

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 2, 2018

E. Rescorla
Mozilla
J. Peterson
Neustar
October 29, 2017

STIR Out-of-Band Architecture and Use Cases
draft-ietf-stir-oob-01.txt

Abstract

The PASSporT format defines a token that can be carried by signaling protocols, including SIP, to cryptographically attest the identity of callers. Not all telephone calls use Internet signaling protocols, however, and some calls use them for only part of their signaling path. This document describes use cases that require the delivery of PASSporT objects outside of the signaling path, and defines architectures and semantics to provide this functionality.

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 2, 2018.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must

include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	2
2. Terminology	4
3. Operating Environments	4
4. Dataflows	5
5. Use Cases	6
5.1. Case 1: VoIP to PSTN Call	6
5.2. Case 2: Two Smart PSTN endpoints	6
5.3. Case 3: PSTN to VoIP Call	7
5.4. Case 4: Gateway Out-of-band	7
6. Storing and Retrieving PASSporTs	8
6.1. Storage	9
6.2. Retrieval	10
7. Solution Architecture	11
7.1. Credentials and Phone Numbers	12
7.2. Call Flow	12
7.3. Security Analysis	13
7.4. Substitution Attacks	13
8. Call Placement Service Discovery	14
9. Credential Lookup	15
10. Acknowledgments	16
11. IANA Considerations	16
12. Security Considerations	16
13. Informative References	16
Authors' Addresses	18

1. Introduction

The STIR problem statement [RFC7340] describes widespread problems enabled by impersonation in the telephone network, including illegal robocalling, voicemail hacking, and swatting. As telephone services are increasingly migrating onto the Internet, and using Voice over IP (VoIP) protocols such as SIP [RFC3261], it is necessary for these protocols to support stronger identity mechanisms to prevent impersonation. For example, [I-D.ietf-stir-rfc4474bis] defines an Identity header of SIP requests capable of carrying a PASSporT [I-D.ietf-stir-passport] object in SIP as a means to cryptographically attest that the originator of a telephone call is authorized to use the calling party number (or, for native SIP cases, SIP URI) associated with the originator of the call. of the request.

Not all telephone calls use SIP today, however; and even those that do use SIP do not always carry SIP signaling end-to-end. Most calls

from telephone numbers still traverse the Public Switched Telephone Network (PSTN) at some point. Broadly, calls fall into one of three categories:

1. One or both of the endpoints is actually a PSTN endpoint.
2. Both of the endpoints are non-PSTN (SIP, Jingle, ...) but the call transits the PSTN at some point.
3. Non-PSTN calls which do not transit the PSTN at all (such as native SIP end-to-end calls).

The first two categories represent the majority of telephone calls associated with problems like illegal robocalling: many robocalls today originate on the Internet but terminate at PSTN endpoints. However, the core network elements that operate the PSTN are legacy devices that are unlikely to be upgradable at this point to support an in-band authentication system. As such, those devices largely cannot be modified to pass signatures originating on the Internet--or indeed any inband signaling data--intact. Even if fields for tunneling arbitrary data can be found in traditional PSTN signaling, in some cases legacy elements would strip the signatures from those fields; in others, they might damage them to the point where they cannot be verified. For those first two categories above, any in-band authentication scheme does not seem practical in the current environment.

But while the core network of the PSTN remains fixed, the endpoints of the telephone network are becoming increasingly programmable and sophisticated. Landline "plain old telephone service" deployments, especially in the developed world, are shrinking, and increasingly being replaced by three classes of intelligent devices: smart phones, IP PBXs, and terminal adapters. All three are general purpose computers, and typically all three have Internet access as well as access to the PSTN. Additionally, various kinds of gateways increasingly front for legacy equipment. All of this provides a potential avenue for building an authentication system that implements stronger identity while leaving PSTN systems intact.

This capability also provides an ideal transitional technology while in-band STIR adoption is ramping up. It permits early adopters to use the technology even when intervening network elements are not yet STIR-aware, and through various kinds of gateways it may allow providers with a significant PSTN investment to still secure their calls with STIR.

This specification therefore builds on the PASSport [I-D.ietf-stir-passport] mechanism and the work of

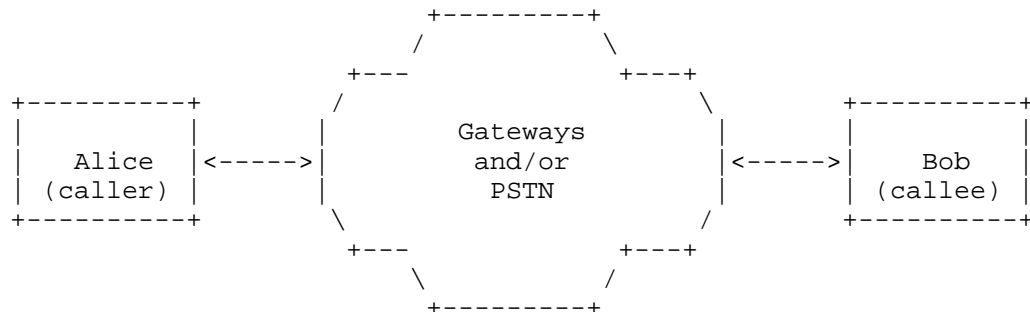
[I-D.ietf-stir-rfc4474bis] to define a way that a PASSporT object created in the originating network of a call can reach the terminating network even when it cannot be carried end-to-end in-band in the call signaling. This relies on a new service defined in this document that permits the PASSporT object to be stored during call processing and retrieved for verification purposes.

2. Terminology

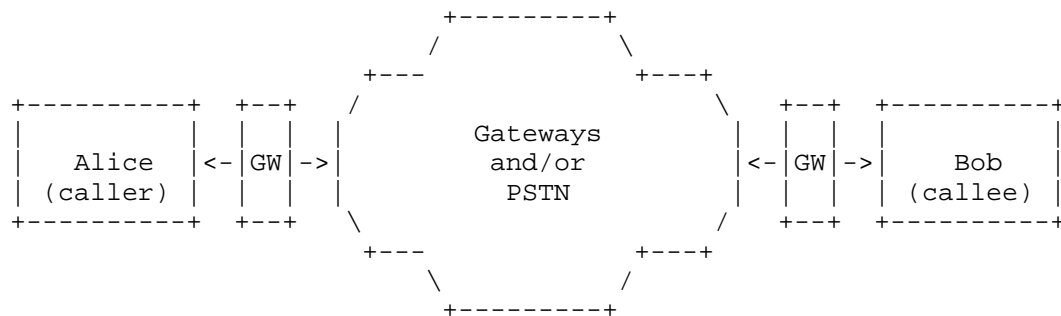
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Operating Environments

This section describes the environments in which the proposed mechanism is intended to operate. In the simplest setting, Alice is calling Bob through some set of gateways and/or the PSTN. Both Alice and Bob have smart devices which can be modified, but they do not have a clear connection between them: Alice cannot inject any data into signaling which Bob can read, with the exception of the asserted destination and origination E.164 numbers. The calling party number might originate from her own device or from the network. These numbers are effectively the only data that can be used for coordination between the endpoints.



In a more complicated setting, Alice and/or Bob may not have a smart or programmable device, but one or both of them are behind a STIR-aware gateway that can participate in out-of-band coordination, as shown below:



In such a case, Alice might have an analog connection to her gateway/switch which is responsible for her identity. Similarly, the gateway would verify Alice's identity, generate the right calling party number information and provide that number to Bob using ordinary POTS mechanisms.

4. Dataflows

Because in these operating environments endpoints cannot pass cryptographic information to one another directly through signaling, any solution must involve some rendezvous mechanism to allow endpoints to communicate. We call this rendezvous service a "call placement service" (CPS), a service where a record of call placement, in this case a PASSporT, can be stored for future retrieval. In principle this service could communicate any information, but minimally we expect it to include a full-form PASSporT that attests the caller, callee, and the time of the call. The callee can use the existence of a PASSporT for a given incoming call as rough validation of the asserted origin of that call. (See Section 9 for limitations of this design.)

