Secure Telephone Identity Revisited
Internet-Draft
Intended status: Standards Track
Expires: 2 October 2026

C. Wendt
R. ナ嗟iwa
Somos, Inc.

31 March 2026

VESPER - Verifiable STI Presentation and Evidence for RTU
draft-wendt-stir-vesper-07

Abstract

This document defines VESPER (Verifiable STI Presentation and Evidence for RTU), a framework that extends the STIR architecture to cryptographically bind telephone number authority, domain identity, and originating provider authorization in a single delegate certificate. The delegate certificate is issued under the certificate policy defined under a STIR compliant eco-system and carries the assigned telephone numbers and authorized originating providers in a TNAuthList extension, the responsible entity’s domain in a SubjectAltName, and an embedded Signed Certificate Timestamp (SCT) proving the certificate was recorded in a public transparency log prior to use. VESPER enables relying parties to verify that a telephone number was assigned to the entity whose domain is presented, and that calls from those numbers are originated by an authorized originating provider.

The framework defines a certificate profile and issuance process grounded in existing STIR and ACME authority token mechanisms, a domain-hosted certificate repository with domain-controlled certificate discovery enabling cross-channel trust signals, a PASSporT usage profile for SIP signaling, and certificate transparency to support ecosystem auditability and detection of mis-issuance.

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 2 October 2026.

Table of Contents

1. Introduction

The Secure Telephone Identity (STI) architecture, based on STI certificates [RFC8226], PASSporTs [RFC8225], and the SIP Identity header field [RFC8224], provides cryptographic integrity protection for calling information in real-time communications. These mechanisms enable relying parties to verify that a telephone number was not modified in transit and that it was signed using credentials authorized for that number. However, the STI architecture does not define how to verify that a telephone number is being used by the entity it was assigned to, nor does it provide a way to identify which originating providers are authorized to place calls from those numbers.

In practice, telephone numbers appear across a wide range of digital contexts: in SIP signaling, on websites, in SMS and rich communication messages, and in email. Today, there is no standard mechanism for a relying party to verify that the entity asserting a telephone number is the same entity it was assigned to, or to confirm that an originating provider is one of the legitimate originators authorized for that number. This gap enables impersonation, unauthorized origination, and the presentation of misleading contact information across digital channels.

VESPER addresses this by defining a delegate certificate that serves as a single, auditable trust artifact binding three things: the telephone numbers assigned to the responsible entity, the domain that entity controls and for which it holds certificate credentials, and the set of originating providers enabled as legitimate originators for calls from those telephone numbers. Because this binding is expressed in a standard X.509 certificate subject to the certificate policy defined in [RFC8226], it can be validated using widely deployed PKI mechanisms and recorded in a transparency system for ecosystem auditability.

This document defines the certificate profile, the certificate repository and domain-controlled certificate discovery mechanism, the PASSporT usage profile, and the relationship to origination policy distribution.

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. Overview

3.1. The VESPER Delegate Certificate

The VESPER framework is built around a delegate certificate issued to the entity that holds the right-to-use for one or more telephone numbers. This certificate is issued under the certificate policy defined in [RFC8226], whose trust anchors govern the authority chain. The delegate certificate represents the issued credentials that bind telephone number authority to the assigned entity, which also holds domain credentials as a corroborating identity signal. Trust assertions in VESPER are expressions of what is certified in this credential, validated against the trust anchors defined in [RFC8226] through the certificate chain.

The certificate carries the following:

* Telephone number authority: one or more telephone numbers (or ranges) in the TNAuthList extension, representing the entity's right-to-use as assigned by a responsible provider or organization. The authority chain is established via a TNAuthList Authority Token issued by that responsible provider or organization and validated through the STI certificate chain.

* Originating provider enablement: one or more service provider codes (SPCs) in the same TNAuthList extension, identifying the originating providers authorized to originate calls from those telephone numbers. Both TN entries and SPC entries MAY appear together in a single TNAuthList, as permitted by [RFC8226].

* Domain credential: a DNS domain name in the SubjectAltName extension (dNSName), representing a domain the entity controls and for which it holds WebPKI credentials. This domain provides a corroborating identity signal that is independent of the telephone number ecosystem and enables certificate discovery via the repository defined in this document.

* Optional claim constraints: JWTClaimConstraints [RFC8226] and/or EnhancedJWTClaimConstraints [RFC9118] extensions, authorizing additional PASSporT claims (such as Rich Call Data) and optionally constraining their values. These constraints are backed by a JWTClaimConstraints Authority Token issued in accordance with [I-D.ietf-acme-authority-token-jwtclaimcon].

