Network Working Group
Internet-Draft
Updates: RFC8224 (if approved)
Intended status: Standards Track
Expires: April 25, 2019

J. Peterson
Neustar

October 22, 2018

PASSporT Extension for Diverted Calls
draft-ietf-stir-passport-divert-04.txt

Abstract

This document extends PASSporT, which conveys cryptographically-signed information about the people involved in personal communications, to include an indication that a call has been diverted from its original destination to a new one. This information can greatly improve the decisions made by verification services in call forwarding scenarios. Also specified here is an encapsulation mechanism for nesting a PASSporT within another PASSporT that assists relying parties in some diversion scenarios.

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 April 25, 2019.

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 with STIR [RFC8224] to convey a signed assertion of the identity of the participants in real-time communications established via a protocol like SIP. This specification extends PASSporT to include an indication that a call has been diverted from its originally destination to a new one.

Although the STIR problem statement [RFC7340] is focused on preventing the impersonation of the caller's identity, which is a common enabler for threats such as robocalling and voicemail hacking on the telephone network today, it also provides a signature over the called number as the authentication service sees it. As [RFC8224] Section 12.1 describes, this protection over the contents of the To header field is intended to prevent a class of cut-and-paste attacks. If Alice calls Bob, for example, Bob might attempt to cut-and-paste the Identity header field in Alice's INVITE into a new INVITE that Bob sends to Carol, and thus be able to fool Carol into thinking the call came from Alice and not Bob. With the signature over the To header field value, the INVITE Carol sees will clearly have been

destined originally for Bob, and thus Carol can view the INVITE as suspect.

However, as [RFC8224] Section 12.1.1 points out, it is difficult for Carol to confirm or reject these suspicions based on the information she receives from the baseline PASSporT object. The common "call forwarding" service serves as a good example of the fact that the original called party number is not always the number to which a call is delivered. The address in the To header field value of SIP requests is not supposed to change, accordingly to baseline [RFC3261], as it is the Request-URI that is supposed to be updated when a call is retargeted, but practically speaking some operational environments do alter the To header field. There are a number of potential ways for intermediaries to indicate that such a forwarding operating has taken place. The History-Info header field [RFC7044] was created to store the Request-URIs that are discarded by a call in transit. The SIP Diversion header field [RFC5806], though historic, is still used for this purpose by some operators today. Neither of these header fields provide any cryptographic assurance of secure redirection, and they can both capture minor syntactical changes in URIs that do not reflect a change to the actual target of a call.

This specification therefore extends PASSporT with an explicit indication that the original called number in PASSporT no longer reflects the destination to which a call is likely to be delivered. Verification services and the relying parties who make authorization decisions about communications may use this indication to confirm that a legitimate retargeting of the call has taken place, rather than a cut-and-paste attack. In support of this goal, this specification also defines a nesting mechanism for PASSporTs that allows the original unmodified PASSporT to be conveyed to relying parties.

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].

3. PASSporT 'div' Claim

This specification defines a new JSON Web Token claim for "div" which indicates a previous destination for a call during its routing process. When a retargeting entity receives a call signed with a PASSporT, it may act as an authentication service and create a new PASSporT containing the "div" claim to attach to the call. Note that a new PASSporT is only necessary when the canonical form of the

"dest" identifier (per the canonicalization procedures in [RFC8224] Section 8) changes due to this retargeting. "div" is populated with a destination address found in the "dest" field of PASSporT received by the retargeting entity as well as a copy of the original PASSporT. These new PASSporTs generated by retargeting entities MUST include the "div" PASSporT type, and an "x5u" field pointing to a credential that the retargeting entity controls. The new PASSporT header will look as follows:

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

A PASSporT claims object containing "div" is populated with a modification of the original token before the call was retargeted: at a high level, the original identifier for the called party in the "dest" array will become the "div" claim in the new PASSporT. If the "dest" array of the original PASSporT contains multiple identifiers, the retargeting entity MUST select only one them to occupy the "div" field in the new PASSporT, and in particular, it MUST select an identifier that is within the scope of the credential that the retargeting entity will specify in the "x5u" of the PASSporT header (as described below).

The new target for the call selected by the retargeting entity becomes the value of the "dest" array of the new PASSporT. The "orig" value MUST be copied into the new PASSporT from the original PASSporT received by the retargeting entity. The retargeting entity SHOULD retain the "iat" value from the original PASSporT, though if in the underlying signaling protocol (e.g. SIP) the retargeting entity changes the date and time information in the retargeted request, the new PASSporT should instead reflect that date and time. "opt" (see Section 5) contains the full form of the original PASSporT from which the "div" was generated. No other extension claims should be copied from the original PASSporT to the "div" PASSporT.

