Internet Engineering Task Force (IETF)
Request for Comments: 8443
Category: Standards Track
ISSN: 2070-1721

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

August 2018

Personal Assertion Token (PASSporT) Extension for Resource Priority Authorization

Abstract

This document extends the Personal Assertion Token (PASSporT) specification defined in RFC 8225 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 is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8443.

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 Secure Telephone Identity Revisited (STIR) [RFC8224] provides a mechanism by which an authority on the originating side of a call, using 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 a mechanism to prioritize access to SIP-signaled resources during periods of communications resource scarcity using the SIP 'Resource-Priority' header. As specified in [RFC4412], the SIP 'Resource-Priority' header field may be used by SIP user agents (UAs) [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 resources (i.e., during congestion scenarios), impacting 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 the SIP 'Resource-Priority' header field can use a PASSPorT claim to cryptographically sign the SIP 'Resource-Priority' header field and convey assertion of the authorization for the SIP 'Resource-Priority' header field. A 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 the SIP 'Resource-Priority' header field 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 the 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", "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. PASSporT "rph" Claim

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

The creator of a PASSporT object adds a "ppt" value of "rph" to the header of a PASSporT object. The PASSporT claims MUST contain an "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]. 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, the intermediaries must generate a new "rph" header and sign the claim with their 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 the "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 r-values, defined as follows in [RFC4412]:

```
r-value = namespace "." r-priority
```

The authentication service derives the value of the PASSPorT claim by verifying the authorization for the SIP 'Resource-Priority' header field (i.e., verifying a calling-user privilege for the SIP 'Resource-Priority' header field based on its identity). The authorization might be derived from customer-profile data or 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' header fields. 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' header fields 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' header fields 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, the SIP 'Resource-Priority' header field SHOULD be stripped from the 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 an "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 the SIP 'Resource-Priority' Header Field

There may be additional information about the calling party or the call that could be relevant to authorization for the SIP 'Resource-Priority' header field. This may include information related to the device subscription of the caller, to any institutions that the caller or device is associated with, or even to 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 the SIP 'Resource-Priority' header field.

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 how an "rph" claim encompasses other data elements are left for future specifications.

6. IANA Considerations

6.1. JSON Web Token Claims

IANA has added a new claim to the "JSON Web Token Claims" registry as defined in [RFC7519].

- Claim Name: "rph"
- Claim Description: Resource Priority Header Authorization
- Change Controller: IESG
- Specification Document(s): Section 3 of RFC 8443

6.2. PASSporT Types

IANA has created a new entry in the "Personal Assertion Token (PASSporT) Extensions" registry for the type "rph", which is specified in this document. In addition, the "PASSporT Resource Priority Header (rph) Types" registry has been 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 has been initially populated with the single value for "auth", which is specified in this document. Registration of new "rph" types shall be under the Specification Required policy[RFC8126].

7. Security Considerations

The security considerations discussed in [RFC8224], 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 the SIP '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":

- 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.

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, <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>.

[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>.

[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>.

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, <https://www.rfc-editor.org/info/rfc7340>.

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

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

Acknowledgements

We would like to thank STIR Working Group members, the 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.

Authors' Addresses

Ray P. Singh
Vencore Labs
150 Mount Airy Road
New Jersey, NJ 07920
United States of America

Email: rsingh@vencorelabs.com

Martin Dolly
AT&T
200 Laurel Avenue
Middletown, NJ 07748
United States of America

Email: md3135@att.com

Subir Das
Vencore Labs
150 Mount Airy Road
New Jersey, NJ 07920
United States of America

Email: sdas@vencorelabs.com

An Nguyen
Office of Emergency Communications
Department of Homeland Security
245 Murray Lane, Building 410
Washington, DC 20528
United States of America

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