There are roughly two plausible dataflow architectures for the CPS:

The callee registers with the CPS. When the caller wishes to place a call to the callee, it sends the PASSporT to the CPS, which immediately forwards it to the callee.

The caller stores the PASSporT with the CPS at the time of call placement. When the callee receives the call, it contacts the CPS and retrieves the PASSporT.

While the first architecture is roughly isomorphic to current VoIP protocols, it shares their drawbacks. Specifically, the callee must maintain a full-time connection to the CPS to serve as a notification channel. This comes with the usual networking costs to the callee and is especially problematic for mobile endpoints. Indeed, if the

endpoints had the capabilities to implement such an architecture, they could surely just use SIP or some other protocol to set up a secure session; even if the media were going through the traditional PSTN, a "shadow" SIP session could convey the PASSporT. Thus, we focus on the second architecture in which the PSTN incoming call serves as the notification channel and the callee can then contact the CPS to retrieve the PASSporT.

5. Use Cases

The following are the motivating use cases for this mechanism. Bear in mind that just as in [I-D.ietf-stir-rfc4474bis] there may be multiple Identity headers in a single SIP INVITE, so there may be multiple PASSporTs in this out-of-band mechanism associated with a single call. For example, a SIP user agent might create a PASSporT for a call with an end user credential, and as the call exits the originating administrative domain the network authentication service might create its own PASSporT for the same call. As such, these use cases may overlap in the processing of a single call.

5.1. Case 1: VoIP to PSTN Call

A call originates in the SIP world in a STIR-aware administrative domain. The local authentication service for that administrative domain creates a PASSporT which is carried in band in the call per [I-D.ietf-stir-rfc4474bis]. The call is routed out of the originating administrative domain and reaches a gateway to the PSTN. Eventually, the call will terminate on a mobile smartphone that supports this out-of-band mechanism.

In this use case, the originating authentication service can store the PASSporT with the appropriate CPS for the target telephone number as a fallback in case SIP signaling will not reach end-to-end. When the destination mobile smartphone receives the call over the PSTN, it consults the CPS and discovers a PASSporT from the originating telephone number waiting for it. It uses this PASSporT to verify the calling party number.

5.2. Case 2: Two Smart PSTN endpoints

A call originates with an enterprise PBX that has both Internet access and a built-in gateway to the PSTN. It will immediately drop its call to the PSTN, but before it does, it provisions a PASSporT on the CPS associated with the target telephone number.

After normal PSTN routing, the call lands on a smart mobile handset that supports the STIR out-of-band mechanism. It queries the appropriate CPS over the Internet to determine if a call has been

placed to it by a STIR-aware device. It finds the PASSporT provisioned by the enterprise PBX and uses it to verify the calling party number.

5.3. Case 3: PSTN to VoIP Call

A call originates with an enterprise PBX that has both Internet access and a built-in gateway to the PSTN. It will immediately drop the call to the PSTN, but before it does, it provisions a PASSporT with the CPS associated with the target telephone number. However, it turns out that the call will eventually route through the PSTN to an Internet gateway, which will translate this into a SIP call and deliver it to an administrative domain with a STIR verification service.

In this case, there are two subcases for how the PASSporT might be retrieved. In subcase 1, the Internet gateway that receives the call from the PSTN could query the appropriate CPS to determine if the original caller created and provisioned a PASSporT for this call. If so, it can retrieve the PASSporT and, when it creates a SIP INVITE for this call, add a corresponding Identity header per [I-D.ietf-stir-rfc4474bis]. When the SIP INVITE reaches the destination administrative domain, it will be able to verify the PASSporT normally. Note that to avoid discrepancies with the Date header field value, only full-form PASSporT should be used for this purpose. In subcase 2, the gateway does not retrieve the PASSporT itself, but instead the verification service at the destination administrative domain does so. Subcase 1 would perhaps be valuable for deployments where the destination administrative domain supports in-band STIR but not out-of-band STIR.

5.4. Case 4: Gateway Out-of-band

A call originates in the SIP world in a STIR-aware administrative domain. The local authentication service for that administrative domain creates a PASSporT which is carried in band in the call per [I-D.ietf-stir-rfc4474bis]. The call is routed out of the originating administrative domain and eventually reaches a gateway to the PSTN.

In this case, the originating authentication service does not support the out-of-band mechanism, so instead the gateway to the PSTN extracts the PASSporT from the SIP request and provisions it to the CPS. (When the call reaches the gateway to the PSTN, the gateway might first check the CPS to see if a PASSporT object had already been provisioned for this call, and only provision a PASSporT if none is present).

Ultimately, the call may terminate on the PSTN, or be routed back to the IP world. In the former case, perhaps the destination endpoints queries the CPS to retrieve the PASSporT provisioned by the first gateway. Or if the call ultimately returns to the IP world, it might be the gateway from the PSTN back to the Internet that retrieves the PASSporT from the CPS and attaches it to the new SIP INVITE it creates, or it might be the terminating administrative domain's verification service that checks the CPS when an INVITE arrives with no Identity header field. Either way the PASSporT can survive the gap in SIP coverage caused by the PSTN leg of the call.

6. Storing and Retrieving PASSporTs

The use cases show a variety of entities accessing the CPS to store and retrieve PASSporTs. The question of how the CPS authorizes the storage and retrieval of PASSporT is thus a key design decision in the architecture. Broadly, the architecture described here is one focused on permitting any entity to store encrypted PASSporTs at the CPS, indexed under the caller number. PASSporTs will be encrypted with associated with the called number, so these PASSporTs may also be retrieved by any entity, as only holders of the corresponding private key will be able to decrypt the PASSporT. This also prevents the CPS itself from learning the contents of PASSporTs, and thus metadata about calls in progress, which would make the CPS a less attractive target for pervasive monitoring (see [RFC7258]). To bolster the privacy story, prevent denial-of-service flooding of the CPS, and to complicate traffic analysis, a few additional mechanisms are also recommended.

The STIR architecture assumes that service providers and in some cases end user devices will have credentials suitable for attesting authority over telephone numbers per [I-D.ietf-stir-certificates]. These credentials provide the most obvious way that a CPS can authorize the storage and retrieval of PASSporTs. However, as use cases 3 and 4 in Section 5 show, it may sometimes make sense for the entity storing or retrieving PASSporTs to be an intermediary rather than a device associated with either the originating or terminating side of a call, and those intermediaries often would not have access to STIR credentials covering the telephone numbers in question. Requiring authorization based on a credential to store PASSporTs is therefore undesirable, though potentially acceptable if sufficient steps are taken to mitigate the privacy risk as described in the next section.

Furthermore, it is an explicit design goal of this mechanism to minimize the potential privacy exposure of using a CPS. Ideally, the out-of-band mechanism should not result in a worse privacy situation than in-band [I-D.ietf-stir-rfc4474bis] STIR: for in-band, we might

say that a SIP entity is authorized to receive a PASSporT if it is an intermediate or final target of the routing of a SIP request. As the originator of a call cannot necessarily predict the routing path a call will follow, an out-of-band mechanism could conceivably even improve on the privacy story. As a first step, transport-level security can provide confidentiality from eavesdroppers for both the storage and retrieval of PASSporTs.

6.1. Storage

For authorizing the storage of PASSporTs, the architecture can permit some flexibility. Note that in this architecture a CPS has no way to tell if a PASSporT is valid; it simply conveys encrypted blocks that it cannot access itself. In that architecture, it does not matter whether the CPS received a PASSporT from the authentication service that created it or from an intermediary gateway downstream in the routing path as in case 4.

Note that this architecture requires clients that stores PASSporTs to have access to a public key associated with the intended called party to be used to encrypt the PASSporT. Discovering this key requires some new service that does not exist today; depending on how the CPS is architected, however, some kind of key store or repository could be implemented adjacent to it, and perhaps even incorporated into its operation. Key discovery is made more complicated by the fact that there can potentially be multiple entities that have authority over a telephone number: a carrier, a reseller, an enterprise, and an end user might all have credentials permitting them to attest that they are allowed to originate calls from a number, say. PASSporTs therefore might need to be encrypted with multiple keys in the hopes that one will be decipherable by the relying party.