So, for an original PASSporT of the form:

```
   { "orig":{"tn":"12155551212"},
     "dest":{"tn":"12155551213"},
     "iat":1443208345 }
```

If the retargeting entity is changing the target from 12155551213 to 12155551214, the new PASSporT with "div" would look as follows:

```
{ "orig":{"tn":"12155551212"},
  "dest":{"tn":"12155551214"},
  "iat":1443208345,
  "div":{"tn":"121555551213"},
  "opt":"eyJ0eXAiOiJwYXNzcG9ydCIsInBwdCI6ImRpdiIsImFsZyI6IkVT \
      MjU2IiwieDV1IjoiaHR0cHM6Ly93d3cuZXhhbXBsZS5jb20vY2VydC5wa3g \
      ifQ==.eyJvcmlnIjp7InRuIjoiMTIxNTU1NTEyMTIifSwiZGVzdCI6eyJ0b \
      iI6IjEyMTU1NTUxMjEzIn0sImlhdCI6MTQ0MzIwODM0NX0=.rq3pjT1hoRw \
      akEGjHCnWSwUnshd0-zJ6F1VOgFWSjHBr8Qjpjlk-cpFYpFYsojNCpTzO3Q \
      fPOlckGaS6hEck7w"} }
```

Note that the "div" claim may contain other elements than just a destination, including a History-Info indicator (see Section 7). After the PASSporT header and claims have been constructed, their signature is generated per the guidance in [RFC8225] - except for the credential required to sign it. While in the ordinary construction of a PASSporT, the credential used to sign will have authority over the identity in the "orig" claim (for example, a certificate with authority over the telephone number in "orig" per [RFC8226]), for all PASSporTs using the "div" type the signature MUST be created with a credential with authority over the identity present in the "div" claim. So for the example above, where the original "dest" is "12155551213", the signer of the new PASSporT object MUST have authority over that telephone number, and need not have any authority over the telephone number present in the "orig" claim.

Instead of having multiple unlinked PASSporTs associated with a single call, it is helpful to relying parties to nest diversion PASSporTs, explicitly relating the original PASSporT to the diverted one. Note that the approach of having multiple Identity headers in a SIP request was considered in prior versions of this specification, but it could be confusing for some verification services. The "opt" extension is REQUIRED for use within in-band SIP use cases as well as out-of-band [I-D.ietf-stir-oob] scenarios. Nested PASSporTs could result in lengthy Identity headers, and some operational experience is needed to ascertain how resilient legacy implementations will be to large headers.

4. Using 'div' in SIP

This section specifies SIP-specific usage for the "div" PASSporT type and its handling in the SIP Identity header field "ppt" parameter value. Other using protocols of PASSporT may define behavior specific to their use of the "div" claim.

4.1. Authentication Service Behavior

An authentication service only adds an Identity header field value containing the "div" PASSporT type to a SIP request that already contains at least one Identity header field value; it MUST NOT add a "div" PASSporT to an INVITE that contains no Identity headers field. As the authentication service will be adding a new PASSporT that contains an encapsulation of the original, it SHOULD remove the original request's Identity header field value before forwarding. Note that a request may contain multiple Identity header field values generated by different authorities; as a consequence, the retargeting authentication service may need to perform this operation on multiple existing PASSporTs, adding a "div" PASSporT per PASSporT in the original. When adding an Identity header field with a PASSporT object containing a "div" claim, SIP authentication services MUST also add a "ppt" parameter to that Identity header with a value of "div". The resulting full form Identity header field to add to the message might look as follows:

```
   Identity: eyJhbGciOiJFUzI1NiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cHM6Ly9
\

jZXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LmNlciJ9.eyJvcmlnIjp7InRuIjoiMTIxNTU1NTE \

yMTIifSwiZGVzdCI6eyJ0biI6IjEyMTU1NTUxMjE0In0sImlhdCI6MTQ0MzIwODM0NSwiZGl2 \

Ijp7InRuIjoiMTIxNTU1NTUxMjEzIn0sIm9wdCI6ImV5SjBlWEFpT2lKd1lYTnpjRzl5ZENJc \

0luQndkQ0k2SW1ScGRpSXNJbUZzWnlJNklrVlRNalUySWl3aWVEVjFJam9pYUhSMGNITTZMeT \

kzZDNjdVpYaGhiWEJzWlM1amIyMHZZMlZ5ZEM1d2EzZ2lmUT09LmV5SnZjbWxuSWpwN0luUnV \

Jam9pTVRJeE5UVTFOVEV5TVRJaWZTd2laR1Z6ZENJNmV5SjBiaUk2SWpFeU1UVTFOVFV4TWpF \

ekluMHNJbWxoZENJNk1UUTBNekl3T0RNME5YMD0ucnEzcGpUMWhvUndha0VHakhDbldTd1Vuc \

2hkMC16SjZGMVZPZ0ZXU2pIQnI4UWpwamxrLWNwRllwRllzb2pOQ3BUek8zUWZQT2xja0dhUz \
          ZoRWNrN3cifX0=.rq3pjT1hoRwakEGjHCnWSwUnshd0-zJ6F1VOgFWSjHBr8Qjpjlk-
cpFYpF \
          YsojNCpTzO3QfPOlckGaS6hEck7w;
      info=<https://biloxi.example.org/biloxi.cer>;alg=ES256;ppt="div"
```

