson
Neustar
C. Wendt
Comcast

June 12, 2017

PASSporT Extension for Caller Name
draft-peterson-stir-cnam-02.txt

Abstract

This document extends PASSporT, a token for conveying cryptographically-signed information about the people involved in personal communications, to include a human-readable display name comparable to the "Caller ID" function common on the telephone network. The element defined for this purpose is extensible to include related information about callers that helps people decide whether to pick up the phone.

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 http://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 December 14, 2017.

Table of Contents

1. Introduction

PASSporT [I-D.ietf-stir-passport] is a token format based on JWT [RFC7519] for conveying cryptographically-signed information about the people involved in personal communications; it is used with STIR [I-D.ietf-stir-rfc4474bis] to convey a signed assertion of the identity of the participants in real-time communications established via a protocol like SIP. The STIR problem statement [RFC7340] declared securing the display name of callers outside of STIR's initial scope, so baseline STIR provides no features for caller name. This specification documents an optional mechanism for PASSporT and the associated STIR mechanisms which extends PASSporT to carry additional elements conveying richer information, provided it is 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 typically be rendered to the called party during alerting.

In the traditional telephone network, the display name associated with a call is typically provided in one of three ways: by the originator of a call, by a third-party service queried at the terminating side, or through a local address book maintained by a

device on the terminating side. The STIR architecture lends itself especially to the first of these approaches, as it assumes that an authority on the originating side of the call provides a cryptographic assurance of the validity of the calling party number in order to prevent impersonation attacks. That same authority could sign for a display name associated with that number, which the terminating side could render to the user when the call is alerting. Even when the originating side does not provide a display name for the caller, the cryptographic attestation of the validity of the calling number provided by STIR still allows the terminating side to query a local or remote service for a name associated with that number without fear that the number has been impersonated by the caller; STIR thus makes "Caller ID" more secure even when there is no first-party attestation of a display name. For these cases, this specification outlines various ways that a display name for a calling party could be determined at the terminating side in a secure fashion.

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 RFC 2119 [RFC2119] and RFC 6919 [RFC6919].

3. PASSporT ’cna’ Claim

This specification defines a new JSON Web Token claim for "cna", the value of which is an array of JSON elements which always includes a display name associated with the originator of personal communications. This name may for example derive from the display-name component of the From header field value of a SIP request, or a similar field in other PASSporT using protocols.

The "cna" claim may appear in any PASSporT claims object as an optional element. The creator of a PASSporT MAY however add a "ppt" value of "cna" to the header of a PASSporT object as well, in which case the PASSporT claims MUST contain a "cna" 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 wih the "ppt" included will look as follows:

```
{ "typ":"passport",
  "ppt":"cna",
  "alg":"RS256",
  "x5u":"https://www.example.com/cert.cer" }
```

The PASSporT claims object will then contain the "cna" key with its corresponding value. The value of "cna" 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].

```
{ "orig":{"tn":"12155551212"},
  "dest":{"tn":"12155551213"},
  "iat":1443208345,
      "iss":"Example, Inc.",
  "cna":{"nam":"Alice A"} }
```

After the header and claims PASSporT objects have been constructed, their signature is generated normally per the guidance in [I-D.ietf-stir-passport].

4. Further Information Associated with Callers

Beyond naming information, 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 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 process 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 "cna" array; see Section 8.3. Specific extensions to the "cna" PASSporT claim are left for future specification.

While in the telephone network, information about the name of the calling party traditionally derives from the originating service provider, 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 "cna" object, which requires special signing rules.

5. Third Party Uses

When secure calling name information is not provided by an originating authentication service, the terminating side may use other means to determine the caller's name. For example, a third-party information service might be queried with the calling party's number in order to learn the name of the calling party and other helpful information. This query could come from an intermediary, or from an end user device, such as a smart phone. The value of using the PASSporT object 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 of subcase of out-of-band [I-D.rescorla-stir-fallback] use cases.

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 "cna" claim. When the terminating verification service 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 (effectively acting as an authentication service) which contains a "cna" PASSporT object provided by the third-party service. If the display name in the "cna" 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.

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 "cna" field in the object as a calling name to render to users while alerting.

5.1. Signing as a Third Party

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

A PASSporT with a "ppt" and "cna" MAY be signed with credentials that do not have authority over the identity that appears in the "orig" element of the PASSporT claims. Relying parties in STIR have always been left to make their own authorization decisions about whether or not the trust the signers of PASSporTs, and in the third-party case, where an entity has explicitly queried a service to acquire the PASSporT object, it may be some external trust or business relationship that induces the relying party to trust a PASSporT.