However, if literally anyone can store PASSporTs in the CPS, an attacker could easily flood the CPS with millions of bogus PASSporTs indexed under a target number, and thereby prevent that called party from finding a valid PASSporT for an incoming call buried in a haystack of fake entries. A CPS must therefore implement some sort of traffic control system to prevent flooding. Preferably, this should not require authenticating the source, as this will reveal to the CPS both the source and destination of traffic.

In order to do this, we propose the use of "blind signatures". A sender will initially authenticate to the CPS, and acquire a signed token for the CPS that will be presented later when storing a PASSporT. The flow looks as follows:

```

Sender                                CPS

Authenticate to CPS ----->
Blinded(K_temp) ----->
<----- Sign(K_cps, Blinded(K_temp))
[Disconnect]

Sign(K_cps, K_temp))
Sign(K_temp, E(K_receiver, PASSporT)) --->

```

At an initial time when no call is yet in progress, a potential client connects to the CPS, authenticates, and sends a blinded version of a freshly generated public key. The CPS returns a signed version of that blinded key. The sender can then unblind the key and gets a signature on `K_temp` from the CPS

Then later, when a client wants to store a `PASSporT`, it connects to the CPS anonymously (preferably over a network connection that cannot be correlated with the token acquisition) and sends both the signed `K_temp` and its own signature over the encrypted `PASSporT`. The CPS verifies both signatures and if they verify, stores the encrypted passport (discarding the signatures).

This design lets the CPS rate limit how many `PASSporTs` a given sender can store just by counting how many times `K_temp` appears; perhaps CPS policy might reject storage attempts and require acquisition of a new `K_temp` after storing more than a certain number of `PASSporTs` indexed under the same destination number in a short interval. This does not of course allow the CPS to tell when bogus data is being provisioned by an attacker, simply the rate at which data is being provisioned. Potentially, feedback mechanisms could be developed that would allow the called parties to tell the CPS when they are receiving unusual or bogus `PASSporTs`.

This architecture also assumes that the CPS will age out `PASSporTs`. A CPS SHOULD NOT keep any stored `PASSporT` for more than sixty seconds. Any reduction in this window makes substitution attacks (see Section 7.4) harder to mount, but making the window too small might conceivably age `PASSporTs` out while a heavily redirected call is still alerting. harder to mount

6.2. Retrieval

For retrieval of `PASSporTs`, this architecture assumes that clients contact the CPS to send requests of the form:

Are there any current PASSporTs for calls destined to 2.222.222.2222?

As all PASSporTs stored at the CPS are encrypted with a key belonging to the intended destination, then potentially the CPS could allow anyone to download PASSporTs for a called number without much fear of compromising private information about calls in progress - provided that the CPS always provides at least one encrypted blob in response to a request, even if there was no call in progress. Otherwise, entities could poll the CPS constantly, or eavesdrop on traffic, to learn whether or not calls were in progress. The CPS MUST generate at least one unique and plausible encrypted response to all retrieval requests, and these dummy encrypted PASSporTs MUST NOT be repeated for later calls.

Because the entity placing a call may discover multiple keys associated with the called party number, multiple valid PASSporTs may be stored in the CPS. A particular called party who retrieves PASSporTs from the CPS may have access to only one of those keys. Thus, the presence of one or more PASSporTs that the called party cannot decrypt - which would be indistinguishable from the "dummy" PASSporTs created by the CPS when no calls are in progress - does not entail that there is no call in progress. A retriever likely will need decrypt all PASSporTs retrieved from the CPS, and may find only one that is valid.

Note that in call forwarding cases, the difficulties in managing the relationship between PASSporTs with the diversion extension [I-D.ietf-stir-passport-divert] become more serious. The originating authentication service would encrypt the PASSporT with the public key of the intended destination, but when a call is forwarded, it may go to a destination that does not possess the corresponding private key. This requires special behavior on the part of the retargeting entity, and probably the CPS as well, to accommodate encrypted PASSporTs that show a secure chain of diversion. A storer could for example notify the CPS that the divert PASSporT it is storing relates to a specific PASSporT already in the CPS, but in so doing, the storer will inevitably reveal more metadata to the CPS.

7. Solution Architecture

In this section, we discuss a strawman architecture for providing the service described in the previous sections. This discussion is deliberately sketchy, focusing on broad concepts and skipping over details. The intent here is merely to provide an overall architecture, not an implementable specification.

7.1. Credentials and Phone Numbers

We start from the premise of the STIR problem statement [RFC7340] that phone numbers can be associated with credentials which can be used to attest ownership of numbers. For purposes of exposition, we will assume that ownership is associated with the endpoint (e.g., a smartphone) but it might well be associated with a provider or gateway acting for the endpoint instead. It might be the case that multiple entities are able to act for a given number, provided that they have the appropriate authority. [I-D.ietf-stir-certificates] describes a credentials system suitable for this purpose; the question of how an entity is determined to have control of a given number is out of scope for the current document.

7.2. Call Flow

An overview of the basic calling and verification process is shown below. In this diagram, we assume that Alice has the number +1.111.111.1111 and Bob has the number +2.222.222.2222.

Alice	Call Placement Service	Bob
Store PASSporT for 2.222.222.2222-->		
Call from 1.111.111.1111 ----->		
	<----- Retrieve PASSporT(s) for 2.222.222.2222?	
	Encrypted PASSporT -(2.222.222.2222,1.111.111.1111)-->	
	[Ring phone with callerid = 1.111.111.1111]	

When Alice wishes to make a call to Bob, she contacts the CPS and stores an encrypted PASSporT on the CPS indexed under Bob's number. The CPS then awaits retrievals for that number.

Once Alice has stored the PASSporT, she then places the call to Bob as usual. At this point, Bob's phone would usually ring and display Alice's number (+1.111.111.1111), which is informed by the existing PSTN mechanisms for relaying a calling party number (i.e., the CIN field of the IAM). Instead, Bob's phone transparently contacts the CPS and requests any current PASSporTs for calls to his number. The CPS responds with any such PASSporTs (assuming they exist). If such

a PASSport exists, and the verification service in Bob's phone decrypts it using his private key, validates it, then Bob's phone can then present the calling party number information as valid. Otherwise, the call is unverifiable. Note that this does not necessarily mean that the call is bogus; because we expect incremental deployment many legitimate calls will be unverifiable.

7.3. Security Analysis

The primary attack we seek to prevent is an attacker convincing the callee that a given call is from some other caller C. There are two scenarios to be concerned with:

The attacker wishes to impersonate a target when no call from that target is in progress.

The attacker wishes to substitute himself for an existing call setup as described in Section 7.4.

If an attacker can inject fake PASSport into the CPS or in the communication from the CPS to the callee, he can mount either attack. As PASSports should be digitally signed by an appropriate authority for the number and verified by the callee (see Section 7.1), this should not arise in ordinary operations. For privacy and robustness reasons, using TLS on the originating side when storing the PASSport at the CPS is recommended.

The entire system depends on the security of the credential infrastructure. If the authentication credentials for a given number are compromised, then an attacker can impersonate calls from that number. However, that is no different from in-band [I-D.ietf-stir-rfc4474bis] STIR.

