STIR
Internet-Draft
Intended status: Standards Track
Expires: May 10, 2019

C. Wendt
Comcast
M. Barnes
iconectiv

November 06, 2018

PASSporT SHAKEN Extension (SHAKEN)
draft-ietf-stir-passport-shaken-05

Abstract

This document extends PASSporT, which is a token object that conveys cryptographically-signed information about the participants involved in communications. The extension is defined, corresponding to the SHAKEN specification, to provide both a specific set of levels-of-confidence to the correctness of the originating identity for a SIP based Communication Service Provider (CSP) telephone network originated call as well as an identifier that allows the CSP to uniquely identify the origination of the call within its network.

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 May 10, 2019.

Copyright Notice

Table of Contents

1. Introduction 2
2. Terminology 3
3. Overview of 'shaken' PASSporT extension 3
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 6
11.1. JSON Web Token claims 7
11.2. PASSporT Types 7
12. Acknowledgements 7
13. References 7
13.1. Normative References 7
13.2. Informative References 8
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 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 both VoIP and TDM/SS7 originated traffic, 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 with the origination of calls from various parts of the VoIP or TDM telephone network. 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: is typically defined as an authenticated relationship with a device that initiated a call, 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 telephone number calling 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, including 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 can not 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 non-PASSporT and non-STI supporting telephone gateway.

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' as defined in [ATIS-1000074].

'A' represents 'Full Attestation' where the signing provider MUST satisfy all of the following conditions:

- Is responsible for the origination of the call onto the IP based service provider voice network.
- Has a direct authenticated relationship with the initiator of the call and can identify the customer associated with the initiator.
- Has established a verified association with the calling party telephone number used for the call.

'B' represents 'Partial Attestation' where the signing provider MUST satisfy all of the following conditions:

- Is responsible for the origination of the call onto its IP-based voice network.
- Has a direct authenticated relationship with the initiator of the call and can identify the customer associated with the initiator.
- Has NOT established a verified association with the calling party telephone number being used for the call.

'C' represents 'Gateway Attestation' where the signing provider MUST satisfy all of the following conditions:

- Is the entry point of the call into its VoIP network.
- Has no relationship with the initiator of the call (e.g., international gateways)

5. PASSporT 'origid' Claim

The purpose of the unique origination identifier is to assign an opaque identifier corresponding to the service-provider-initiated calls themselves, customers, classes of devices, or other groupings that a service provider might want to use for determining things like reputation or trace back identification of customers or gateways. The value of 'origid' claim is a UUID as defined in [RFC4122].

SHAKEN isn't prescriptive in the exact usage of origid other than the UUID format as a globally unique identifier representing the originator of the call to whatever granularity the PASSporT signer determines is sufficient for the ability to trace the original origination point of the call.

6. Example "shaken" PASSporT

```
Protected Header
{
   "alg":"ES256",
   "typ":"passport",
   "ppt":"shaken",
   "x5u":"https://cert.example.org/passport.cer"
}
Payload
{
   "attest":"A"
   "dest":{"uri":["sip:alice@example.com"]}
   "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 claims 'attest' and 'origid' are formally defined in [ATIS-1000074] for usage in SIP [RFC3261] aligned with the use of the identity header field defined in [RFC8224].

8. Order of Claim Keys

The order of the claim keys MUST follow the rules of [RFC8225] Section 9; 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 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 [RFC3261] Section 26, SIP messages inherently carry identifying information of the caller and callee. The value of the 'origid' claim, as defined in SHAKEN [ATIS-1000074] and described in this document, is intended to be a opaque and unique identifier of an element on the path of a given request. This identifier is used by an originating telephone service provider to identify where within their network (e.g. a gateway or particular service element) a call was initiated. This facilitates identifying and stopping bad actors trying to spoof identities or make fraudulent calls. The opacity of the 'origid' claim value is intended to minimize direct exposure of information about the origination of a set of calls sharing the 'origid' value. It should be recognized, however, that the potential for discovering patterns through correlation of those calls exists. This could allow a recipient of many calls to, for instance, learn that a set of callers are using a particular service or coming through a common gateway. However, this threat already exists in SIP. There is information in the SIP messages(in the form of Record-Route, Via, and potentially History-Info header field values that can be analyzed the same way (and may correlate closely with the 'origid' value). If the operator of an element is concerned about the correlation of 'origid' values, the element could be configured to use a unique 'origid' value per call in such a way that the operator can associate those 'origid' values to the correct element when doing lookups in their backend systems.

11. IANA Considerations

11.1. JSON Web Token claims

This specification requests that the IANA add 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): [RFCThis]

Claim Name: "origid"

Claim Description: Originating Identifier as defined in SHAKEN framework

Change Controller: IESG

Specification Document(s): [RFCThis]

11.2. PASSporT Types

This specification requests that the IANA add a new entry to the Personal Assertion Token (PASSporT) Extensions registry for the type "shaken" which is specified in [RFCThis].

12. 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.

13. References

13.1. 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>.

[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>.

[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>.

13.2. 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>.

[RFC3323] Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)", RFC 3323, DOI 10.17487/RFC3323, November 2002, <https://www.rfc-editor.org/info/rfc3323>.

[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>.

Authors' Addresses

Chris Wendt
Comcast
One Comcast Center
Philadelphia, PA 19103
USA

Email: chris-ietf@chriswendt.net

Mary Barnes
iconectiv

Email: mary.ietf.barnes@gmail.com