6. Using 'cna' in SIP

This section specifies SIP-specific usage for the "cna" claim in PASSporT, and in the SIP Identity header field value. Other using protocols of PASSporT may define their own usages for the "cna" claim.

6.1. Authentication Service Behavior

An authentication service creating a PASSporT containing a "cna" claim MAY include a "ppt" for "cna" or not. Third party authentication services as described in Section 5.1 MUST include a "ppt" of "cna". If "ppt" does contain a "cna", then any SIP authentication services MUST add a "ppt" parameter to the Identity header containing that PASSporT with a value of "cna". The resulting Identity header might look as follows:

```
Identity: "sv5CTo05KqpSmtHt3dcEiO/1CWTSZtnG3iV+1nmurLXV/HmtyNS7Ltrg9dlxkWzo
    eU7d7OV8HweTTDobV3itTmgPwCFjaEmMyEI3d7SyN21yNDo2ER/Ovgtw0Lu5csIp
    pPqOg1uXndzHbG7mR6Rl9BnUhHufVRbp51Mn3w0gfUs="; \
        info=<https://biloxi.example.org/biloxi.cer>;alg=ES256;ppt="cna"
```

This specification assumes that by default, a SIP authentication service will derive the value of "cna" from the display-name component of the From header field value of the request. It is however a matter of authentication service policy to decide how it populates the value of "cna", 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 "cna" 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.

6.2. Verification Service Behavior

[I-D.ietf-stir-rfc4474bis] Section 6.2 Step 5 requires that specifications defining "ppt" values describe any additional verifier behavior. The behavior specified for the "ppt" values of "cna" 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 "cna" 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 "cna", then the verification service MUST extract the value associated with the "cna" "nam" key in the object. If the signature validates, then the verification service can use the value of the "cna" "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.

Verification services may alter their authorization policies for the credentials accepted to sign PASSporTs when third parties generate PASSporT objects, per Section 5.1. No guidance on verification service policy is given here.

The behavior of a SIP UAS upon receiving an INVITE containing a PASSporT object with a "cna" 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.

7. Acknowledgments

We would like to thank YOU for contributions to this problem statement and framework.

8. IANA Considerations

8.1. JSON Web Token Claims

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

Claim Name: "cna"

Claim Description: Caller Name Information

Change Controller: IESG

Specification Document(s): [RFCThis]

8.2. PASSporT Types

This specification requests that the IANA add a new entry to the PASSporT Types registry for the type "cna" which is specified in [RFCThis].

8.3. PASSporT CNA Types

This document requests that the IANA create a new registry for PASSporT CNA types. Registration of new PASSporT CNA types shall be under the Specification Required policy.

This registry is to be initially populated with a single value for "nam" which is specified in [RFCThis].

9. Security Considerations

Revealing information such as the name, location, and affiliation of a person necessarily entails certain privacy risks. Baseline PASSporT has no particular confidentiality requirement, as the information it signs over in a using protocol like SIP is all information that SIP carries in the clear anyway. Transport-level security can hide those SIP fields from eavesdroppers, and the same confidentiality mechanisms would protect any PASSporT(s) carried in SIP.

More TBD.

10. Informative References

[I-D.ietf-stir-passport]
Wendt, C. and J. Peterson, "Personal Assertion Token (PASSporT)", draft-ietf-stir-passport-11 (work in progress), February 2017.

[I-D.ietf-stir-rfc4474bis]
Peterson, J., Jennings, C., Rescorla, E., and C. Wendt, "Authenticated Identity Management in the Session Initiation Protocol (SIP)", draft-ietf-stir-rfc4474bis-16 (work in progress), February 2017.

[I-D.rescorla-stir-fallback]
Rescorla, E. and J. Peterson, "STIR Out of Band Architecture and Use Cases", draft-rescorla-stir-fallback-01 (work in progress), October 2016.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://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, <http://www.rfc-editor.org/info/rfc3261>.

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

[RFC7340] Peterson, J., Schulzrinne, H., and H. Tschofenig, "Secure Telephone Identity Problem Statement and Requirements", RFC 7340, DOI 10.17487/RFC7340, September 2014, <http://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, <http://www.rfc-editor.org/info/rfc7519>.

Authors' Addresses

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

Email: jon.peterson@neustar.biz

Chris Wendt
Comcast
One Comcast Center
Philadelphia, PA 19103
USA

Email: chris-ietf@chriswendt.net