STIR
Internet-Draft
Intended status: Standards Track
Expires: November 9, 2018

T. Asveren
Ribbon

May 8, 2018

PASSPorT Extension for P-Charge-Info Header
draft-asveren-stir-p-charge-info-00

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) P-Charge-Info' header, which is used for conveying information about the entity to be charged for a particular real time session.

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 9, 2018.

Table of Contents

1. Introduction

PASSporT RFC 8225 [RFC8225] is a token format based on JSON Web Token (JWT) RFC 7519 [RFC7519] for conveying cryptographically signed information about the identities involved in personal communications; it is used with STIR RFC 8224 [RFC8224] to convey a signed assertion of the identity of the participants in real-time communications established via a protocol like SIP RFC 3261 [RFC3261]. This specification extends PASSporT to allow cryptographic-signing of the 'SIP P-Charge-Info' header [RFCXXX], which is used to provide information about the party to be charged for a real time session.

'SIP P-Charge-Info' header could be spoofed and abused by unauthorized entities. Compromise of the 'SIP P-Charge-Info' header would allow charging fraud.

Extension mechanisms defined in RFC8225 can be utilized to cyrptographically sign the 'SIP P-Charge-Info' header. This would allow a receiving entity to verify the validity of this header.

This specification documents an extension to PASSporT and the associated STIR mechanisms to provide a function to sign the 'SIP P-Charge-Info' header.

2. Requirements Language

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.

3. PASSPortT 'pci' Claim

This specification defines a new JSON Web Token claim for "pci", which provides an assertion for information in 'SIP P-Charge-Info' header.

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

The "pci" claim will provide an assertion for information in the 'SIP P-Charge-Info' header as defined in [RFCXXX] .

After the header and claims PASSporT objects have been constructed, their signature is generated normally per the guidance in [RFC8225]. The credentials (i.e., Certificate) used to create the signature must have authority over the "pci" claim and there is only one authority per claim. If P-Charge-Info header is added or by the intermediaries along the path, intermediaries must generate a new "pci" header and sign the claim with its own authority.

The following is an example "pci" claim for a 'SIP P-Charge-Info' header field with a value of "12125550100"

```
 {
  "orig":{"tn":"12155550112"},
  "dest":{["tn":"12125550113"]},
  "iat":1443208345,
  "pci":{["tn": "12125550100"]}
 }
```

4. Using 'pci' in SIP

This section specifies SIP-specific usage for the "pci" 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 "pci" claim.

4.1. Authentication Service Behavior

An authentication service adds an Identity header field containing the "pci" PASSporT type to an SIP request only if it adds a P-Charge-Info header to the request. Whether to add such an Identity header is controlled by local policy. When adding an Identity header field with a PASSporT object containing a "pci" claim, SIP authentication services MUST also add a "ppt" parameter to that Identity header with a value of "pci". The resulting Identity header field to add to the message might look as follows:

```
Identity: eyJhbGciOiJFUzI1NiIsInR5cCI6InBhc3Nwb3J0IiwieDV1I \
joiaHR0cHM6Ly9jZXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LmNlciJ9.eyJ \
kZXN0Ijp7InVyaSI6WyJzaXA6YWxpY2VAZXhhbXBsZS5jb20iXX0sImlhdC \
I6IjE0NDMyMDgzNDUiLCJvcmlnIjp7InRuIjoiMTIxNTU1NTEyMTIifX0.r \
q3pjT1hoRwakEGjHCnWSwUnshd0-zJ6F1VOgFWSjHBr8Qjpjlk-cpFYpFYs \
ojNCpTzO3QfPOlckGaS6hEck7w;info=<https://biloxi.example.org \
/biloxi.cert>;alg=ES256;ppt="pci"
```

4.2. Verification Service Behavior

RFC 8224 [RFC8224] Section 6.2 Step 5 requires that specifications defining "ppt" values describe any additional verifier behavior. The behavior specified for the "pci" value of "ppt" is as follows. The verification service MUST extract the value associated with the "pci" key in a PASSPorT with a "ppt" value of "pci". If the signature validates, then the verification service can use the value of the "pci" claim as validation that P-Charge-Info in the received request is authentic. The verifier MUST also ensure that the generator of Identity header is authorized to declare the value used for P-Charge-Info as the party to be charged. How this can be achieved is out of the scope of this specification.

4.3. Other Behavior

An entity dropping P-Charge-Info MUST drop the corresponding Identity header with "ppt" parameter value of "pci".

5. IANA Considerations

This specification requests that the IANA add a new claim to the JSON Web Token Claims registry as defined in RFC 7519 [RFC7519].

Claim Name: "pci"

Claim Description: Party to be charged for a session

Change Controller: IESG

Specification Document(s): [RFCThis]

6. Security Considerations

This specification describes a security feature, and is primarily concerned with increasing security for information regarding the party to be charged for a real time session.

A malicious entity may add a P-Charge-Info value and a corresponding Identity header for charge abuse. This would be detected either because the signature validation fails or because the malicious entity does not have authority to declare the value of P-Charge-Info as the party to be charged.

A malicious entity may drop the P-Charge-Info and the corresponding Identity header. This would cause infoirmation about the actual party to cherge not being present for a receiver entity which otherwise would use it for billing purposes. One way to avoid this type of attack would be, for example, to enforce presence of P-Charge-Info header by the billing entity and reject the session if there is none. This check may be performed only for certain sessions based on origination and/or destination identity for the call.

7. Acknowledgements

8. Informative 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>.

[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>.

[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>.

Author's Address

Tolga Asveren
Ribbon Communications
Freehold, NJ 07728
USA

Email: tasveren@rbbn.com