Workgroup: Network Working Group
Internet-Draft:
draft-ietf-stir-servprovider-oob-05
Published: 23 October 2023
Intended Status: Standards Track
Expires: 25 April 2024
Authors: J. Peterson
Neustar

Out-of-Band STIR for Service Providers

Abstract

The Secure Telephone Identity Revisited (STIR) framework defines means of carrying its Persona Assertion Tokens (PASSporTs) either in-band, within the headers of a SIP request, or out-of-band, through a service that stores PASSporTs for retrieval by relying parties. This specification defines a way that the out-of-band conveyance of PASSporTs can be used to support large service providers, for cases in which in-band STIR conveyance is not universally available.

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 25 April 2024.

Table of Contents

1. Introduction

STIR [RFC8224] provides a cryptographic assurance of the identity of calling parties in order to prevent impersonation, which is a key enabler of unwanted robocalls, swatting, vishing, voicemail hacking, and similar attacks (see [RFC7340]). The STIR out-of-band [RFC8816] framework enables the delivery of PASSporT [RFC8225] objects through a Call Placement Service (CPS), rather than carrying them within a signaling protocol such as SIP. Out-of-band conveyance is valuable when end-to-end SIP delivery of calls is partly or entirely unavailable due to network border policies, calls routinely transitting a gateway to the PSTN, or similar circumstances.

While out-of-band STIR can be implemented as an open Internet service, it then requires complex security measures to enable the CPS function without allowing the CPS to collect data about the parties placing calls. This specification describes CPS implementations that act specifically on behalf of service providers who will be processing the calls that STIR secures, and thus who will necessarily know the parties communicating, so an alternative security architecture becomes possible. These functions may be crucial to the adoption of STIR in some environments, like legacy non-IP telephone networks, where in-band transmission of PASSporTs may not be feasible.

Environments that might support this flavor of STIR out-of-band include carriers, large enterprises, call centers, or any Internet service that aggregates on behalf of a large number of telephone

endpoints. That last case may include certain classes of gateway or transit providers.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Service Provider Deployment Architecture for Out-of-Band STIR

The architecture in this specification assumes that every participating service provider is associated with one or more designated CPS instances. A service provider's CPS serves as a place where callers, or in some cases gateways, can deposit a PASSporT when attempting to place a call to a subscriber of the destination service provider; if the caller's domain supports in-band STIR, this can be done at the same time as an in-band STIR call is placed. The terminating service provider could operate the CPS themselves, or a third party could operate the CPS on the destination's behalf. This model does not assume a monolithic CPS that acts on behalf of all service providers, but nor does it prohibit multiple service providers from sharing a CPS provider. Moreover, a particular CPS can be a logically distributed entity compromised of several geographically distant entities that flood PASSporTs among themselves to support an anycast-like service.

The process of locating a destination CPS and submitting a PASSporT naturally requires Internet connectivity to the CPS. If the CPS is deployed in the terminating service provider network, any such network connectivity could instead be leveraged by a caller to initiate a SIP session, during which in-band STIR could be used normally. The applicability of this architecture is therefore to those cases where, for whatever reason, SIP requests cannot reliably convey PASSporTs end-to-end, but an HTTP transaction can reliably be sent to the CPS from an out-of-band authentication service (OOB-AS). It is hoped that as IP connectivity between telephone providers increases, there will be less need for an out-of-band mechanism, but it can serve as a fallback mechanism in cases where service providers cannot predict whether end-to-end delivery of SIP calls will occur.

4. Advertising a CPS

If more than one CPS exists for a given deployment, there will need to be some means of discovering CPSs, either administratively or programmatically. Many services providers have bilateral agreements to peer with one another, and in those environments, identifying

their respective CPS's could be a simple matter of provisioning. A consortium of service providers could agree to choose from a list of available CPS providers, say. But in more pluralist environments, some mechanism is needed to discover the CPS associated with the target of a call.

In order to allow the CPS chosen by a service provider to be discovered securely, this specification defines a CPS advertisement. Effectively, a CPS advertisement is a document which contains the URL of a CPS, as well as any information needed to determine which PASSporTs should be submitted to that CPS (e.g., Service Provider Codes (SPCs) or telephone number ranges). An advertisement may be signed with a STIR [RFC8226] credential, or another credential that is trusted by the participants in a given STIR environment. The advantage to signing with STIR certificates is that they contain a "TNAuthList" value indicating the telephone network resources that a service provider controls. This information can be matched with a TNAuthList value in the CPS advertisement to determine whether the signer has the authority to advertise a particular CPS as the proper destination for PASSporTs.