* Transparency: a Signed Certificate Timestamp (SCT) embedded in the certificate, proving that the certificate was submitted to and recorded in a transparency log before use.

Short-lived certificates MUST be used. Implementations MUST support the profile in [I-D.ietf-stir-certificates-shortlived] and MUST convey the certificate chain inline using the x5c header parameter and MUST include the x5u header parameter referencing the certificate at its domain-controlled repository location.

3.2. Domain as a Corroborating Trust Credential

Prior STIR specifications establish telephone number authority through the TNAuthList but do not bind that authority to the real-world entity to which the number was assigned. VESPER addresses this by also recording a domain credential held by that entity, a domain the entity controls and for which it holds WebPKI certificate credentials.

The domain in the delegate certificate SubjectAltName corresponds to a domain the entity controls. Control of that domain, established through the entity’s ability to obtain certificate credentials for it, provides a corroborating identity signal that is independent of the telephone number ecosystem. When a relying party validates a VESPER delegate certificate, it obtains verifiable evidence that a specific entity, which holds those domain credentials, has been assigned the telephone numbers in the certificate by a responsible provider or organization.

3.3. User Identity and Delegation

The VESPER delegate certificate authorizes the entity that holds it to use the telephone numbers it contains. Within that entity, individual users or automated agents may be further authorized to originate communications using those numbers through mechanisms defined by the entity’s own governance, such as sub-credentials or access control policies, without those individuals being identified in the delegate certificate itself. A single telephone number may be authorized for use by multiple users or agents, as is common in shared lines and call center deployments. The delegate certificate identifies the entity that holds the right-to-use for the telephone numbers it contains, not the individual users or agents originating communications on behalf of that entity. Where caller identity at the individual level is desired, mechanisms such as Rich Call Data [RFC9795] or other PASSporT extensions provide optional paths for conveying that information.

3.4. Certificate Repository and Domain-Controlled Certificate Discovery

An entity that holds a VESPER delegate certificate MUST publish that certificate at a stable HTTPS location under its domain. The specific path is not prescribed; any HTTPS URL whose domain matches the dNSName SubjectAltName of the delegate certificate is valid. The TLS certificate on the hosting server MUST match the dNSName SubjectAltName of the VESPER delegate certificate, validated through standard WebPKI TLS. No cross-signing between the STI delegate certificate and the web TLS certificate is required or defined.

This specification defines two token representations derived from the delegate certificate: a PASSporT as defined in [RFC8225] for use in SIP signaling, and a basic JWT form that provides portable proof of right-to-use for a telephone number in contexts outside of SIP signaling, such as cases where a traditional letter of authorization or other evidence of TN association is required. Each is defined in detail in the sections below.

4. VESPER Roles and Certificate Issuance

4.1. Roles

The VESPER framework defines the following functional roles.

1. Domain Operator: the entity that controls a domain and holds the right-to-use for one or more telephone numbers. The Domain Operator is the subject of the VESPER delegate certificate, publishes the certificate at a stable HTTPS location under its domain, and uses the delegate certificate’s private key to sign PASSporTs and RTU Tokens.

2. Right-to-Use (RTU) Authority: the responsible provider or organization that allocates telephone numbers and issues TNAuthList Authority Tokens as RTU evidence for delegate certificate issuance (e.g., a TNSP or RespOrg).

3. STI Certification Authority (STI CA): issues VESPER delegate certificates after validating RTU evidence and domain association, operating under the certificate policy defined in [RFC8226].

4. Transparency Log Operator: records issued delegate certificates and returns SCTs to support ecosystem auditability and detection of mis-issuance.

4.2. Delegate Certificate Issuance Process

In the VESPER framework, a delegate certificate is issued through the following sequence:

1. The RTU Authority produces a TNAuthList Authority Token representing the right-to-use for the telephone number(s) being assigned. The STI CA operates under a certificate policy that recognizes the RTU Authority's authority to make this assignment.

2. The certificate subject generates a CSR and presents it to the STI CA along with the TNAuthList Authority Token, validated via ACME mechanisms as defined in [RFC9447], [RFC9448], and [I-D.ietf-acme-authority-token-jwtclaimcon]. If additional PASSporT claims are to be authorized (e.g., Rich Call Data [RFC9795]), a JWTClaimConstraints Authority Token [I-D.ietf-acme-authority-token-jwtclaimcon] is also presented; the STI CA MUST NOT widen the constraints specified in that token.