7.4. Substitution Attacks

All that receipt of the PASSport from the CPS proves to the called party is that Alice is trying to call Bob (or at least was as of very recently) - it does not prove that any particular incoming call is from Alice. Consider the scenario in which we have a service which provides an automatic callback to a user-provided number. In that case, the attacker can try to arrange for a false caller-id value, as shown below:

Attacker	Callback Service	CPS	Bob

Place call to Bob ----->			
	Store PASSporT for CS:Bob ----->		
Call from CS (forged caller-id info) ----->			
	Call from CS -----> X		
			<----- Retrieve PASSporT for CS:Bob
	PASSporT for CS:Bob ----->		
			[Ring phone with callerid = CS]

In order to mount this attack, the attacker contacts the Callback Service (CS) and provides it with Bob's number. This causes the CS to initiate a call to Bob. As before, the CS contacts the CPS to insert an appropriate PASSporT and then initiates a call to Bob. Because it is a valid CS injecting the PASSporT, none of the security checks mentioned above help. However, the attacker simultaneously initiates a call to Bob using forged caller-id information corresponding to the CS. If he wins the race with the CS, then Bob's phone will attempt to verify the attacker's call (and succeed since they are indistinguishable) and the CS's call will go to busy/voice mail/call waiting. Note: in a SIP environment, the callee might notice that there were multiple INVITES and thus detect this attack.

8. Call Placement Service Discovery

In order for the two ends of the out-of-band dataflow to coordinate, they must agree on a way to discover a CPS and retrieve PASSporT objects from it based solely on the rendezvous information available: the calling party number and the called number. Because the storage of PASSporTs in this architecture is indexed by the called party number, it makes sense to discover a CPS based on the called party number as well. There are a number of potential service discovery mechanisms that could be used for this purpose. The means of service discovery may vary by use case.

Although the discussion above is written in terms of a single CPS, having a significant fraction of all telephone calls result in storing and retrieving PASSporTs at a single monolithic CPS has obvious scaling problems, and would as well allow the CPS to gather

metadata about a very wide set of callers and callees. These issues can be alleviated by operational models with a federated CPS; any service discovery mechanism for out-of-band STIR should enable federation of the CPS function.

Some service discovery possibilities under consideration include the following:

If a credential lookup service is already available (see Section 9), the CPS location can also be recorded in the callee's credentials; an extension to [I-D.ietf-stir-certificates] could for example provide a link to the location of the CPS where PASSporTs should be stored for a destination.

There exist a number of common directory systems that might be used to translate telephone numbers into the URIs of a CPS. ENUM [RFC6116] is commonly implemented, though no "golden root" central ENUM administration exists that could be easily reused today to help the endpoints discover a common CPS. Other protocols associated with queries for telephone numbers, such as the TeRI [I-D.peterson-modern-teri] protocol, could also serve for this application.

Another possibility is to use a single distributed service for this function. VIPR [I-D.rosenberg-dispatch-vipr-overview] proposed a RELOAD [RFC6940] usage for telephone numbers to help direct calls to enterprises on the Internet. It would be possible to describe a similar RELOAD usage to identify the CPS where calls for a particular telephone number should be stored. One advantage that the STIR architecture has over VIPR is that it assumes a credential system that proves authority over telephone numbers; those credentials could be used to determine whether or not a CPS could legitimately claim to be the proper store for a given telephone number.

Future versions of this specification will identify suitable service discovery mechanisms for out-of-band STIR.

9. Credential Lookup

In order to encrypt a PASSporT (see Section 6.1), the caller needs access to the callee's credentials (specifically their public key). This requires some sort of directory/lookup system. This document does not specify any particular scheme, but a list of requirements would be something like:

Obviously, if there is a single central database and the caller and callee each contact it in real time to determine the other's

credentials, then this represents a real privacy risk, as the central database learns about each call. A number of mechanisms are potentially available to mitigate this:

Have endpoints pre-fetch credentials for potential counterparties (e.g., their address book or the entire database).

Have caching servers in the user's network that proxy their fetches and thus conceal the relationship between the user and the credentials they are fetching.

Clearly, there is a privacy/timeliness tradeoff in that getting up-to-date knowledge about credential validity requires contacting the credential directory in real-time (e.g., via OCSP). This is somewhat mitigated for the caller's credentials in that he can get short-term credentials right before placing a call which only reveals his calling rate, but not who he is calling. Alternately, the CPS can verify the caller's credentials via OCSP, though of course this requires the callee to trust the CPS's verification. This approach does not work as well for the callee's credentials, but the risk there is more modest since an attacker would need to both have the callee's credentials and regularly poll the database for every potential caller.

We consider the exact best point in the tradeoff space to be an open issue.

10. Acknowledgments

The ideas in this document come out of discussions with Richard Barnes and Cullen Jennings. We'd also like to thank Robert Sparks for helpful suggestions.

11. IANA Considerations

This memo includes no request to IANA.

12. Security Considerations

This entire document is about security, but the detailed security properties depend on having a single concrete scheme to analyze.

13. Informative References

[I-D.ietf-stir-certificates]
Peterson, J. and S. Turner, "Secure Telephone Identity Credentials: Certificates", draft-ietf-stir-certificates-14 (work in progress), May 2017.

- [I-D.ietf-stir-passport]
Wendt, C. and J. Peterson, "Personal Assertion Token (PASSporT)", draft-ietf-stir-passport-11 (work in progress), February 2017.
- [I-D.ietf-stir-passport-divert]
Peterson, J., "PASSporT Extension for Diverted Calls", draft-ietf-stir-passport-divert-00 (work in progress), July 2017.
- [I-D.ietf-stir-rfc4474bis]
Peterson, J., Jennings, C., Rescorla, E., and C. Wendt, "Authenticated Identity Management in the Session Initiation Protocol (SIP)", draft-ietf-stir-rfc4474bis-16 (work in progress), February 2017.
- [I-D.peterson-modern-teri]
Peterson, J., "An Architecture and Information Model for Telephone-Related Information (TeRI)", draft-peterson-modern-teri-03 (work in progress), July 2017.
- [I-D.rosenberg-dispatch-vipr-overview]
Rosenberg, J., Jennings, C., and M. Petit-Huguenin, "Verification Involving PSTN Reachability: Requirements and Architecture Overview", draft-rosenberg-dispatch-vipr-overview-04 (work in progress), October 2010.
- [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>>.
- [RFC6116] Bradner, S., Conroy, L., and K. Fujiwara, "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)", RFC 6116, DOI 10.17487/RFC6116, March 2011, <<https://www.rfc-editor.org/info/rfc6116>>.
- [RFC6940] Jennings, C., Lowekamp, B., Ed., Rescorla, E., Baset, S., and H. Schulzrinne, "REsource LOcation And Discovery (RELOAD) Base Protocol", RFC 6940, DOI 10.17487/RFC6940, January 2014, <<https://www.rfc-editor.org/info/rfc6940>>.

- [RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <<https://www.rfc-editor.org/info/rfc7258>>.
- [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>>.

Authors' Addresses

Eric Rescorla
Mozilla

Email: ekr@rtfm.com

Jon Peterson
Neustar, Inc.
1800 Sutter St Suite 570
Concord, CA 94520
US

Email: jon.peterson@neustar.biz

Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 3, 2018

J. Peterson
Neustar
October 30, 2017

PASSporT Extension for Diverted Calls
draft-ietf-stir-passport-divert-01.txt

Abstract

This document extends PASSporT, which conveys cryptographically-signed information about the people involved in personal communications, to include an indication that a call has been diverted from its original destination to a new one. This information can greatly improve the decisions made by verification services in call forwarding scenarios.

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 3, 2018.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	2
2. Terminology	3
3. PASSport 'div' Claim	3
4. Using 'div' in SIP	5
4.1. Authentication Service Behavior	5
4.2. Verification Service Behavior	6
5. Using 'div' in STIR out-of-band	6
6. Extending 'div'	7
7. Acknowledgments	7
8. IANA Considerations	7
9. Security Considerations	7
10. Informative References	8
Author's Address	9

1. Introduction

PASSport [I-D.ietf-stir-passport] is a token format based on JWT [RFC7519] for conveying cryptographically-signed information about the people 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 include an indication that a call has been diverted from its originally destination to a new one.