A SIP authentication service typically will derive the new value of "dest" from a new Request-URI that is set for the SIP request before it is forwarded. Older values of the Request-URI may appear in header fields like Diversion or History-Info; this document specifies no specific interaction between the "div" mechanism and those SIP header fields. Note as well that because PASSporT operates on canonicalized telephone numbers and normalized URIs, many smaller changes to the syntax of identifiers that might be captured by other mechanisms that record retargeting (like History-Info) will likely not require a "div" PASSporT.

4.2. 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 "div" value of "ppt" is as follows.

In order to use the "div" extension, a verification service needs to inspect any nested PASSporT objects within PASSporTs it validates, as an Identity header field value containing "div" necessarily refers to an earlier PASSporT nested. If a nested PASSporT within a "div" PASSporT contains a "dest" claim with a value not equivalent to the "div" claim in the "div" PASSporT, that "div" PASSporT SHOULD NOT be considered valid. It is possible that this nested PASSporT will also contain a "div", and that it will in turn chain to a still earlier PASSporT nested within it. Ultimately, by looking at this chain of transformations and validating the associated signatures, the verification service will be able to ascertain that the appropriate parties were responsible for the retargeting of the call to its ultimate destination; this can help the verification service to determine that the original PASSporT in the call was not simply used in a cut-and-paste attack. This will help relying parties to make any associated authorization decisions in terms of how the call will be treated - though, per [RFC8224] Section 6.2.1, that decision is a matter of local policy.

5. Definition of 'opt'

The presence of an original PASSporT claims object element, designated as "opt", signifies that a PASSporT encapsulates another entire PASSporT within it, typically a PASSporT that was transformed in some way to create the current PASSporT. Relying parties may need to consult the encapsulated PASSporT in order to validate the identity of a caller. "opt" as defined in this specification may be used by future PASSporT extensions as well as in conjunction with "div".

"opt" MUST contain a quoted base64 encoded full-form PASSporT; it MUST NOT contain a compact form PASSporT. For an example of a "div" PASSporT containing "opt," see Section 3.

6. 'div' and Redirection

The "div" mechanism exists primarily to prevent false negatives at verification services when an arriving SIP request, due to intermediary retargeting, does not appear to be intended for its eventual recipient, because its "dest" value designates a different original destination.

Any intermediary that assigns a new target to a request can, instead of retargeting and forwarding the request, instead redirect with a 3xx response code. In ordinary operations, a redirection poses no difficulties for the operations of baseline STIR: when the UAC receives the 3xx response, it will initiate a new request to the new target (typically the target carried in the Contact header field

value of the 3xx), and the "dest" of the PASSporT created for the new request will match that new target. As no impersonation attack can arise from this case, it creates no new requirements for STIR.

However, some UACs record the original target of a call with mechanisms like History-Info [RFC7044] or Diversion [RFC5806], and may want to leverage STIR to demonstrate to the ultimate recipient that the call has been redirected securely: that is, that the original destination was the one that sent the redirection message that led to the recipient receiving the request. The semantics of the PASSporT necessary for that assertion are the same as those for the "div" retargeting cases above. The only wrinkle is that the PASSporT needs to be generated by the redirecting entity and sent back to the originating user agent client within the 3xx response.

