STIR
Internet-Draft
Intended status: Standards Track
Expires: November 25, 2018

R. Singh
Vencore Labs
M. Dolly
AT&T
S. Das
Vencore Labs
A. Nguyen
Office of Emergency Communication/DHS

May 24, 2018

PASSporT Extension for Resource Priority Authorization
draft-ietf-stir-rph-06

Abstract

This document extends the PASSporT (Personal Assertion Token) 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, which is used for communications resource prioritization.

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 November 25, 2018.

Copyright Notice

Table of Contents

1. Introduction

PASSporT [RFC8225] is a token format based on JSON Web Token (JWT) [RFC7519] for conveying cryptographically signed information about the identities involved in personal communications. PASSporT with STIR [RFC8224] provides a mechanism by which an authority on the originating side of a call via a protocol like SIP [RFC3261] can provide a cryptographic assurance of the validity of the calling party telephone number in order to prevent impersonation attacks.

[RFC4412] defines the 'SIP Resource-Priority' header field for communications 'Resource-Priority'. As specified in [RFC4412], the 'SIP Resource-Priority' header field may be used by SIP user agents [RFC3261] (including Public Switched Telephone Network (PSTN) gateways and SIP proxy servers) to influence prioritization afforded to communication sessions including PSTN calls (e.g., to manage scarce network resources during network congestion scenarios). However, the 'SIP Resource-Priority' header field could be spoofed and abused by unauthorized entities, the threat models and use cases of which are described in [RFC7375] and [RFC7340], respectively.

Compromise of the 'SIP Resource-Priority' header field [RFC4412] could lead to misuse of network resource (i.e., during congestion scenarios) resulting in impacts to the application services supported using the 'SIP Resource-Priority' header field.

[RFC8225] allows extensions by which an authority on the originating side verifying the authorization of a particular communication for 'SIP Resource-Priority' can use a PASSPorT claim to cryptographically sign the 'SIP Resource-Priority' header field and convey assertion of the authorization for 'Resource-Priority'. Signed 'SIP Resource-Priority' header field will allow a receiving entity (including entities located in different network domains/boundaries) to verify the validity of assertions authorizing 'Resource-Priority' and to act on the information with confidence that the information has not been spoofed or compromised.

This specification documents an extension to PASSporT and the associated STIR mechanisms to provide a function to cryptographically sign the 'SIP Resource-Priority' header field. This PASSporT object is used to provide attestation of a calling user authorization for priority communications. This is necessary in addition to the PASSporT object that is used for calling user telephone number attestation. How this extension to PASSporT is used for real-time communications supported using 'SIP Resource-Priority' header field is outside the scope of this document. In addition, the PASSPorT extension defined in this document is intended for use in environments where there are means to verify that the signer of the 'SIP Resource-Priority' header field is authoritative.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119] and in RFC 8174 [RFC8174].

3. PASSporT 'rph' Claim

This specification defines a new JSON Web Token claim for "rph", which provides an assertion for information in 'SIP Resource-Priority' header field.

The creator of a PASSporT object adds a "ppt" value of "rph" to the header of a PASSporT object, in which case the PASSporT claims MUST contain a "rph" 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":"rph",
  "alg":"ES256",
  "x5u":"https://www.example.org/cert.cer"
}
```

The "rph" claim will provide an assertion of authorization, "auth", for information in the 'SIP Resource-Priority' header field based on [RFC4412] and the syntax is:

```
{
Resource-Priority = "Resource-Priority" : r-value,
r-value= namespace  "."  r-priority
}
```

Specifically, the "rph" claim includes an assertion of the priority-level of the user to be used for a given communication session. The value of the "rph" claim is an Object with one or more keys. Each key is associated with a JSON Array. These arrays contain Strings that correspond to the r-values indicated in the 'SIP Resource-Priority' header field.

The following is an example "rph" claim for a 'SIP Resource-Priority' header field with one r-value of "ets.0" and with another r-value of "wps.0":

```
 {
  "orig":{"tn":"12155550112"},
  "dest":{["tn":"12125550113"]},
  "iat":1443208345,
  "rph":{"auth":["ets.0", "wps.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, intermediaries must generate a new "rph" header and sign the claim with its own authority.

The use of the compact form of PASSporT is not specified in this document.

4. ’rph’ in SIP

This section specifies SIP-specific usage for the "rph" claim in PASSporT.

4.1. Authentication Service Behavior

The Authentication Service will create the "rph" claim using the values discussed in section 3 of this document that are based on [RFC4412]. The construction of "rph" claim follows the steps described in Section 4.1 of [RFC8224].

The resulting Identity header for "rph" might look as follows(backslashes shown for line folding only):

```
Identity:eyJhbGciOiJFUzI1NiIsInBwdCI6InJwaCIsInR5cCI6InBhc3Nwb3J0\
IiwieDV1IjoiaHR0cHM6Ly93d3cuZXhhbXBsZS5jb20vY2VydC5jZXIifQo.eyJkZ\
XN0Ijp7WyJ0biI6IjEyMTI1NTUwMTEzIl19LCJpYXQiOiIxNDQzMjA4MzQ1Iiwib3\
JpZyI6eyJ0biI6IjEyMTU1NTUwMTEyIn0sInJwaCI6eyJhdXRoIjpbImV0cy4wIiw\
id3BzLjAiXX19Cg.s37S6VC8HM6Dl6YzJeQDsrZcwJ0lizxhUrA7f_98oWBHvo-cl\
-n8MIhoCr18vYYFy3blXvs3fslM_oos2P2Dyw;info=<https://www.example.\
org/cert.cer>;alg=ES256;ppt="rph"
```

A SIP authentication service will derive the value of "rph" from the ’SIP Resource-Priority’ header field based on policy associated with service specific use of the "namespace "." r-priority" for r-values based on [RFC4412]. The authentication service derives the value of the PASSPorT claim by verifying the authorization for ’SIP Resource-Priority’ (i.e., verifying a calling user privilege for ’Resource-Priority’ based on its identity) which might be derived from customer profile data or from access to external services.