The format of a service provider CPS advertisement consists of a simple JSON object containing one or more pairs of TNAuthList values pointing to the URIs of CPSs, e.g. { "0-1234":"https://cps.example.com" }. The format of this is a hyphen-separated concatenation of the [RFC8226] TNAuthList TNEntry values ("0" for SPC, "1" for telephone number range, "2" for individual telephone numnber) with the TNAuthList value. Note for in case "1", telephone number ranges are expressed by a starting telephone number followed by a count, and the count itself is here also by hyphen-separated from the TN (e.g., "1-15714341000-99"). An advertisement can contain multiple such ranges by adding more pairs. CPS URIs MUST be HTTPS URIs. These CPS URIs SHOULD be publicly reachable, as service providers cannot usually anticipate all of the potential callers that might want to connect with them, but in more constrained environments, they MAY be only reachable over a closed network.

Advertising an SPC may be inappropriate in environments where an originating domains has no ready means to determine whether a given called telephone number falls within a scope of an SPC (such as a national routing database that maps telephone numbers to SPCs). In such environments, TN based advertisements could enable discovery instead. Also, note that PASSporTs can be used to sign communication where the "orig" and/or "dest" are not telephone numbers as such, but instead URI-based identifiers; these PASSporTs typically would not be signed by an [RFC8226] certificate, and future specification would be required to identify URI-based prefixes for CPS advertisements.

CPS advertisements could be made available through existing or new databases, potentially aggregated across multiple service providers and distributed to call originators as necessary. They could be discovered during the call routing process, including through a DNS lookup. They could be shared through a distributed database among the participants in a multilateral peering arrangement.

An alternative to CPS advertisements that may be usable in some environments is adding a field to STIR [RFC8226] certificates identifying the CPS URI issued to individual service providers. As these certificates are themselves signed by a CA, and contain their own TNAuthList, the URI would be bound securely to the proper telephone network identifiers. As STIR assumes a community of relying parties who trust these credentials, this method perhaps best mirrors the trust model required to allow a CPS to authorize PASSporT submission and retrieval.

5. Submitting a PASSporT

Submitting a PASSporT to a CPS as specified in the STIR out-of-band framework [RFC8816] requires security measures which are intended to prevent the CPS from learning the identity of the caller (or callee), to the degree possible. In this service provider case, however, the CPS is operated by the service provider of the callee (or an entity operating on their behalf), and as such the information that appears in the PASSporT is redundant with call signaling that the terminating party will receive anyway. Therefore, the service provider out-of-band framework does not attempt to conceal the identity of the originating or terminating party from the CPS.

An out-of-band authentication service (OOB-AS) forms a secure connection with the target CPS. This may happen at the time a call is being placed, or it may be a persistent connection, if there is a significant volume of traffic sent over this interface. The OOB-AS SHOULD authenticate itself to the CPS via mutual TLS using its STIR credential [RFC8226], the same one it would use to sign calls; this helps mitigate the risk of flooding that more open OOB implementations may face. Furthermore, use of mutual TLS prevents attackers from replaying captured PASSporTs to the CPS. A CPS makes its own policy decision as to whether it will accept calls from a particular OOB-AS, and at what volumes. A CPS can use this mechanism can authorize service providers who already hold STIR credentials to submit PASSporTs to a CPS, but alternative mechanisms would be required for any entities that do not hold a STIR credential, including gateway or transit providers who want to submit PASSporTs. See Section 7 below for more on their behavior.

Service provider out-of-band PASSporTs do not need to be encrypted for storage at the CPS, although use of transport-layer security to

prevent eavesdropping on the connection between the CPS and OOB-ASs is REQUIRED. PASSporTs will typically be submitted to the CPS at the time they are created by an AS; if the PASSporT is also being used for in-band transit within a SIP request, the PASSporT can be submitted to the CPS before or after the SIP request is sent, at the discretion of the originating domain. An OOB-AS will use a REST interface to submit PASSporTs to the CPS as described in [RFC8816] Section 9. PASSporTs persist at the CPS for as long as is required for them to be retrieved (see the next section), but in any event for no longer than the freshness interval of the PASSporT itself (a maximum of sixty seconds).

6. PASSporT Retrieval

The STIR out-of-band framework [RFC8816] proposes two means that called parties can acquire PASSporTs out-of-band: through a retrieval interface, or through a subscription interface. In the service provider context, where many calls to or from the same number may pass through a CPS simultaneously, an out-of-band capable verification service (OOB-VS) may therefore operate in one of two modes: it can either pull PASSporTs from the CPS after calls arrive, or receive push notifications from the CPS for incoming calls.