Although the STIR problem statement [RFC7340] is focused on preventing the impersonation of the caller's identity, which is a common enabler for threats such as robocalling and voicemail hacking on the telephone network today, it also provides a signature over the called number as the authentication service sees it. As [I-D.ietf-stir-rfc4474bis] Section 12.1 describes, this protection over the contents of the To header field is intended to prevent a class of cut-and-paste attacks. If Alice calls Bob, for example, Bob might attempt to cut-and-paste the Identity header field in Alice's INVITE into a new INVITE that Bob sends to Carol, and thus be able to fool Carol into thinking the call came from Alice and not Bob. With the signature over the To header field value, the INVITE Carol sees will clearly have been destined originally for Bob, and thus Carol can view the INVITE as suspect.

However, as [I-D.ietf-stir-rfc4474bis] Section 12.1.1 points out, it is difficult for Carol to confirm or reject these suspicions based on the information she receives from the baseline PASSport object. The

common "call forwarding" service serves as a good example of the fact that the original called party number is not always the number to which a call is delivered. The address in the To header field value of SIP requests is not supposed to change, accordingly to baseline [RFC3261], as it is the Request-URI that is supposed to be updated when a call is retargeted, but practically speaking some operational environments do alter the To header field. There are a number of potential ways for intermediaries to indicate that such a forwarding operating has taken place. The History-Info header field [RFC7044] was created to store the Request-URIs that are discarded by a call in transit. The SIP Diversion header field [RFC5806], though historic, is still used for this purpose by some operators today. Neither of these header fields provide any cryptographic assurance of secure redirection, and they can both capture minor syntactical changes in URIs that do not reflect a change to the actual target of a call.

This specification therefore extends PASSporT with an explicit indication that original called number in PASSporT no longer reflects the destination to which a call is likely to be delivered. Verification services and the relying parties who make authorization decisions about communications may use this indication to confirm that a legitimate retargeting of the call has taken place, rather than a cut-and-paste attack.

2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in [RFC2119].

3. PASSporT 'div' Claim

This specification defines a new JSON Web Token claim for "div" which indicates a previous destination for a call during its routing process. When a retargeting entity receives a call signed with a PASSporT, it may act as an authentication service and create a new PASSporT containing the "div" claim to attach to the call (without removing the original PASSporT). Note that a new PASSporT is only necessary when the canonical form of the "dest" identifier (per the canonicalization procedures in [I-D.ietf-stir-rfc4474bis] Section 8) changes due to this retargeting. "div" is typically populated with a destination address found in the "dest" field of PASSporT received by the retargeting entity. These new PASSporT generated by retargeting entities MUST include the "div" PASSporT type, and an "x5u" field pointing to a credential that the retargeting entity controls. The new PASSporT will look as follows:

```
{ "typ":"passport",  
  "ppt":"div",  
  "alg":"ES256",  
  "x5u":"https://www.example.com/cert.pkx" }
```

A PASSporT claims object containing "div" is populated with a modification of the original token before the call was retargeted: at a high level, the original identifier for the called party in the "dest" array will become the "div" claim in the new PASSporT. If the "dest" array of the original PASSporT contains multiple identifiers, the retargeting entity MUST select only one them to occupy the "div" field in the new PASSporT. and in particular, it MUST select an identifier that is within the scope of the credential that the retargeting entity will specify in the "x5u" of the PASSporT header (as described below).

The new target for the call selected by the retargeting entity becomes the value of the "dest" array of the new PASSporT. The "orig" value MUST be copied into the new PASSporT from the original PASSporT received by the retargeting entity. The retargeting entity SHOULD retain the "iat" value from the original PASSporT, though if in the underlying signaling protocol (e.g. SIP) the retargeting entity changes the date and time information in the retargeted request, the new PASSporT should instead reflect that date and time. No other extension claims should be copied from the original PASSporT to the "div" PASSporT.

So, for an original PASSporT of the form:

```
{ "orig":{"tn":"12155551212"},  
  "dest":{"tn":"12155551213"},  
  "iat":1443208345 }
```

If the retargeting entity is changing the target from 12155551213 to 12155551214, the new PASSporT with "div" would look as follows:

```
{ "orig":{"tn":"12155551212"},  
  "dest":{"tn":"12155551214"},  
  "iat":1443208345,  
  "div":{"tn":"12155551213"} }
```

After the PASSporT header and claims have been constructed, their signature is generated per the guidance in [I-D.ietf-stir-passport] - except for the credential required to sign it. While in the ordinary construction of a PASSporT, the credential used to sign will have authority over the identity in the "orig" claim (for example, a certificate with authority over the telephone number in "orig" per [I-D.ietf-stir-certificates]), for all PASSporTs using the "div" type

the signature MUST be created with a credential with authority over the identity present in the "div" claim. So for the example above, where the original "dest" is "12155551213", the signer of the new PASSport object MUST have authority over that telephone number, and need not have any authority over the telephone number present in the "orig" claim.

4. Using 'div' in SIP

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

4.1. Authentication Service Behavior

An authentication service only adds an Identity header field containing the "div" PASSport type to an SIP request that already contains at least one Identity header field; it MUST NOT add a "div" request to an INVITE that contains no other Identity headers fields. Note that the authentication service doing so does not remove or replace any existing Identity header fields, it simply adds a new one. When adding an Identity header field with a PASSport object containing a "div" claim, SIP authentication services MUST also add a "ppt" parameter to that Identity header with a value of "div". The resulting compact form Identity header field to add to the message might look as follows:

```
Identity: ..sv5CTo05KqpSmtHt3dcEiO/1CWTSZtnG3iV+lnmurLXV/HmtYNS7Ltrg9dlxkWzo
eU7d7OV8HweTTDobV3itTmgPwCFjaEmMyEI3d7SyN21yNDo2ER/Ovgtw0Lu5csIp
pPqOgluXndzHbG7mR6Rl9BnUhHufVRbp5lMn3w0gfUs; \
info=<https://biloxi.example.org/biloxi.cer>;alg=ES256;ppt="div"
```

A SIP authentication service typically will derive the new value of "dest" from a new Request-URI that is set for the SIP request before it is forwarded. Older values of the Request-URI may appear in header fields like Diversion or History-Info; this document specifies no specific interaction between the "div" mechanism and those SIP header fields. Note as well that because PASSport operates on canonicalized telephone numbers and normalized URIs, many smaller changes to the syntax of identifiers that might be captured by other mechanisms (like History-Info) that record regargeting will likely not require a "div" PASSport.

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 "div" value of "ppt" is as follows.

In order to use the "div" extension, a verification service needs to inspect all of the valid Identity header field values associated with a request, as an Identity header field value containing "div" necessarily refers to an earlier PASSporT already in the message. In particular, the verification service must find a PASSporT associated with the call, one created earlier, that contains a "dest" claim with a value equivalent to the "div" claim in the current PASSporT. It is possible that this earlier PASSporT will also contain a "div", and that it will in turn chain to a still earlier PASSporT stored in a different Identity header field value. Ultimately, by looking at this chain of transformations and validating the associated signatures, the verification service will be able to ascertain that the appropriate parties were responsible for the retargeting of the call to its ultimate destination; this can help the verification service to determine that original PASSporT in the call was not simply used in a cut-and-paste attack. This will help relying parties to make any associated authorization decisions in terms of how the call will be treated - though, per [I-D.ietf-stir-rfc4474bis] Section 6.2.1, that decision is a matter of local policy.

Note that Identity header fields are not ordered in a SIP request, and in a case where there is a multiplicity of Identity header fields in a request, some sorting may be required to match divert PASSporTs to their originals.

5. Using 'div' in STIR out-of-band

When storing a PASSporT with "div" at a Call Placement Service (CPS) for STIR out-of-band [I-D.ietf-stir-rfc4474bis] scenarios, clients should include an "opt" element within "div". "opt" contains the full form of the original PASSporT from which the "div" was generated. If the diverting entity originally received that PASSporT encrypted, it MUST decrypt it before storing it in "opt." The entire "div" PASSporT would then be signed and re-encrypted normally for storage at an out-of-band Call Placement Service (CPS).