3. Upon successful validation, the STI CA issues a delegate certificate. STI CAs SHOULD issue short-lived certificates as specified in [I-D.ietf-stir-certificates-shortlived], and subjects SHOULD automate renewal.

4. The issued certificate MUST be submitted to a transparency log as defined in [I-D.ietf-stir-certificate-transparency]. The resulting SCT MUST be embedded in the certificate prior to deployment.

The issued delegate certificate MUST include:

* A TNAuthList extension [RFC8226], representing the telephone number(s) the certificate holder is authorized to use and, where applicable, the SPC(s) of authorized originating providers. TN entries and SPC entries MAY appear together in a single TNAuthList extension.

If the certificate is intended to authorize additional PASSporT claims beyond [RFC8225], it MUST also include:

* A JWTClaimConstraints extension [RFC8226] and/or EnhancedJWTClaimConstraints extension [RFC9118].

4.3. VESPER Certificate Profile

VESPER delegate certificates MUST conform to the STIR certificate profile in [RFC8226] and MUST support the short-lived certificate profile in [I-D.ietf-stir-certificates-shortlived]. The certificate MUST contain the following:

* Subject: SHOULD include an Organization (O) field reflecting the entity's name.

* SubjectAltName: MUST include a dNSName entry carrying the entity's domain. This domain MUST be DNS-resolvable and MUST match the domain of the certificate repository host.

* TNAuthList [RFC8226]: MUST include one or more TN entries representing telephone numbers assigned to the certificate subject, and MAY include one or more SPC entries identifying authorized originating providers. TN and SPC entries MAY appear together in a single TNAuthList extension.

* SCT: MUST include an embedded Signed Certificate Timestamp as defined in [I-D.ietf-stir-certificate-transparency], proving the certificate was submitted to a transparency log prior to deployment. Relying parties MUST validate the embedded SCT as part of certificate validation.

* JWTClaimConstraints [RFC8226] and/or EnhancedJWTClaimConstraints [RFC9118] (OPTIONAL): MUST be present if the certificate is intended to authorize PASSporT claims beyond [RFC8225]. The STI CA MUST NOT widen the constraints specified in the JWTClaimConstraints Authority Token.

CAs SHOULD issue certificates with short validity intervals as specified in [I-D.ietf-stir-certificates-shortlived], and subjects SHOULD automate renewal.

4.4. VESPER Authentication and Verification Procedures

These procedures extend the baseline STIR authentication and verification models defined in [RFC8224], [RFC8225], and [RFC8226].

4.4.1. Authentication Service Behavior

When originating a call or message, the Authentication Service:

* Constructs a PASSporT containing orig, dest, iat, and any optional claims authorized by JWTClaimConstraints in the certificate.

* Signs the PASSporT using a VESPER delegate certificate whose TNAuthList authorizes the orig telephone number and that contains an embedded SCT.

* Conveys the certificate chain inline using the x5c header parameter.

* Includes the x5u header parameter containing the HTTPS URL of the delegate certificate at its location in the domain-controlled repository.

4.4.2. Verification Service Behavior

Upon receiving a PASSporT, the Verification Service MUST:

* Validate the PASSporT signature.

* Validate the certificate trust chain against the trust anchors defined in [RFC8226] using the x5c header parameter.

* Confirm the TNAuthList extension authorizes the orig telephone number.

* Validate the embedded SCT.

* If JWTClaimConstraints or EnhancedJWTClaimConstraints extensions are present, verify that all asserted claims conform to those constraints.

* Confirm that the domain in the x5u URL matches the dNSName SubjectAltName of the signing certificate.

The PASSporT MUST be rejected if any of the above checks fail.

4.4.3. Connected Identity

When VESPER is used with Connected Identity [I-D.ietf-stir-rfc4916-update], the destination party returns a PASSporT of type rsp in a SIP 200 OK, signed using a VESPER delegate certificate authorized for the dest telephone number. The rsp PASSporT MUST include the original orig and dest values and a fresh iat. The originating party MUST verify the rsp PASSporT using the same certificate validation steps above, applied to the dest telephone number and the destination party’s certificate.

5. RTU Token

The RTU Token is a JWT [RFC7519] signed by the private key of the VESPER delegate certificate, with the certificate chain conveyed in the JOSE header using the x5c parameter. The delegate certificate is the primary trust artifact; the RTU Token signature demonstrates that the presenter holds the corresponding private key. The token is intended for distribution contexts where portable evidence of right-to-use is needed outside of SIP signaling.

