WG Working Group
Internet-Draft
Intended status: Standards Track
Expires: 9 March 2026

R. Sliwa
C. Wendt
Somos Inc.

5 September 2025

Transparent Discovery of STIR Out-of-Band Call Placement Services
draft-sliwa-stir-oob-transparent-discovery-00

Abstract

This document defines a Discovery Service for STIR Out-of-Band (OOB) Call Placement Services (CPS). The Discovery Service enables Authentication Services (AS) and Verification Services (VS) to quickly determine which CPS is responsible for a given telephone number (TN) or Service Provider Code (SPC), allowing retrieval of PASSporTs even when SIP Identity headers are removed by non-IP or hybrid network segments. The Discovery Service leverages a CPS URI certificate extension, which allows STIR Certificates or Delegate Certificates to embed an HTTPS URI for the CPS serving the TNs or SPCs covered by the certificate.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://github.com/appliedbits/draft-sliwa-stir-oob-transparent-discovery. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-sliwa-stir-oob-transparent-discovery/.

Discussion of this document takes place on the Secure Telephone Identity Revisited Working Group mailing list (mailto:stir@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/stir/. Subscribe at https://www.ietf.org/mailman/listinfo/stir/.

Source for this draft and an issue tracker can be found at https://github.com/appliedbits/draft-sliwa-stir-oob-transparent-discovery.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

This Internet-Draft will expire on 9 March 2026.

Copyright Notice

Table of Contents

1. Introduction

In a STIR ecosystem, defined primarily by [RFC8224], [RFC8225], and [RFC8226], and specifically when enabling Out-of-Band (OOB) delivery of PASSporTs defined in [RFC8816], a Call Placement Service (CPS) plays a vital role, particularly when SIP Identity headers are lost or removed in non-IP or hybrid network environments. While the role of CPS was well established in [RFC8816], the challenge remained for the definition of discovering which CPS is responsible for a specific telephone number (TN) or Service Provider Code (SPC) in a secure, scalable, and interoperable way.

This document introduces a CPS Discovery Service designed to solve that challenge. The CPS Discovery Service provides a transparent and cryptographically verifiable method for identifying the correct CPS for any given TN or SPC identified in the TNAuthList of a STIR certificate defined in [RFC8226], supporting OOB call authentication without requiring static configuration or bilateral agreements between service providers.

The CPS Discovery Service operates by leveraging the CPS URI certificate extension defined in [I-D.sliwa-stir-cert-cps-ext]. This extension allows STIR Certificates [RFC8226] or Delegate Certificates [RFC9060] to encode an HTTPS URI pointing to the CPS responsible for the TNs or SPCs listed in the certificate’s TNAuthList. Once such certificates are published to STIR Certificate Transparency (STI-CT) logs defined in [I-D.wendt-stir-certificate-transparency], the CPS URI becomes immediately visible, auditable, and publicly verifiable by relying parties.

To facilitate CPS discovery, the Discovery Service continuously monitors these CT logs, extracts CPS URIs from newly issued or updated certificates, and registers mappings from TNs or SPCs to CPS endpoints. These mappings are exposed via a simple REST API that supports fast, automated lookups by Authentication Services (AS) and Verification Services (VS).

By combining CPS URI certificate extensions with CT monitoring and a queryable discovery interface, this approach enables automatic OOB CPS discovery. It can integrate with existing STIR framework components and requires only an additional lookup step to improve the robustness and scalability of Out-of-Band PASSporT delivery.

2. Conventions and Definitions

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. Architectural Overview

This document defines a mechanism for discovering Call Placement Services (CPS) responsible for specific telephone numbers (TNs) or Service Provider Codes (SPCs) by monitoring STI Certificate Transparency (STI-CT) logs for certificates that include a CPS URI extension.

Entities that operate a CPS obtain delegate certificates with TNAuthList entries covering the TNs or SPCs they serve. These certificates include a CPS URI extension as defined in [I-D.sliwa-stir-cert-cps-ext], indicating the HTTPS endpoint of the CPS. Once issued, these certificates are submitted to STI-CT logs.

Any relying party may monitor STI-CT logs for new or updated certificates containing a CPS URI extension. Upon detection, the CPS URI and its associated TNAuthList entries are extracted and recorded. This enables parties to associate TNs or SPCs with corresponding CPS URIs based on the content of logged certificates.

