Secure Telephone Identity Revisited
Internet-Draft
Intended status: Standards Track
Expires: 7 May 2026

R. Sliwa
C. Wendt
Somos Inc.

3 November 2025

Call Placement Service (CPS) URI Certificate Extension for STI Certificates
draft-sliwa-stir-cert-cps-ext-01

Abstract

This document specifies a non-critical X.509 v3 certificate extension that conveys the HTTPS URI of a Call Placement Service (CPS) associated with the telephone numbers authorized in a STIR Delegate Certificate. The extension enables originators and verifiers of STIR PASSporTs to discover, with a single certificate lookup, where Out-of-Band (OOB) PASSporTs can be retrieved. The mechanism removes bilateral CPS provisioning, allows ecosystem-scale discovery backed by STI Certificate Transparency (STI-CT), and is fully backward compatible with existing STIR certificates and OOB APIs.

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-cert-cps-ext. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-sliwa-stir-cert-cps-ext/.

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-cert-cps-ext.

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/.

Copyright Notice

Table of Contents

1. Introduction

The STIR (Secure Telephone Identity Revisited) framework provides a means of cryptographically asserting the identity of the calling party in a telephone call by using PASSporTs carried in SIP requests, as defined in [RFC8224] and [RFC8225]. To support deployment in environments where SIP Identity headers may be removed or are not end-to-end transmittable, such as in non-IP or hybrid telephony networks, the STIR Out-of-Band (OOB) mechanism was introduced in [RFC8816]. In OOB scenarios, PASSporTs are published to a Call

Placement Service (CPS) where they may be retrieved independently of the SIP signaling path.

To enable discovery of the appropriate CPS for a given telephone number or SPC, this document defines a certificate extension that binds a CPS URI to the identity resources listed in the TNAuthList of the STI certificate. This CPS URI extension provides a verifiable association between a number resource and its corresponding CPS, enabling relying parties to discover CPS endpoints by observing STI Certificate Transparency (STI-CT) logs defined in [I-D.wendt-stir-certificate-transparency].

This specification defines the syntax and semantics of the CPS URI certificate extension, describes how it is encoded in [X.509] certificates also defined in [RFC5280], and outlines validation procedures for Certification Authorities and relying parties. This extension is intended to be used in conjunction with existing STIR certificates defined in [RFC8226] and delegate certificates defined in [RFC9060] infrastructure, and supports enhanced transparency and automation in OOB PASSporT routing.

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. The id-pe-oobURI Certificate Extension

This [X.509] extension is non-critical, applicable only to end-entity certificates, and defined with ASN.1 [X.680] [X.681] [X.682] [X.683] later in this section.

This extension is intended for use in end-entity STI certificates [RFC8226] and delegate certificates [RFC9060] that include TNAuthList values authorizing the use of specific telephone numbers or Service Provider Codes (SPCs). The OOB URI extension provides a means for the certificate holder to declare the HTTPS endpoint of a Call Placement Service (CPS) defined in [RFC8816] that can be used to publish or retrieve PASSporTs for the covered resources.

The presence of this extension allows relying parties to discover the CPS associated with a given telephone number without relying on static configuration or bilateral agreements. This facilitates scalable and verifiable Out-of-Band PASSporT delivery as defined in [RFC8816], using information already published in publicly logged STI certificates.

The extension is encoded as a sequence of IA5Strings containing absolute HTTPS URIs and is identified by an object identifier (OID) assigned in the PKIX id-pe arc. Additional details about the encoding, semantics, and validation rules for the OOB URI list are defined in the sections below.

3.1. ASN.1 Module Syntax

The extension ASN.1 module is defined as follows:

```
OOB-CERT-EXTENSION DEFINITIONS EXPLICIT TAGS ::=
BEGIN

id-pe OBJECT IDENTIFIER ::=
  { iso(1) identified-organization(3) dod(6) internet(1)
    security(5) mechanisms(5) pkix(7) 1 }

id-pe-oobURI OBJECT IDENTIFIER ::= { id-pe TBD }

OOBURIs ::= SEQUENCE SIZE (1..MAX) OF IA5String

END
```

Certificates containing a OOBURI that is not an absolute HTTPS URI as defined in [RFC3986] MUST be considered invalid by relying parties.

Note: The numeric assignment TBD is temporary. IANA will allocate a permanent arc under "PKIX SubjectPublicKeyInfo Certificate Extensions" during RFC publication.

3.2. Extension Semantics

Each IA5String value in the sequence MUST be an absolute URI [RFC3986] that:

* Uses the "https" scheme.

* Identifies the root of the CPS HTTPS API interface (e.g., "https://cps.example.net/oob/v1").

The sequence MUST contain at least one URI. Producers MAY include multiple URIs to provide resiliency or geographic locality information.

3.3. Criticality

The extension MUST be marked non-critical so that implementations that do not understand it can still validate the certificate.

3.4. Processing Rules

* A STIR Authentication Service (AS), defined in [RFC8224], that holds a Delegate Certificate containing id-pe-cpsURI SHOULD publish OOB PASSporTs to the indicated CPS.

* A STIR Verification Service (VS), defined in [RFC8224] that receives a PASSporT signed by such a certificate MAY derive the CPS endpoint by reading the extension, or MAY query an external discovery directory that is populated by monitoring the STI-CT logs.

* If the extension and an external directory disagree, verifiers SHOULD treat the call as unverifiable unless local policy states otherwise.

