Internet Engineering Task Force (IETF)
Request for Comments: 8588
Category: Standards Track
ISSN: 2070-1721

C. Wendt
Comcast
M. Barnes
iconectiv

May 2019

Personal Assertion Token (PaSSporT) Extension for Signature-based Handling of Asserted information using toKENs (SHAKEN)

Abstract

This document extends the Personal Assertion Token (PASSporT), which is a token object that conveys cryptographically signed information about the participants involved in communications. The extension is defined based on the "Signature-based Handling of Asserted information using toKENs (SHAKEN)" specification by the ATIS/SIP Forum IP-NNI Task Group. It provides both (1) a specific set of levels of confidence in the correctness of the originating identity of a call originated in a SIP-based telephone network as well as (2) an identifier that allows the Service Provider (SP) to uniquely identify the origin of the call within its network.

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/rfc8588.

Table of Contents

1. Introduction 3
2. Terminology 3
3. Overview of "shaken" PASSporT Extension 4
4. PASSporT "attest" Claim 4
5. PASSporT "origid" Claim 4
6. Example "shaken" PASSporT 5
7. Using "shaken" in SIP 5
8. Order of Claim Keys 5
9. Security Considerations 6
10. Privacy Considerations 6
11. IANA Considerations 7
11.1. JSON Web Token claims 7
11.2. PASSporT Types 7
12. References 7
12.1. Normative References 7
12.2. Informative References 8
Acknowledgements 9
Authors' Addresses 9

1. Introduction

The Signature-based Handling of Asserted information using toKENs (SHAKEN) [ATIS-1000074] specification defines a framework for using Secure Telephone Identity Revisited (STIR) protocols including the Personal Assertion Token (PASSporT) [RFC8225], SIP Authenticated Identity Management [RFC8224], and the STIR certificate framework [RFC8226] for implementing the cryptographic validation of an authorized originator of telephone calls using SIP. Because the current telephone network contains traffic originated from both VoIP and TDM/SS7 (Time Division Multiplexing / Signaling System 7), there are many scenarios that need to be accounted for where PASSporT signatures may represent either direct or indirect call origination scenarios. The SHAKEN [ATIS-1000074] specification defines levels of attestation of the origination of the call as well as an origination identifier that can help create a unique association between the origin of a particular call to the point in the VoIP or TDM telephone network the call came from to identify, for example, either a customer or class of service that call represents. This document specifies these values as claims to extend the base set of PASSporT claims.

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.

In addition, the following terms are used in this document:

- Verified association: Typically defined as an authenticated relationship between a customer and a device that initiated a call on behalf of that customer, for example, a subscriber account with a specific SIM card or set of SIP credentials.

- PASSporT: Defined in [RFC8225] is a JSON Web Token [RFC7519] defined specifically for securing the identity of an initiator of personal communication. This document defines a specific extension to PASSporT.

3. Overview of "shaken" PASSporT Extension

The SHAKEN framework is designed to use PASSporT [RFC8225] as a method of asserting the caller's telephone identity. In addition to the PASSporT base claims, there are two additional claims that have been defined for the needs of a service provider to signal information beyond just the telephone identity. First, in order to help bridge the transition of the state of the current telephone network (which has calls with no authentication and non-SIP [RFC3261] signaling not compatible with the use of PASSporT and Secure Telephone Identity (STI) in general), there is an attestation claim. This provides three levels of attestation: a full attestation when the service provider can fully attest to the calling identity, a partial attestation when the service provider originated a telephone call but cannot fully attest to the calling identity, and a gateway attestation, which is the lowest level of attestation and represents the service provider receiving a call from a telephone gateway that does not support PASSporT or STI.

The second claim is a unique origination identifier that should be used by the service provider to identify different sources of telephone calls to support a traceback mechanism that can be used for enforcement and identification of a source of illegitimate calls.

The use of the compact form of PASSporT is not specified in this document and is not specified for use in SHAKEN [ATIS-1000074].

The next two sections define these new claims.

4. PASSporT "attest" Claim

This indicator allows for both identifying the service provider that is vouching for the call as well as clearly indicating what information the service provider is attesting to. The "attest" claim can be one of the following three values: 'A', 'B', or 'C'. These values correspond to 'Full Attestation', 'Partial Attestation', and 'Gateway Attestation', respectively. See [ATIS-1000074] for the definitions of these three levels of attestation.

5. PASSporT "origid" Claim

The purpose of the "origid" claim is described in [ATIS-1000074]. The value of "origid" claim is a Universally Unique Identifier (UUID) as defined in [RFC4122]. Please refer to Section 10 for a discussion of the privacy considerations around the use of this value.