Pulling of PASSporTs from the CPS will follow the basic REST flow described in [RFC8816] Section 9. In the pull model, a terminating service provider polls the CPS via its OOB-VS after having received a call for which the call signaling does not itself carry a PASSporT. Exactly how a CPS determines which PASSporTs an OOB-VS is eligible to receive over this interface is a matter of local policy. If a CPS serves only one service provider, then all PASSporTs submitted to the CPS are made available to the OOB-VS of that provider; indeed, the CPS and OOB-VS may be colocated or effectively operated as a consolidated system. In a multi-provider environment, the STIR credential of the terminating domain can be used by the CPS to determine the range of TNAuthLists for which an OOB-VS is entitled to receive PASSporTs; this may be through a mechanism like mutual TLS, or through using the STIR credential to sign a token that is submitted to the CPS by the retrieving OOB-VS. Note that a multi-provider CPS will need to inspect the "dest" element of a PASSporT to determine which OOB-VS should receive the PASSporT.

In a push model, an OOB-VS could for example subscribe to a range of telephone numbers or SPCs, which will be directed to that OOB-VS by the CPS (provided the OOB-VS is authorized to receive them by the CPS). PASSporT might be sent to the OOB-VS either before or after unsigned call signaling has been received by the terminating domain. In either model, the terminating side may need to delay rendering a call verification indicator when alerting, in order to await the potential arrival of a PASSporT at the OOB-VS. The exact timing of

this, and its interaction with the substitution attack described in [RFC8816] Section 7.4, is left for future work.

7. Gateways

In some deployment architectures, gateways might perform a function that interfaces with a CPS for the retrieval or storage of PASSporTs, especially in cases when in-band STIR service providers need to exchange secure calls with providers that can only be reached by STIR out-of-band. For example, a closed network of in-band STIR providers may send SIP INVITEs to a gateway in front of a traditional PSTN tandem that services a set of legacy service providers. In that environment, a gateway might extract a PASSporT from an in-band SIP INVITE and store it in a CPS that was established to handle requests for one or more legacy providers, who in turn consume those PASSporTs through an OOB-VS to assist in robocall mitigation and similar functions.

The simplest way to implement a gateway performing this sort of function for a service provider CPS system is to issue credentials to the gateway that allow it to act on behalf of the legacy service providers it supports: this would allow it to both add PASSporTs to the CPS acting on behalf of the legacy providers, and also to create PASSporTs for in-band STIR conveyance from the legacy-providers to terminating service providers in the closed STIR network. For example, a service provider could issue a delegate certificate [RFC9060] for this purpose.

8. Acknowledgments

We would like to thank Alex Fenichel for contributions to this specification.

9. IANA Considerations

This memo includes no request to IANA.

10. Security Considerations

The Security Considerations of [RFC8816] apply to this document as well, including concerns about potential denial-of-service vectors and traffic analysis. However, that specification's model focused a great deal on the privacy implications of uploading PASSporTs to a third-party web service. This draft mitigates those concerns by making the CPS one of the parties to call setup (or an entity contractual acting on their behalf). That said, any architecture in which PASSporTs are shared with a federated or centralized CPS raises potential concerns about data collection [RFC7258].

Unlike [RFC8816], this document proposes the use of STIR certificates to authenticate transactions with a CPS as well as signatures for CPS advertisements. This presumes an environment where STIR certificates are issued by trust anchors which are already trusted by the CPS, potentially to gateways and similar services. Common STIR deployments use Service Provider Codes (SPCs) instead of telephone numbers ranges to identify service providers today; determining whether a given SPC entitles a service provider to access PASSporTs for a given telephone number is not trivial, but is a necessary component of this CPS architecture. If anyone with a STIR certificate is able to publish or access PASSporTs for any telephone number, this would create an intolerable security and privacy vulnerability.

11. References

11.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8224] Peterson, J., Jennings, C., Rescorla, E., and C. Wendt, "Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 8224, DOI 10.17487/RFC8224, February 2018, <https://www.rfc-editor.org/info/rfc8224>.

[RFC8225] Wendt, C. and J. Peterson, "PASSporT: Personal Assertion Token", RFC 8225, DOI 10.17487/RFC8225, February 2018, <https://www.rfc-editor.org/info/rfc8225>.

[RFC8226] Peterson, J. and S. Turner, "Secure Telephone Identity Credentials: Certificates", RFC 8226, DOI 10.17487/RFC8226, February 2018, <https://www.rfc-editor.org/info/rfc8226>.

[RFC8816] Rescorla, E. and J. Peterson, "Secure Telephone Identity Revisited (STIR) Out-of-Band Architecture and Use Cases", RFC 8816, DOI 10.17487/RFC8816, February 2021, <https://www.rfc-editor.org/info/rfc8816>.

11.2. Informative References

[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>.

[RFC9060] Peterson, J., "Secure Telephone Identity Revisited (STIR) Certificate Delegation", RFC 9060, DOI 10.17487/RFC9060, September 2021, <https://www.rfc-editor.org/info/rfc9060>.

Author's Address

Jon Peterson
Neustar, Inc.

Email: jon.peterson@team.neustar