Relying parties SHOULD ensure that the certificate containing the CPS URI is present in a trusted Certificate Transparency log before using the URI for OOB operations.

4. Use with Out-of-Band

Figure 1 shows the message flow when the extension is present:

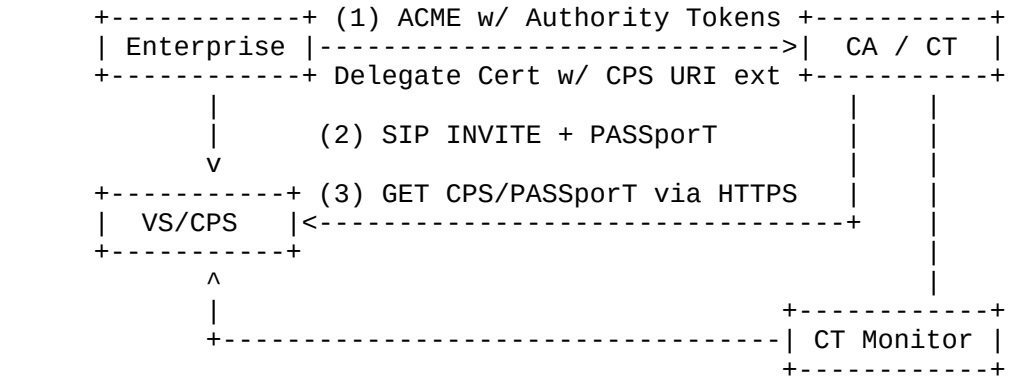

Figure 1

1. The enterprise obtains a Delegate Certificate containing the CPS URI. The CA submits the certificate to STI-CT.

2. On each call, the AS signs a PASSporT with Delegate Certificate containing SCT.

3. The terminating VS reads the CPS URI from the certificate and fetches the PASSporT.

5. Operational Considerations

* Logging: CAs issuing certificates with id-pe-cpsURI MUST submit the certificate to STI-CT logs.

* Rotation: Changing a CPS hostname or path requires certificate re-issuance. Operators SHOULD minimize TTLs on old URIs during migration.

* Monitoring: Relying parties and CPS discovery services SHOULD monitor trusted STI-CT logs for new or updated CPS URI declarations to ensure timely access and detect misconfiguration.

6. Security Considerations

The CPS URI certificate extension introduces a mechanism for associating telephone number resources with CPS endpoints through STI certificates. The following considerations apply:

* Misuse or Misissuance: A malicious or misconfigured entity may include a CPS URI in a certificate without authorization for the corresponding TNAuthList resources. Certification Authorities (CAs) MUST validate that the entity requesting the certificate has authority over the listed numbers or SPCs before issuing the certificate.

* URI Integrity: The CPS URI is not digitally signed independently of the certificate. Relying parties MUST validate the entire certificate chain and ensure the certificate is properly logged in a Certificate Transparency log before using the URI.

* Certificate Expiry and Revocation: CPS URI information may become outdated due to certificate expiration or revocation. Relying parties SHOULD evaluate certificate validity and revocation status when interpreting CPS mappings.

* Log Availability and Monitoring: Relying parties that depend on CT log monitoring for CPS discovery SHOULD monitor multiple trusted logs to ensure timely detection of CPS declarations and prevent omission attacks.

* Information Exposure: The publication of CPS URIs in publicly logged certificates may reveal deployment metadata. This exposure is consistent with existing STIR delegate certificate practices and does not introduce additional privacy risk beyond what is already present in TNAuthList usage.

7. IANA Considerations

IANA is requested to assign a new object identifier (OID) for the CPS URI certificate extension in the "PKIX Extension Registry" as follows:

* Name: id-pe-oobURI

* OID: to be assigned

* Description: Certificate extension for specifying a Call Placement Service (CPS) URI for STIR Out-of-Band PASSporTs

* Reference: This document

8. Normative References

[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>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <https://www.rfc-editor.org/rfc/rfc3986>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/rfc/rfc5280>.

[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>.

[X.509] International Telecommunication Union, "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks", ITU-T Recommendation X.509, ISO/IEC 9594-8, October 2016, <https://www.itu.int/rec/T-REC-X.509>.

[X.680] International Telecommunication Union, "Information Technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation", ITU-T Recommendation X.680, ISO/IEC 8824-1, August 2015, <https://www.itu.int/rec/T-REC-X.680>.

[X.681] International Telecommunication Union, "Information Technology - Abstract Syntax Notation One (ASN.1): Information object specification", ITU-T Recommendation X.681, ISO/IEC 8824-2, August 2015, <https://www.itu.int/rec/T-REC-X.681>.

[X.682] International Telecommunication Union, "Information Technology - Abstract Syntax Notation One (ASN.1): Constraint specification", ITU-T Recommendation X.682, ISO/IEC 8824-3, August 2015, <https://www.itu.int/rec/T-REC-X.682>.

[X.683] International Telecommunication Union, "Information Technology - Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications", ITU-T Recommendation X.683, ISO/IEC 8824-4, August 2015, <https://www.itu.int/rec/T-REC-X.683>.

Acknowledgments

TODO acknowledge.

Authors' Addresses

Rob Sliwa
Somos Inc.
Email: robjsliwa@gmail.com

Chris Wendt
Somos Inc.
Email: chris@appliedbits.com