The RTU Token MUST include:

* iss: the entity's domain (matching the dNSName SubjectAltName of the signing certificate)

* iat, exp: issuance and expiration times; exp SHOULD be set to a short validity interval to limit the replay surface

* orig: the telephone number being asserted, consistent with the TNAuthList of the signing certificate

The token MAY include additional claims authorized by the JWTClaimConstraints extension of the signing certificate (e.g., Rich Call Data [RFC9795]).

6. Security Considerations

VESPER provides verifiable evidence that an entity authorized to use one or more telephone numbers has signed a communication, with the delegate certificate serving as the primary trust artifact. The primary security properties are: prevention of unauthorized parties from asserting telephone number authority; prevention of over-claiming beyond what the certificate authorizes; and ecosystem auditability through certificate transparency.

The certificate repository MUST be served over HTTPS and implementations SHOULD apply rate limiting to reduce the effectiveness of automated probing. The x5u URL in PASSporT headers MUST reference the certificate at its domain-controlled repository location; Verification Services MUST confirm the domain in the x5u URL matches the dNSName SubjectAltName of the signing certificate, providing proof of domain control without requiring a network fetch. The embedded SCT MUST be validated as defined in [I-D.ietf-stir-certificate-transparency] to confirm the certificate was publicly recorded before use. Short-lived certificates reduce dependence on revocation; relying parties MUST enforce certificate validity windows and SHOULD enforce freshness checks on PASSporT iat claims using existing STIR replay mitigations.

7. IANA Considerations

This document defines no new IANA registrations. VESPER uses existing PASSporT claims defined in [RFC8225] and certificate extensions defined in [RFC8226] and [RFC9118].

8. Acknowledgments

The authors would like to acknowledge Jon Peterson for valuable feedback on this document, and the STIR working group for the foundational specifications on which VESPER builds.

9. Normative References

[I-D.ietf-acme-authority-token-jwtclaimcon]
Wendt, C. and D. Hancock, "JWTClaimConstraints profile of ACME Authority Token", Work in Progress, Internet-Draft, draft-ietf-acme-authority-token-jwtclaimcon-01, 26 March 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-acme-authority-token-jwtclaimcon-01>.

[I-D.ietf-stir-certificate-transparency]
Wendt, C., ナ嗟iwa, R., Fenichel, A., and V. A. Gaikwad, "STI Certificate Transparency", Work in Progress, Internet-Draft, draft-ietf-stir-certificate-transparency-01, 23 November 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-stir-certificate-transparency-01>.

[I-D.ietf-stir-certificates-shortlived]
Peterson, J., "Short-Lived Certificates for Secure Telephone Identity", Work in Progress, Internet-Draft, draft-ietf-stir-certificates-shortlived-04, 4 November 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-stir-certificates-shortlived-04>.

[I-D.ietf-stir-rfc4916-update]
Peterson, J. and C. Wendt, "Connected Identity for STIR", Work in Progress, Internet-Draft, draft-ietf-stir-rfc4916-update-07, 7 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-stir-rfc4916-update-07>.

[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>.

[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/rfc/rfc7519>.

[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>.

[RFC9118] Housley, R., "Enhanced JSON Web Token (JWT) Claim Constraints for Secure Telephone Identity Revisited (STIR) Certificates", RFC 9118, DOI 10.17487/RFC9118, August 2021, <https://www.rfc-editor.org/rfc/rfc9118>.

[RFC9447] Peterson, J., Barnes, M., Hancock, D., and C. Wendt, "Automated Certificate Management Environment (ACME) Challenges Using an Authority Token", RFC 9447, DOI 10.17487/RFC9447, September 2023, <https://www.rfc-editor.org/rfc/rfc9447>.

[RFC9448] Wendt, C., Hancock, D., Barnes, M., and J. Peterson, "TNAuthList Profile of Automated Certificate Management Environment (ACME) Authority Token", RFC 9448, DOI 10.17487/RFC9448, September 2023, <https://www.rfc-editor.org/rfc/rfc9448>.

[RFC9795] Wendt, C. and J. Peterson, "Personal Assertion Token (PASSporT) Extension for Rich Call Data", RFC 9795, DOI 10.17487/RFC9795, July 2025, <https://www.rfc-editor.org/rfc/rfc9795>.

Authors' Addresses

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

Rob ナ嗟iwa
Somos, Inc.
United States of America
Email: robjsliwa@gmail.com