A "div" PASSporT containing the "opt" would look as follows:


```
{
  "orig": {"tn": "12155551212"},
  "dest": {"tn": "12155551214"},
  "iat": 1443208345,
  "div": {"tn": "121555551213"},
  "opt": "eyJhbGciOiJFUzIiNiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IiBkaioHR0cHM6Ly9jZXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LmNlciJ9.eyJkZXN0Ijp7InVyaSI6WyJzaXA6YWxpY2VAZXhhbXBsZS5jb20iXX0sImV4IjE6IjE6NDMyMDgzNDUuIiLCJvcmlnIjp7InRuIjoimTIxNTU1NTEyMTIifX0.rq3pjTlhoRwakEGjHCnWSwUnshd0-zJ6F1VOgFWSjHBr8Qjplk-cpFYpFYsojNCpTzO3QfPOLckGaS6hEck7w"} }
```

The "opt" extension is not required for any unencrypted in-band PASSporT conveyance. For forward compatibility reasons, its use is not forbidden in those environments.

6. Extending 'div'

Past experience has shown that there may be additional information about the motivation for retargeting that relying parties might consider when making authorization decisions about a call, see for example the "reason" associated with the SIP Diversion header field [RFC5806]. Future extensions to this specification might incorporate reasons into "div".

7. Acknowledgments

We would like to thank Robert Sparks for contributions to this document.

8. IANA Considerations

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

Claim Name: "div"

Claim Description: New Target of a Call

Change Controller: IESG

Specification Document(s): [RFCThis]

9. Security Considerations

This specification describes a security feature, and is primarily concerned with increasing security when calls are forwarded. Including information about how calls were retargeted during the routing process can allow downstream entities to infer particulars of

the policies used to route calls through the network. However, including this information about forwarding is at the discretion of the retargeting entity, so if there is a requirement to keep the original called number confidential, no PASSport should be created for that retargeting - the only consequence will be that downstream entities will be unable to correlate an incoming call with the original PASSport without access to some prior knowledge of the policies that could have caused the retargeting.

10. Informative References

[I-D.ietf-stir-certificates]

Peterson, J. and S. Turner, "Secure Telephone Identity Credentials: Certificates", draft-ietf-stir-certificates-14 (work in progress), May 2017.

[I-D.ietf-stir-oob]

Rescorla, E. and J. Peterson, "STIR Out of Band Architecture and Use Cases", draft-ietf-stir-oob-00 (work in progress), July 2017.

[I-D.ietf-stir-passport]

Wendt, C. and J. Peterson, "Personal Assertion Token (PASSport)", draft-ietf-stir-passport-11 (work in progress), 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)", draft-ietf-stir-rfc4474bis-16 (work in progress), 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, <<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>>.

[RFC5806] Levy, S. and M. Mohali, Ed., "Diversion Indication in SIP", RFC 5806, DOI 10.17487/RFC5806, March 2010, <<https://www.rfc-editor.org/info/rfc5806>>.

- [RFC7044] Barnes, M., Audet, F., Schubert, S., van Elburg, J., and C. Holmberg, "An Extension to the Session Initiation Protocol (SIP) for Request History Information", RFC 7044, DOI 10.17487/RFC7044, February 2014, <<https://www.rfc-editor.org/info/rfc7044>>.
- [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>>.
- [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>>.

Author's Address

Jon Peterson
Neustar, Inc.
1800 Sutter St Suite 570
Concord, CA 94520
US

Email: jon.peterson@neustar.biz

Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 4, 2018

J. Peterson
Neustar
C. Wendt
Comcast
July 3, 2017

PASSporT Extension for Rich Call Data
draft-ietf-stir-passport-rcd-00.txt

Abstract

This document extends PASSporT, a token for conveying cryptographically-signed information about personal communications, to include rich data that can be rendered to users, such as a human-readable display name comparable to the "Caller ID" function common on the telephone network. The element defined for this purpose is extensible to include related information about calls that helps people decide whether to pick up the phone.

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 <http://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 January 4, 2018.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must

include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	2
2. Terminology	3
3. PASSport 'rcd' Claim	3
4. Further Information Associated with Callers	4
5. Third-Party Uses	5
5.1. Signing as a Third Party	6
6. Levels of Assurance	6
7. Using 'rcd' in SIP	6
7.1. Authentication Service Behavior	7
7.2. Verification Service Behavior	7
8. Acknowledgments	8
9. IANA Considerations	8
9.1. JSON Web Token Claims	8
9.2. PASSport Types	9
9.3. PASSport RCD Types	9
10. Security Considerations	9
11. Informative References	9
Authors' Addresses	10

1. Introduction

PASSport [I-D.ietf-stir-passport] is a token format based on JWT [RFC7519] for conveying cryptographically-signed information about the people 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. The STIR problem statement [RFC7340] declared securing the display name of callers outside of STIR's initial scope, so baseline STIR provides no features for caller name. This specification documents an optional mechanism for PASSport and the associated STIR mechanisms which extends PASSport to carry additional elements conveying richer information: information that is intended to be rendered to an end user to assist a called party in determining whether to accept or trust incoming communications. This includes the name of the person on one side of a communications session, the traditional "Caller ID" of the telephone network, along with related display information that would be rendered to the called party during alerting, or potentially used by an automaton to determine whether and how to alert a called party.

In the traditional telephone network, the display name associated with a call is typically provided in one of three ways: by a third-

party service queried at the terminating side, by the originator of the call, or through a local address book maintained by a device on the terminating side. The STIR architecture lends itself especially to the first of these approaches, as it assumes that an authority on the originating side of the call provides a cryptographic assurance of the validity of the calling party number in order to prevent impersonation attacks. That same authority could sign for a display name associated with that number, which the terminating side could render to the user when the call is alerting. Even when the originating side does not provide a display name for the caller, the cryptographic attestation of the validity of the calling number provided by STIR still allows the terminating side to query a local or remote service for a name associated with that number without fear that the number has been impersonated by the caller; STIR thus makes "Caller ID" more secure even when there is no first-party attestation of a display name. For these cases, this specification outlines various ways that a display name for a calling party could be determined at the terminating side in a secure fashion.

2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119 [RFC2119] and RFC 6919 [RFC6919].

3. PASSporT 'rcd' Claim

This specification defines a new JSON Web Token claim for "rcd", Rich Call Data, the value of which is an array of JSON subelements. The initial subelement defined here is a display name, "nam", associated with the originator of personal communications, which may for example derive from the display-name component of the From header field value of a SIP request, or a similar field in other PASSporT using protocols.

The "rcd" claim may appear in any PASSporT claims object as an optional element. The creator of a PASSporT MAY however add a "ppt" value of "rcd" to the header of a PASSporT as well, in which case the PASSporT claims MUST contain a "rcd" 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": "rcd",  
  "alg": "ES256",  
  "x5u": "https://www.example.com/cert.cer" }
```

The PASSporT claims object will then contain the "rcd" key with its corresponding value. The value of "rcd" is an array of JSON objects, of which one, the "nam" object, is mandatory. The key syntax of "nam" follows the display-name ABNF given in [RFC3261].