This approach provides the following properties:

* Transparency: CPS endpoint declarations are logged and auditable through STI-CT.

* Verifiability: Mappings are derived from signed certificates anchored in existing STIR trust infrastructure and supported by Signed Certificate Timestamps (SCTs).

* No bilateral provisioning: Originating and terminating parties do not require prior agreement or static configuration to determine the correct CPS.

* Compatibility: The mechanism is fully compatible with the STIR Out-of-Band (OOB) architecture as defined in [RFC8816] and requires no modification to existing CPS publish or retrieve interfaces.

While this discovery mechanism is inherently distributed, relying solely on STI-CT log monitoring and information published in signed certificates, it does not preclude the existence of centralized or convenience-based services that aggregate CPS URI data. Such services may offer simplified access patterns, enhanced performance, or monitoring utilities for relying parties. However, any such intermediary or cache-based service MUST preserve the verifiable nature of the CPS URI bindings by exposing the original certificate, Signed Certificate Timestamps (SCTs), and associated TNAuthList values. Consumers of CPS discovery data SHOULD validate the integrity and provenance of this information using the underlying CT log entries and certificate signatures, as defined in this document and related STIR specifications.

4. Components

The discovery mechanism relies on existing STIR framework components and STI-CT logs. No new interfaces are required between entities. CPS operators signal the location of their service using a certificate extension, and relying parties extract and verify these declarations by monitoring CT logs.

4.1. Call Placement Service (CPS)

A Call Placement Service (CPS), as defined in [RFC8816], is a network-accessible endpoint that stores PASSporTs for later retrieval during call verification. CPSs are used when SIP Identity headers are removed or unavailable, such as in non-IP or hybrid telephony environments. Originating entities publish PASSporTs to the CPS associated with the called party’s number, and terminating entities retrieve them during call processing.

This specification does not modify the behavior or interfaces of CPS endpoints. It only describes how CPS endpoint information is published and discovered using STIR certificates and delegate certificates and STI-CT.

4.2. Certificate Holders

Entities responsible for telephone numbers or SPCs, such as service providers or enterprises, obtain STIR certificates or delegate certificates with TNAuthList entries covering those resources. These certificates may optionally as defined in this document include a CPS URI extension indicating the HTTPS endpoint of the CPS that serves those numbers to facilitate discovery.

When these certificates are submitted to a recognized STI-CT log, the CPS URI becomes visible to relying parties monitoring the log. This allows third parties to discover the CPS associated with a number without requiring pre-provisioning or bilateral configuration.

4.3. Transparency Log Monitors

Any party may monitor STI-CT logs for certificates containing a CPS URI extension. Upon detecting a new or updated certificate, the monitor performs the following:

* Verifies the certificate chain to a trusted STI root
* Validates the certificate’s Signed Certificate Timestamps (SCTs)
* Extracts the TNAuthList and CPS URI from the certificate
* Associates the covered TNs or SPCs with the indicated CPS URI

Monitors may use this data to maintain a local registry or cache of TN to CPS and SPC to CPS mappings. These mappings can be used by Authentication Services or Verification Services during call processing.

5. CPS Discovery Mechanisms

This section describes the mechanism by which Call Placement Service (CPS) information is discovered through monitoring of STI-CT logs. This method provides a distributed, cryptographically verifiable, and interoperable means of associating telephone numbers (TNs) or Service Provider Codes (SPCs) with CPS endpoints.

5.1. Certificate-Based CPS Publication

CPS operators often associated with entities authorized for telephone numbers or SPCs obtain STIR certificates or delegate certificates containing a TNAuthList and the CPS URI certificate extension as defined in [I-D.sliwa-stir-cert-cps-ext]. The CPS URI identifies the CPS HTTPS endpoint where Out-of-Band (OOB) PASSporTs can be published or retrieved for the associated identifiers.

These certificates are submitted to one or more recognized STI-CT logs. Each submission yields a Signed Certificate Timestamp (SCT), which proves inclusion in the log and enables public verification.

