STIR
Internet-Draft
Intended status: Standards Track
Expires: July 8, 2018

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

January 04, 2018

PASSporT Extension for Resource-Priority Authorization
draft-ietf-stir-rph-02

Abstract

This document extends the STIR PASSporT specification to allow the inclusion of cryptographically-signed assertions of authorization for the values populated in the 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 July 8, 2018.

Copyright Notice

Table of Contents

1. Introduction 2
2. Terminology 3
3. PASSporT 'rph' Claim 3
4. 'rph' in SIP 4
4.1. Authentication Service Behavior 4
4.2. Verification Service Behavior 5
5. Further Information Associated with Resource-Priority 6
6. IANA Considerations 6
6.1. JSON Web Token Claims Registration 6
6.2. PASSporT 'rph' Types 6
7. Security Considerations 7
7.1. Avoidance of replay and cut and paste attacks 7
7.2. Solution Considerations 7
7.3. Acknowledgements 7
8. References 7
8.1. Normative References 7
8.2. Informative References 8
Authors' Addresses 8

1. Introduction

PASSporT [I-D.ietf-stir-passport] is a token format based on JWT [RFC7519] for conveying cryptographically-signed information about the identities 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. This specification extends PASSporT to allow cryptographic-signing of the SIP 'Resource-Priority' header field defined in [RFC4412].

[RFC4412] defines the SIP 'Resource-Priority' header field for communications Resource Priority. As specified in [RFC4412], the 'Resource-Priority' header field may be used by SIP user agents [RFC3261], including, Public Switched Telephone Network (PSTN) gateways and terminals, and SIP proxy servers to influence prioritization afforded to communication sessions,including PSTN calls. However, the SIP 'Resource-Priority' header field could be spoofed and abused by unauthorized entities.

The STIR architecture [RFC7340]assumes that an authority on the originating side of a call provides a cryptographic assurance of the

validity of the calling party number in order to prevent impersonation attacks. The STIR architecture allows extension that can be utilized by authorities supporting real-time communication services using the 'Resource-Priority' header field to cryptographically sign the SIP 'Resource-Priority' header field and convey assertion of the authorization for 'Resource-Priority'. For example, the authority on the originating side verifying the authorization of a particular communication for Resource-Priority can use a PASSPorT claim to cryptographically-sign the SIP 'Resource-Priority' header field and convey an assertion of the authorization for 'Resource-Priority'. This will allow a receiving entity (including entities located in different network domains/boundaries) to verify the validity of assertions authorizing Resource-Priority. Cryptographically-signed SIP 'Resource-Priority' headers will allow a receiving entity to verify and act on the information with confidence that the information have not been spoofed or compromised.

This specification documents an optional extension to PASSporT and the associated STIR mechanisms to provide a function to 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 the optional extension to PASSporT is used for real-time communications supported using SIP 'Resource-Priority' header field is defined in other documents and is outside the scope of this document.

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].

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.

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 (i.e., Resource-Priority: namespace "." r-priority) based on [RFC4412]. Specifically, the "rph" claim includes assertion of the priority-level of the user to be used for a given communication session. The value of the "rph" claim is an array containing one or more of JSON objects for the content of the SIP ’Resource-Priority’ header that is being asserted of which one of the "rph" object, is mandatory.

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

```
 { "orig":{"tn":"12155551212"}
  "dest":{["tn":"12125551213"]},
  "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 [I-D.ietf-stir-passport] using the full form of PASSPorT. The credentials (e.g., authority responsible for authorizing Resource-Priority) used to create the signature must have authority over the "rph" claim and there is only one authority per claim. The authority MUST use its credentials (i.e., CERT) associated with the specific service supported by the SIP namespace in the claim.

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 based on [RFC4412]. The construction of "rph" claim follows the steps described in Section 4 of [I-D.ietf-stir-rfc4474bis].

The resulting Identity header for "rph" might look as follows:

"eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJleUowZVhBaU9pSnd
ZWE56Y0c5eWRDSXNEUW9pY0hCMElqb2ljbkJvSWl3TkNpSmhiR2NpT2lKRlV6STFO
aUlzRFFvaWVEVjFJanBvZEhSd2N6b3ZMM2QzZHk1bGVHRnRjR3hsTG1OdmJTOWpaW
EowTG1ObGNuME5DZzBLIHx84oCZLuKAmXx8IGV5QWliM0pwWnlJNmV5SjBiaUk2SW
pFeU1UVTFOVFV4TWpFeUluME5DaUprWlhOMElqcDdXeUowYmlJNklqRXlNVEkxTlR
VeE1qRXpJbDE5TEEwS0ltbGhkQ0k2TVRRME16SXdPRE0wTlN3TkNpSnljR2dpT25z
aVlYVjBhQ0k2V3lKbGRITXVNQ0lzSW5kd2N5NHdJbDE5RFFvPSJ9.s37S6VC8HM6D
l6YzJeQDsrZcwJ0lizxhUrA7f_98oWBHvo-cl-n8MIhoCr18vYYFy3blXvs3fslM_
oos2P2Dyw"; info= "https://www.example.org/cert.cer";alg=ES256;
ppt="rph"

A SIP authentication service typically will derive the value of "rph" from the ’Resource-Priority’ header field based on policy associated with service specific use of the "namespace "." r-priority" values based on [RFC4412]. The authentication service derives the value of the PASSPorT claim by verifying the authorization for 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 "." r-priority" pairs, either in a single SIP Resource-Priority header or across multiple SIP Resource-Priority headers. However, it is not necessary to sign all content of a SIP Resource-Priority header or all SIP Resource-Priority headers in a given SIP message. An authority is only responsible for signing the content of a SIP Resource-Priority header for which it has authority (e.g., a specific "namespace "." r-priority").

4.2. 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 "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 Resource-Priority, which would in turn be used for priority treatment in accordance with local policy for the associated communication service.

In addition, [I-D.ietf-stir-rfc4474bis] Section 6.2 Step 4 requires "iat" value in "rph" claim to be verified.

The behavior of a SIP UAs 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. The use of the compact form of PASSporT is not specified in this document.

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 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.

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 Registration

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

6.2. PASSporT ’rph’ Types

This document requests that the IANA add a new entry to the PASSporT Types registry for the type "rph" which is specified in [RFCThis]. This specification also requests that the IANA create a new registry for PASSporT "rph" types. Registration of new PASSporT "rph" types shall be under the specification required policy. This registry is to be initially populated with a single value for "auth" which is specified in [RFCThis].

7. Security Considerations

The security considerations discussed in [I-D.ietf-stir-rfc4474bis] in Section 10 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 is used to convey the priority of the communication as defined in [RFC4412]. To avoid the replay, and cut and paste attacks, the procedures described in Section 10.1 of [I-D.ietf-stir-rfc4474bis] MUST be followed.

7.2. Solution Considerations

The use of extension to PASSporT tokens with "ppt" value "rph" based on the validation of the digital signature and the associated certificate requires consideration of the authentication and authority or reputation of the signer to attest to the identity being asserted. The following considerations should be recognized when using PASSporT extension with "ppt" value of "rph":

- An authority (signer) is only allowed to sign the content of a SIP 'Resource-Priority' header for which it has the right authority. The authority that signs the token MUST have a secure method for authentication of the end user or the device.

- The verification of the signature MUST include means of verifying that the signer is authoritative for the signed content of the SIP 'Resource-Priority' header.

7.3. Acknowledgements

We would like to thank STIR 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 for his valuable inputs.

8. References

8.1. Normative References

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

[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>.

[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>.

8.2. Informative References

[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>.

[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>.

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