```
{ "orig":{"tn":"12155551212"},  
  "dest":{"tn":"12155551213"},  
  "iat":1443208345,  
  "iss":"Example, Inc.",  
  "rcd":{"nam":"Alice Atlanta"} }
```

After the header and claims PASSporT objects have been constructed, their signature is generated normally per the guidance in [I-D.ietf-stir-passport].

4. Further Information Associated with Callers

Beyond naming information, there may be additional human-readable information about the calling party that should be rendered to the end user in order to help the called party decide whether or not to pick up the phone. This is not limited to information about the caller, but includes information about the call itself, which may derive from analytics that determine based on call patterns or similar data if the call is likely to be one the called party wants to receive. Such data could include:

- information related to the location of the caller, or

- any organizations or institutions that the caller is associated with, or even categories of institutions (is this a government agency, or a bank, or what have you), or

- hyperlinks to images, such as logos or pictures of faces, or to similar external profile information, or

- information that will be processed by an application before rendering it to a user, like social networking data that shows that an unknown caller is a friend-of-a-friend, or reputation scores derived from crowdsourcing, or confidence scores based on broader analytics about the caller and callee.

All of these data elements would benefit from the secure attestations provided by the STIR and PASSporT frameworks. A new IANA registry has been defined to hold potential values of the "rcd" array; see Section 9.3. Specific extensions to the "rcd" PASSporT claim are left for future specification.

While in the traditional telephone network, the business relationship between calling customers and their telephone service providers is the ultimate root of information about a calling party's name, some other forms of data like crowdsourced reputation scores might derive from third parties. It is more likely that when those elements are present, they will be in a third-party "rcd" PASSport.

5. Third-Party Uses

While rich data about the call can be provided by an originating authentication service, the terminating side or an intermediary in the call path could also acquire rich call data by querying a third-party service. In telephone operations today, a third-party information service is commonly queried with the calling party's number in order to learn the name of the calling party, and potentially other helpful information could also be passed over that interface. The value of using a PASSport to convey this information from third parties lies largely in the preservation of the original authority's signature over the data, and the potential for the PASSport to be conveyed from intermediaries to endpoint devices. Effectively, these use cases form of subcase of out-of-band [I-D.rescorla-stir-fallback] use cases. The manner in which third-party services are discovered is outside the scope of this document.

An intermediary use case might look as follows: a SIP INVITE carries a display name in its From header field value and an initial PASSport object without the "rcd" claim. When the a terminating verification service implemented at a SIP proxy server receives this request, and determines that the signature is valid, it might query a third-party service that maps telephone numbers to calling party names. Upon receiving the PASSport in a response from that third-party service, the terminating side could add a new Identity header field to the request for the "rcd" PASSport object provided by the third-party service. It would then forward the INVITE to the terminating user agent. If the display name in the "rcd" PASSport object matches the display name in the INVITE, then the name would presumably be rendered to the end user by the terminating user agent.

A very similar flow could be followed by an intermediary closer to the origination of the call. Presumably such a service could be implemented at an originating network in order to decouple the systems that sign for calling party numbers from the systems that provide rich data about calls.

In an alternative use case, the terminating user agent might query a third-party service. In this case, no new Identity header field would be generated, though the terminating user agent might receive a PASSport object in return from the third-party service, and use the

"rcd" field in the object as a calling name to render to users while alerting.

5.1. Signing as a Third Party

When a third party issues a PASSporT with an "rcd" claim, the PASSporT MUST contain the "rcd" "ppt" type in its header object. It moreover MUST include an "iss" claim as defined in [RFC7519] to indicate the source of this PASSporT; that field SHOULD be populated with the subject of the credential used to sign the PASSporT.

A PASSporT with a "ppt" of "rcd" MAY be signed with credentials that do not have authority over the identity that appears in the "orig" element of the PASSporT claims. Relying parties in STIR have always been left to make their own authorization decisions about whether or not to trust the signers of PASSporTs, and in the third-party case, where an entity has explicitly queried a service to acquire the PASSporT object, it may be some external trust or business relationship that induces the relying party to trust a PASSporT.

6. Levels of Assurance

As "rcd" can be provided by either first or third parties, relying parties could benefit from an additional claim that indicates the relationship of the attesting party to the caller. Even in first party cases, this admits of some complexity: the Communications Service Provider (CSP) to which a number was assigned might in turn delegate the number to a reseller, who would then sell the number to an enterprise, in which case the CSP might have little insight into the caller's name. In third party cases, a caller's name could derive from any number of data sources, on a spectrum between public data scraped from web searches to a direct business relationship to the caller. As multiple PASSporTs can be associated with the same call, potentially a verification service could receive attestations of the caller name from multiple sources, which have different levels of granularity or accuracy.

Therefore PASSporTs that carry "rcd" data SHOULD also carry an indication of the relationship of the generator of the PASSporT to the caller. [TBD claim - take from SHAKEN?]

7. Using 'rcd' in SIP

This section specifies SIP-specific usage for the "rcd" claim in PASSporT, and in the SIP Identity header field value. Other using protocols of PASSporT may define their own usages for the "rcd" claim.

7.1. Authentication Service Behavior

An authentication service creating a PASSporT containing a "rcd" claim MAY include a "ppt" for "rcd" or not. Third-party authentication services following the behavior in Section 5.1 MUST include a "ppt" of "rcd". If "ppt" does contain a "rcd", then any SIP authentication services MUST add a "ppt" parameter to the Identity header containing that PASSporT with a value of "rcd". The resulting Identity header might look as follows:

```
Identity: "sv5CTo05KqpSmtHt3dcEiO/1CWTSZtnG3iV+lnmurLXV/HmtYNS7Ltrg9dlxkWzo
eU7d7OV8HweTTDobV3itTmgPwCFjaEmMyEI3d7SyN21yNDo2ER/Ovgtw0Lu5csIp
pPqOgluXndzHbG7mR6Rl9BnUhufVRbp5lMn3w0gfUs="; \
info=<https://biloxi.example.org/biloxi.cer>;alg=ES256;ppt="rcd"
```

This specification assumes that by default, a SIP authentication service will derive the value of "rcd" from the display-name component of the From header field value of the request. It is however a matter of authentication service policy to decide how it populates the value of "rcd", which MAY also derive from other fields in the request, from customer profile data, or from access to external services. If the authentication service generates a PASSporT object containing "rcd" with a value that is not equivalent to the From header field display-name value, it MUST use the full form of the PASSporT object in SIP.

7.2. 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 "rcd" is as follows. If the PASSporT is in compact form, then the verification service SHOULD extract the display-name from the From header field value, if any, and use that as the value for the "rcd" key when it recomputes the header and claims of the PASSporT object. If the signature validates over the recomputed object, then the verification should be considered successful.

However, if the PASSporT is in full form with a "ppt" value of "rcd", then the verification service MUST extract the value associated with the "rcd" "nam" key in the object. If the signature validates, then the verification service can use the value of the "rcd" "nam" key as the display name of calling party, which would in turn be rendered to alerted users or otherwise leveraged in accordance with local policy. This will allow SIP networks that convey the display name through a field other than the From header field to interoperate with this specification.

The third-party "rcd" PASSporT cases presents some new challenges, as an attacker could attempt to cut-and-paste such a third-party PASSporT into a SIP request in an effort to get the terminating user agent to render the display name or confidence values it contains to a call that should have no such assurance. A third-party "rcd" PASSporT provides no assurance that the calling party number has not been spoofed: if it is carried in a SIP request, for example, then some other PASSporT in another Identity header field value would have to carry a PASSporT attesting that. A verification service **MUST** determine that the calling party number shown in the "orig" of the "rcd" PASSporT corresponds to the calling party number of the call it has received, and that the "iat" field of the "rcd" PASSporT is within the date interval that the verification service would ordinarily accept for a PASSporT.

Verification services may alter their authorization policies for the credentials accepted to sign PASSporTs when third parties generate PASSporT objects, per Section 5.1. This may include accepting a valid signature over a PASSporT even if it is signed with a credential that does not attest authority over the identity in the "orig" claim of the PASSporT, provided that the verification service has some other reason to trust the signer. No further guidance on verification service authorization policy is given here.

The behavior of a SIP UAS upon receiving an INVITE containing a PASSporT object with a "rcd" claim will largely remain a matter of implementation policy. In most cases, implementations would render this calling party name information to the user while alerting. Any user interface additions to express confidence in the veracity of this information are outside the scope of this specification.

8. Acknowledgments

We would like to thank Robert Sparks for helpful suggestions.

9. IANA Considerations

9.1. JSON Web Token Claims

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

Claim Name: "rcd"

Claim Description: Caller Name Information

Change Controller: IESG

Specification Document(s): [RFCThis]

9.2. PASSporT Types

This specification requests that the IANA add a new entry to the PASSporT Types registry for the type "rcd" which is specified in [RFCThis].

9.3. PASSporT RCD Types

This document requests that the IANA create a new registry for PASSporT RCD types. Registration of new PASSporT RCD types shall be under the Specification Required policy.

This registry is to be initially populated with a single value for "nam" which is specified in [RFCThis].

10. Security Considerations

Revealing information such as the name, location, and affiliation of a person necessarily entails certain privacy risks. Baseline PASSporT has no particular confidentiality requirement, as the information it signs over in a using protocol like SIP is all information that SIP carries in the clear anyway. Transport-level security can hide those SIP fields from eavesdroppers, and the same confidentiality mechanisms would protect any PASSporT(s) carried in SIP.

More TBD.

11. Informative References

[I-D.ietf-stir-passport]

Wendt, C. and J. Peterson, "Personal Assertion Token (PASSporT)", draft-ietf-stir-passport-11 (work in progress), 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)", draft-ietf-stir-rfc4474bis-16 (work in progress), February 2017.

[I-D.rescorla-stir-fallback]

Rescorla, E. and J. Peterson, "STIR Out of Band Architecture and Use Cases", draft-rescorla-stir-fallback-02 (work in progress), June 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>>.
- [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>>.
- [RFC6919] Barnes, R., Kent, S., and E. Rescorla, "Further Key Words for Use in RFCs to Indicate Requirement Levels", RFC 6919, DOI 10.17487/RFC6919, April 2013, <<http://www.rfc-editor.org/info/rfc6919>>.
- [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>>.
- [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>>.

Authors' Addresses

Jon Peterson
Neustar, Inc.
1800 Sutter St Suite 570
Concord, CA 94520
US

Email: jon.peterson@neustar.biz

Chris Wendt
Comcast
One Comcast Center
Philadelphia, PA 19103
USA

Email: chris-ietf@chriswendt.net

STIR
Internet-Draft
Intended status: Standards Track
Expires: March 18, 2018

R. Singh
Vencore Labs
M. Dolly
AT&T
S. Das
Vencore Labs
A. Nguyen
Office of Emergency Communication/DHS
September 14, 2017

PASSporT Extension for Resource-Priority Authorization
draft-ietf-stir-rph-01

Abstract

This document extends the PASSporT object to convey cryptographically-signed assertions of authorization for communications 'Resource-Priority'. It extends PASSporT to allow cryptographic-signing of the SIP 'Resource-Priority' header field which is used for communications resource prioritization. It also describes how the PASSporT extension is used in SIP signaling to convey assertions of authorization of the information in the SIP 'Resource-Priority' header field.

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 March 18, 2018.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

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 past attacks	7
7.2. Solution Considerations	7
7.3. Acknowledgements	7
8. References	7
8.1. Normative References	8
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, 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 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".