5.2. Discovery via Log Monitoring

Relying parties (e.g., Authentication Services, Verification Services, or intermediary discovery components) monitor STI-CT logs for new or updated certificates that include a CPS URI extension. Upon detection, the monitor performs the following steps:

1. Verifies the certificate chain to a trusted STI root.

2. Validates the SCT(s) associated with the certificate.

3. Extracts the TNAuthList and the CPS URI extension.

4. Associates the covered TNs or SPCs with the CPS URI.

The resulting mappings are used to determine the appropriate CPS endpoint during call placement and verification. This process allows discovery to be performed in real-time or asynchronously using CT log clients, without requiring direct interaction with the certificate holder or CPS operator.

6. End-to-End Process Summary

1. A STIR certificate or delegate certificate is issued containing TNAuthList and CPS URI.

2. The certificate is logged in an STI-CT log, generating SCTs.

3. A monitoring system observes the log and extracts TN-CPS and SPC-CPS mappings.

4. Authentication or Verification Services consult the mappings to identify the CPS endpoint corresponding to a given TN or SPC.

5. PASSporTs are published or retrieved using the discovered CPS URI as part of the OOB authentication process.

This approach removes the need for authoritative registries, REST-based discovery interfaces, or bilateral provisioning agreements. All discovery is based on cryptographic credentials and public transparency logs, ensuring an auditable and interoperable discovery process.

7. Expected Monitor Behavior

Parties that wish to perform CPS discovery may monitor one or more STI-CT logs for delegate certificates containing the CPS URI extension. Monitors are expected to:

* Validate certificate chains to STI trust anchors.

* Verify inclusion of certificates via Signed Certificate Timestamps (SCTs).

* Extract the CPS URI and TNAuthList from certificates.

* Associate telephone numbers or SPCs with the declared CPS URI.

Monitors may use this information to enable Authentication Services (AS) or Verification Services (VS) to locate the appropriate CPS endpoint. Implementations may maintain local caches or registries based on the extracted data, respecting certificate validity periods and revocation status when available.

8. Security Considerations

The CPS discovery mechanism relies on the integrity of STIR delegate certificates and STI-CT logs. Several security considerations apply:

* Misissued Certificates: A CPS URI could be falsely claimed in a certificate. Relying parties must validate that certificates are issued by trusted STIR Certification Authorities and verify TNAuthList accuracy during issuance.

* Log Misbehavior: CT logs may omit or backdate entries. Implementations should monitor multiple CT logs and validate Signed Certificate Timestamps (SCTs) to ensure visibility and integrity.

* Stale or Revoked Certificates: CPS mappings derived from expired or revoked certificates may lead to incorrect routing. Implementations should check certificate validity and revocation status before using extracted mappings.

* Information Exposure: CPS URIs and TNAuthList entries are publicly logged. This may reveal operational details but does not introduce new exposures beyond existing STIR practices.

This mechanism inherits the security properties of the STIR certificate infrastructure and CT logging, offering verifiable, auditable discovery without requiring bilateral trust.

9. IANA Considerations

This document has no IANA actions.

10. Normative References

[I-D.sliwa-stir-cert-cps-ext]
ナ嗟iwa, R. and C. Wendt, "Call Placement Service (CPS) URI Certificate Extension for STI Certificates", Work in Progress, Internet-Draft, draft-sliwa-stir-cert-cps-ext-00, 5 September 2025, <https://datatracker.ietf.org/doc/html/draft-sliwa-stir-cert-cps-ext-00>.

[I-D.wendt-stir-certificate-transparency]
Wendt, C., ナ嗟iwa, R., Fenichel, A., and V. A. Gaikwad, "STI Certificate Transparency", Work in Progress, Internet-Draft, draft-wendt-stir-certificate-transparency-06, 11 June 2025, <https://datatracker.ietf.org/doc/html/draft-wendt-stir-certificate-transparency-06>.

[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/rfc/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/rfc/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/rfc/rfc8224>.

[RFC8225] Wendt, C. and J. Peterson, "PASSporT: Personal Assertion Token", RFC 8225, DOI 10.17487/RFC8225, February 2018, <https://www.rfc-editor.org/rfc/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/rfc/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/rfc/rfc8816>.

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

Acknowledgments

TODO acknowledge.

Authors' Addresses

Rob Sliwa
Somos Inc.
United States of America
Email: robjsliwa@gmail.com

Chris Wendt
Somos Inc.
United States of America
Email: chris@appliedbits.com