[RFC4412] allows multiple "namespace "." priority value" pairs, either in a single ’SIP Resource-Priority’ header field or across multiple ’SIP Resource-Priority’ headers. An authority is responsible for signing all the content of a ’SIP Resource-Priority’ header field for which it has the authority.

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 "ppt" values of "rph" is as follows:

The verification service MUST extract the value associated with the "auth" key in a full form PASSPorT with a "ppt" value of "rph". If the signature validates, then the verification service can use the value of the "rph" claim as validation that the calling party is

authorized for ’SIP Resource-Priority’ as indicated in the claim. This value would in turn be used for priority treatment in accordance with local policy for the associated communication service. If the signature validation fails, the verification service should infer that the calling party is not authorized for ’SIP Resource-Priority’ as indicated in the claim. In such cases, the priority treatment for the associated communication service is handled as per the local policy of the verifier. In such scenarios, ’SIP Resource-Priority’ header field SHOULD be stripped from SIP request and the network entities should treat the call as an ordinary call.

In addition, [RFC8224] Section 6.2 Step 4 requires the "iat" value in "rph" claim to be verified.

The behavior of a SIP UA upon receiving an INVITE containing a PASSporT object with a "rph" claim will largely remain a matter of implementation policy for the specific communication service. In most cases, implementations would act based on confidence in the veracity of this information.

5. Further Information Associated with ’Resource-Priority’

There may be additional information about the calling party or the call that could be relevant to authorization for ’SIP Resource-Priority’. This may include information related to the device subscription of the caller, or to any institutions that the caller or device is associated with, or even categories of institutions. All of these data elements would benefit from the secure attestations provided by the STIR and PASSporT frameworks. The specification of the "rph" claim could entail the optional presence of one or more such additional information fields applicable to ’SIP Resource-Priority’.

A new IANA registry has been defined to hold potential values of the "rph" array; see Section 6.2. The definition of the "rph" claim may have one or more such additional information field(s). Details of such "rph" claim to encompass other data elements are left for future version of this specification.

6. IANA Considerations

6.1. 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: "rph"

- o Claim Description: Resource Priority Header Authorization
- o Change Controller: IESG
- o Specification Document(s): Section 3 of [RFCThis]

6.2. PASSporT Types

This specification also requests that the IANA creates a new entry to the PASSporT Types registry for the type "rph" which is specified in [RFCThis]. In addition, another registry needs to be created in which each entry must contain two fields: the name of the "rph" type and the specification in which the type is described. This registry is to be initially populated with a single value for "auth" which is specified in [RFCThis]. Registration of new "rph" types shall be under the specification required policy.

7. Security Considerations

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

7.1. Avoidance of replay and cut and paste attacks

The PASSporT extension with a "ppt" value of "rph" MUST only be sent with SIP INVITE when ’Resource-Priority’ header field is used to convey the priority of the communication as defined in [RFC4412]. To avoid replay, and cut and paste attacks, the recommendations provided in Section 12.1 of [RFC8224] MUST be followed.

7.2. Solution Considerations

Using extensions to PASSporT tokens with a "ppt" value of "rph" requires knowledge of the authentication, authorization, and reputation of the signer to attest to the identity being asserted, including validating the digital signature and the associated certificate chain to a trust anchor. The following considerations should be recognized when using PASSporT extensions with a "ppt" value of "rph":

- o A signer is only allowed to sign the content of a ’SIP Resource-Priority’ header field for which it has the proper authorization. Before signing tokens, the signer MUST have a secure method for authentication of the end user or the device being granted a token.

- The verification of the signature MUST include means of verifying that the signer is authoritative for the signed content of the resource priority namespace in the PASSporT.

7.3. Acknowledgements

We would like to thank STIR WG members, ATIS/SIP Forum Task Force on IPNNI members, and the NS/EP Priority Services community for contributions to this problem statement and specification. We would also like to thank David Hancock and Ning Zhang for their valuable inputs.

8. References

8.1. 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, <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>.

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

[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>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <http://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, <http://www.rfc-editor.org/info/rfc8224>.

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

8.2. Informative References

[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>.

[RFC7375] Peterson, J., "Secure Telephone Identity Threat Model", RFC 7375, DOI 10.17487/RFC7375, October 2014, <http://www.rfc-editor.org/info/rfc7375>.

Authors' Addresses

Ray P. Singh
Vencore Labs
150 Mount Airy Road
New Jersey, NJ 07920
USA

Email: rsingh@vencorelabs.com

Martin Dolly
AT&T
200 Laurel Avenue
Middletown, NJ 07748
USA

Email: md3135@att.com

Subir Das
Vencore Labs
150 Mount Airy Road
New Jersey, NJ 07920
USA

Email: sdas@vencorelabs.com

An Nguyen
Office of Emergency Communication/DHS
245 Murray Lane, Building 410
Washington, DC 20528
USA

Email: an.p.nguyen@HQ.DHS.GOV