6. Example "shaken" PASSporT

```
Protected Header
{
   "alg":"ES256",
   "typ":"passport",
   "ppt":"shaken",
   "x5u":"https://cert.example.org/passport.cer"
}
Payload
{
   "attest":"A"
   "dest":{"tn":["12155550131"]}
   "iat":"1443208345",
   "orig":{"tn":"12155550121"},
   "origid":"123e4567-e89b-12d3-a456-426655440000"
}
```

7. Using "shaken" in SIP

The use of the "shaken" PASSporT type and the "attest" and "origid" claims for SIP is formally defined in [ATIS-1000074] using the SIP [RFC3261] Identity header field defined in [RFC8224].

8. Order of Claim Keys

The order of the claim keys MUST follow the rules of Section 9 of [RFC8225]; the claim keys MUST appear in lexicographic order. Therefore, the claim keys discussed in this document appear in the PASSporT Payload in the following order:

- attest
- dest
- iat
- orig
- origid

9. Security Considerations

This document defines a new PASSporT [RFC8225] extension. The considerations related to the security of the PASSporT object itself are the same as those described in [RFC8225].

[RFC8224] defines how to compare the values of the "dest", "orig", and "iat" claims against fields in a SIP message containing a PASSporT as part of validating that request. The values of the new "attest" and "origid" claims added by this extension are not used in such a validation step. They are not compared to fields in the SIP message. Instead, they simply carry additional information from the signer to the consumer of the PASSporT. This new information shares the same integrity protection and non-repudiation properties as the base claims in the PASSporT.

10. Privacy Considerations

As detailed in Section 26 of [RFC3261], SIP messages inherently carry identifying information of the caller and callee. The addition of STIR cryptographically attests that the signing party vouches for the information given about the callee, as is discussed in the Privacy Considerations of [RFC8224].

SHAKEN [ATIS-1000074] furthermore adds an "origid" value to the STIR PASSporT, which is an opaque unique identifier representing an element on the path of a given SIP request. This identifier is generated by an originating telephone service provider to identify where within their network (e.g. a gateway or particular service element) a call was initiated; "origid" can facilitate forensic analysis of call origins when identifying and stopping bad actors trying to spoof identities or make fraudulent calls.

The opacity of the "origid" claim value is intended to minimize exposure of information about the origination of calls labeled with an "origid" value. It is therefore RECOMMENDED that implementations generate a unique "origid" value per call in such a way that only the generator of the "origid" can determine when two "origid" values represent the same or different elements. If deployed systems instead use a common or related "origid" for service elements in their network, the potential for discovering patterns through correlation of those calls exists. This could allow a recipient of calls to, for instance, learn that a set of callers are using a particular service or coming through a common gateway. It is expected that SHAKEN PASSporTs are shared only within an [RFC3324] trust domain and will be stripped before calls exit that trust domain, but this information still could be used by analytics on

intermediary and terminating systems to reveal information that could include geographic location and even device-level information, depending on how the "origid" is generated.

11. IANA Considerations

11.1. JSON Web Token claims

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

Claim Name: attest
Claim Description: Attestation level as defined in SHAKEN framework
Change Controller: IESG
Specification Document(s): RFC 8588

Claim Name: origid
Claim Description: Originating Identifier as defined in SHAKEN framework
Change Controller: IESG
Specification Document(s): RFC 8588

11.2. PASSporT Types

IANA has added a new entry in the "Personal Assertion Token (PASSporT) Extensions" registry for the type "shaken", which is specified in this document.

12. References

12.1. Normative References

[ATIS-1000074] ATIS/SIP Forum IP-NNI Task Group, "Signature-based Handling of Asserted information using toKENs (SHAKEN)", January 2017, <https://access.atis.org/apps/group_public/download.php/32237/ATIS-1000074.pdf>.

[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>.

[RFC4122] Leach, P., Mealling, M., and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace", RFC 4122, DOI 10.17487/RFC4122, July 2005, <https://www.rfc-editor.org/info/rfc4122>.

[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>.

[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>.

12.2. 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, <https://www.rfc-editor.org/info/rfc3261>.

[RFC3324] Watson, M., "Short Term Requirements for Network Asserted Identity", RFC 3324, DOI 10.17487/RFC3324, November 2002, <https://www.rfc-editor.org/info/rfc3324>.

Acknowledgements

The authors would like to thank those that helped review and contribute to this document including specific contributions from Jon Peterson, Russ Housley, Robert Sparks, and Andrew Jurczak. The authors would like to acknowledge the work of the ATIS/SIP Forum IP-NNI Task Force to develop the concepts behind this document.

Authors' Addresses

Chris Wendt
Comcast
One Comcast Center
Philadelphia, PA 19103
United States of America

Email: chris-ietf@chriswendt.net

Mary Barnes
iconectiv

Email: mary.ietf.barnes@gmail.com