```
{  "orig":{"tn":"12155551212"},
  "dest":{"tn":"12125551213"},
  "iat":1443208345,
  "rph":{"auth":"ets.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.eyJpc3MiOiJleUowZVhBaU9pSndZWE56Y0c5eWRDSXNEUW9pY0hCMElqb2ljbkJvSWl3TkNpSmhiR2NpT2lKRlV6STFOaUlrRFFvaWVEVjFJanBvZEhSd2N6b3ZMM2QzZHk1bGVHRnRjR3hstG1OdmJTOWpaWEowTG1ObGNuME5DZz09IHx84oCZLuKAmXx8IGV5SnZjbWxuSWpwN0luUnVJam9pTVRJeE5UVTFOVEV5TVRJaWZTd2dEUW9pYVdGMElqb2lNVFEwTXpJd09ETTBOU0lzMUEwS0ltUmxjM1FpT25zaWRHNGlPaU14TWpFMU5UVTFNVEl4TXlKOURRb2ljbkJvSWpwN0ltRjFkR2dpT2lKbGRITXVNQ0o5RFFvTkNnMESgICAgIiwibmJmIjojNDk4NDg5MTU5LCJleHAiOiJlOTg0OTI3NTksImhhdCI6MTQ5ODQ4OTE1OX0.0ia2-qJTlDJICsJ_Af2A5slhO2iJU-kAHG-HRVVhRiUea6acIoD0w2Bc3Ap4iZ6izx7haRj55MtKKCWY5_bItA";
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.

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

- o Claim Name: "rph"
- o Claim Description: Resource Priority Header
- o Change Controller: IESG
- o 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 past 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":

- o 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.
- o 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>>.
- [RFC6919] Barnes, R., Kent, S., and E. Rescorla, "Further Key Words for Use in RFCs to Indicate Requirement Levels", RFC 6919, DOI 10.17487/RFC6919, April 2013, <<http://www.rfc-editor.org/info/rfc6919>>.
- [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

stir
Internet-Draft
Intended status: Standards Track
Expires: May 3, 2018

C. Wendt
Comcast
M. Barnes
MLB@Realtime Communications
October 30, 2017

PASSporT SHAKEN Extension (SHAKEN)
draft-wendt-stir-passport-shaken-01

Abstract

This document extends PASSporT, a token object that conveys cryptographically-signed information about the participants involved in personal communications, to include information defined as part of the SHAKEN [ATIS-1000074] specification for indicating an attestation level and originating ID.

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 3, 2018.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	2
2. Terminology	2
3. Overview of 'shaken' PASSport extension	3
4. PASSport 'attest' Claim	3
5. PASSport 'origid' Claim	4
6. Example	4
7. Using 'shaken' in SIP	5
8. IANA Considerations	5
8.1. JSON Web Token claims	5
8.2. PASSport Types	6
9. Security Considerations	6
10. Acknowledgements	6
11. References	6
11.1. Normative References	6
11.2. Informative References	7
Authors' Addresses	7

1. Introduction

The SHAKEN specification defines a framework for using STIR protocols including PASSport [I-D.ietf-stir-passport], RFC4474bis [I-D.ietf-stir-rfc4474bis] and the STIR certificate framework [I-D.ietf-stir-certificates] 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 is 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 attribution 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 indicators as a specified PASSport extension.

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 [RFC2119].

3. Overview of 'shaken' PASSporT extension

The SHAKEN framework is designed to use PASSporT [I-D.ietf-stir-passport] 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 or 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 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 a 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:

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

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

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

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

- o Is the entry point of the call into its VoIP network.
- o 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. There will likely be best practices documents that more precisely guide it's usage in real deployments.

6. Example

```
Protected Header
{
  "alg": "ES256",
  "typ": "passport",
  "ppt": "shaken",
  "x5u": "https://cert.example.org/passport.crt"
}
Payload
{
  "attest": "A"
  "dest": { "uri": ["sip:alice@example.com"] }
  "iat": "1443208345",
  "orig": { "tn": "12155551212" },
  "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 defined in [I-D.ietf-stir-rfc4474bis]. The carriage of the 'attest' and 'origid' values are in the full PASSporT token included in the identity header as specified in [ATIS-1000074].

8. IANA Considerations

8.1. 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]

8.2. PASSporT Types

This specification requests that the IANA add a new entry to the PASSporT Types registry for the type "shaken" which is specified in [RFCThis].

9. Security Considerations

TBD

10. Acknowledgements

TBD

11. References

11.1. Normative References

[ATIS-1000074]

ATIS/SIP Forum NNI Task Group, "Signature-based Handling of Asserted information using toKENs (SHAKEN)", January 2017.

[I-D.ietf-stir-certificates]

Peterson, J. and S. Turner, "Secure Telephone Identity Credentials: Certificates", draft-ietf-stir-certificates-14 (work in progress), May 2017.

[I-D.ietf-stir-passport]

Wendt, C. and J. Peterson, "Personal Assertion Token (PASSporT)", draft-ietf-stir-passport-11 (work in progress), 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)", draft-ietf-stir-rfc4474bis-16 (work in progress), February 2017.

[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>>.

11.2. 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>>.

Authors' Addresses

Chris Wendt
Comcast
One Comcast Center
Philadelphia, PA 19103
USA

Email: chris-ietf@chriswendt.net

Mary Barnes
MLB@Realtime Communications

Email: mary.ietf.barnes@gmail.com