This introduces more complexity than might immediately be apparent. In the first place, a 3xx response can convey multiple targets through the Contact header field value; to accommodate this, the "div" PASSporT MAY include one "dest" array value per Contact, but if the retargeting entity wants to keep the Contact list private from targets, it may need to generate one PASSporT per Contact. Bear in mind as well that the original SIP request could have carried multiple Identity header field values that had been added by different authentication services in the request path, so a redirecting entity might need to generate one nested "div" PASSporT per each PASSporT in the original request. Often this will mean just one "div" PASSporT, but for some deployment scenarios, it could require an impractical number of combinations. But in very complex call routing scenarios, attestation of source identity would only add limited value anyway.

STIR-aware intermediaries that redirect requests MAY therefore convey one or more PASSporTs in the backwards direction within Identity headers. This document consequently updates [RFC8224] to permit carrying Identity headers in SIP 300-class responses. It is left to authentication services to determine which Identity headers should be copied into any new requests resulting from the redirection, if any: use of these Identity headers by entities receiving a 3xx response is OPTIONAL.

Finally, note that if an intermediary in the response path consumes the 3xx and explores new targets itself while performing sequential forking, it will effectively retarget the call on behalf of the redirecting server, and this will create the same need for "div" PASSporTs as any other retargeted call.

7. Extending 'div' to work with Service Logic Tracking

It is anticipated that "div" may be used in concert with History-Info [RFC7044] in some deployments. It may not be clear from the "orig" and "dest" values which History-Info header a given PASSporT correlates to, especially because some of the target changes tracked by History-Info will not be reflected in a "div" PASSporT (see Section 1). Therefore an "hi" element may appear in "div" corresponding to the History-Info header field index parameter value. So for a History-Info header with an index value of "1.2.1", the claims object of the corresponding PASSporT with "div" might look like:

```
{ "orig":{"tn":"12155551212"},
  "dest":{"tn":"12155551214"},
  "iat":1443208345,
  "div":{"tn":"121555551213",
         "hi":"1.2.1"}
  "opt":[...]" }
```

Past experience has shown that there may be additional information about the motivation for retargeting that relying parties might consider when making authorization decisions about a call, see for example the "reason" associated with the SIP Diversion header field [RFC5806]. Future extensions to this specification might incorporate reasons into "div".

8. Acknowledgments

We would like to thank Eric Burger, Dave Hancock, Chris Wendt and Robert Sparks for contributions to this document.

9. IANA Considerations

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

9.1. 'div' registration

Claim Name: "div"

Claim Description: New Target of a Call

Change Controller: IESG

Specification Document(s): [RFCThis]

9.2. 'opt' registration

Claim Name: "opt"

Claim Description: Encapsulated JSON token

Change Controller: IESG

Specification Document(s): [RFCThis]

10. Security Considerations

This specification describes a security feature, and is primarily concerned with increasing security when calls are forwarded. Including information about how calls were retargeted during the routing process can allow downstream entities to infer particulars of the policies used to route calls through the network. However, including this information about forwarding is at the discretion of the retargeting entity, so if there is a requirement to keep the original called number confidential, no PASSporT should be created for that retargeting - the only consequence will be that downstream entities will be unable to correlate an incoming call with the original PASSporT without access to some prior knowledge of the policies that could have caused the retargeting.

Any extension that makes PASSporTs larger creates a potential amplification mechanism for SIP-based DDoS attacks. Since diversion PASSporTs are created as a part of normal forwarding activity, this risk arises at the discretion of the retargeting domain: simply using 3xx response redirections rather than retargeting (with supply a "div" per Section 6) mitigates the potential impact. Under unusual traffic loads, even domains that might ordinarily retarget requests can switch to redirection.

11. References

11.1. Normative 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>.

[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>.

[RFC7044] Barnes, M., Audet, F., Schubert, S., van Elburg, J., and C. Holmberg, "An Extension to the Session Initiation Protocol (SIP) for Request History Information", RFC 7044, DOI 10.17487/RFC7044, February 2014, <https://www.rfc-editor.org/info/rfc7044>.

[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>.

11.2. Informative References

[I-D.ietf-stir-oob] Rescorla, E. and J. Peterson, "STIR Out-of-Band Architecture and Use Cases", draft-ietf-stir-oob-03 (work in progress), July 2018.

[RFC5806] Levy, S. and M. Mohali, Ed., "Diversion Indication in SIP", RFC 5806, DOI 10.17487/RFC5806, March 2010, <https://www.rfc-editor.org/info/rfc5806>.

[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>.

Author's Address

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

Email: jon.peterson@team.neustar