Secure Telephone Identity Revisited
Internet-Draft
Intended status: Informational
Expires: 3 October 2026

C. Wendt
Somos, Inc.

1 April 2026

Verifiable STI Presentation and Evidence for RTU (VESPER) Use Cases and Requirements
draft-wendt-stir-vesper-use-cases-03

Abstract

This document describes use cases and requirements for VESPER (Verifiable STI Presentation and Evidence for RTU), an extension to the Secure Telephone Identity Revisited (STIR) framework. VESPER defines a delegate certificate profile that binds telephone number authority, entity identity, and originating provider authorization into a single verifiable trust artifact, grounded in Right-to-Use (RTU) validation and recorded in a public transparency log. The document identifies the trust gaps that motivate this work and describes requirements for verifiable origination authorization.

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 3 October 2026.

Copyright Notice

Table of Contents

1. Introduction

The Secure Telephone Identity Revisited (STIR) framework ([RFC8224], [RFC8225], and [RFC8226]) enables cryptographic signing of calls using credentials constrained by TNAuthList [RFC8226], grounded in explicit Right-to-Use (RTU) validation by recognized numbering authorities or responsible providers. STIR verifies that a signing credential is authorized for a specific telephone number, but does not establish what entity holds that right-to-use, how that entity can be identified, or whether communications from the originating provider carry valid RTU-backed authorization for the telephone number being presented.

VESPER proposes addressing these gaps through a delegate certificate [I-D.wendt-stir-vesper] that binds telephone number authority to the entity that holds the right-to-use. The certificate can additionally carry corroborating identity signals, such as a domain controlled by the entity. Domain credentials carry entity identity assurances through existing validation procedures that are closely analogous to the entity verification practices discussed in many identity and communications trust frameworks, without requiring standardization of those contextual processes. When both RTU validation and domain validation independently point to the same entity, the combined signal is substantially stronger than either provides alone: the two independent trust chains mutually corroborate the entity's identity, making the overall credential significantly more resistant to forgery or misrepresentation. The certificate can also identify which originating providers have been explicitly authorized by the RTU holder. Certificates issued in this framework are recorded in public transparency logs [I-D.ietf-stir-certificate-transparency] before use, supporting independent auditability without centralizing control.

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.

Right-to-Use (RTU): A cryptographically verifiable authorization binding one or more telephone numbers to the entity that has been assigned and is accountable for their use, established through recognized numbering authorities or responsible providers.

Delegate Certificate: A subordinate certificate issued to the entity that has been assigned a telephone number, as defined in [RFC9060], carrying those numbers in a TNAuthList extension. The delegate certificate serves as the primary credential authenticating the assignee's association with their telephone numbers and their right-to-use.

TNAuthList: A certificate extension defined in [RFC8226] that conveys the telephone numbers, number ranges, or service provider codes for which a certificate holder is authorized.

Service Provider Code (SPC): An identifier assigned to an originating service provider, defined as a choice entry in the TNAuthList extension in [RFC8226]. In North America this is typically an Operating Company Number (OCN) or Service Provider Identifier (SPID).

Authority Token: A signed JWT assertion issued by a recognized numbering authority or responsible provider to convey the right-to-use for specific telephone numbers or service provider codes, defined in [RFC9447] and [RFC9448]. A JWTClaimConstraints Authority Token [I-D.ietf-acme-authority-token-jwtclaimcon] may additionally authorize specific PASSporT claims the certificate holder is permitted to assert.

Signed Certificate Timestamp (SCT): A cryptographic proof returned by a transparency log, as defined in [I-D.ietf-stir-certificate-transparency], that a certificate has been submitted to and recorded in the log prior to use.

3. Use Cases

The following scenarios illustrate the trust gaps that VESPER is designed to address. Each describes a real-world situation where the absence of verifiable telephone number authority creates meaningful risk, and what becomes possible when that authority can be cryptographically established. These scenarios span both business-to-consumer (B2C) and business-to-business (B2B) contexts, reflecting the range of trust relationships in which telephone number authority matters.

3.1. Trusted Caller ID and Verified Messaging

Consumers receive fraudulent calls and messages that spoof trusted telephone numbers, often accompanied by coordinated web or messaging interactions to reinforce the deception. Because there is no standard mechanism for a relying party to verify that the entity presenting a number is the same entity it was assigned to, attackers can credibly simulate legitimate communications across channels.

VESPER enables the RTU holder to cryptographically bind their numbers to delegate certificates that can be validated across SIP signaling, messaging, and web-based contexts. Relying parties can verify both telephone number authority and, where present, the associated domain-controlled context, before applying local trust decisions.

3.2. Preventing Impersonation and Business Communication Fraud

Fraudsters impersonate businesses by spoofing well-known telephone numbers and directing targets to fraudulent websites or callback numbers. Because recipients rely on number recognition as a proxy for legitimacy, this attack is effective across voice, messaging, and web channels simultaneously.

VESPER enables enterprises to maintain a consistent cryptographic binding between their assigned numbers and their domain-controlled identity, issued on the basis of RTU Authority Tokens. Communications referencing those numbers can be verified as authorized by the same accountable entity across any channel.

3.3. Preventing Financial Fraud Through Caller Impersonation

Financial institutions are frequent targets of impersonation: adversaries spoof bank telephone numbers and reinforce the deception through fraudulent web portals or follow-up messages. Customers who recognize the number often extend that trust to the broader interaction even when the surrounding context is malicious.

VESPER enables financial institutions to cryptographically assert their authorized use of specific telephone numbers and bind those numbers to their domain-controlled context. Relying applications can validate this authorization before presenting trust indicators or proceeding with sensitive interactions.

3.4. Explicit Origination Eligibility for Multi-Provider Communications

In enterprise deployments, telephone numbers are frequently originated across multiple providers, platforms, and calling applications. STIR authentication confirms that a call was signed by a credentialed provider but does not establish whether that provider was explicitly authorized by the enterprise holding the right-to-use for that number. An originating provider may sign calls without the RTU holder’s knowledge or consent. Furthermore, an originating service provider’s STIR/SHAKEN Attestation "A" claim, which represents a direct, authorized customer relationship, is today self-certified with no external validation.

VESPER addresses this by enabling RTU holders to include service provider codes (SPCs) alongside telephone number entries in the TNAuthList of their delegate certificate. When both are present, the certificate asserts the entity’s right-to-use for the telephone numbers and identifies the originating providers it expects to attest calls from those numbers on the entity’s behalf. A provider whose SPC appears in the RTU holder’s TNAuthList has verifiable enterprise authorization behind its attestation; a provider whose SPC is absent does not. Terminating networks and relying parties can use this signal to distinguish authorized origination from technically valid but unauthorized traffic.

3.5. Authenticated Access and Identity Assurance for Digital Services

Digital services increasingly use telephone numbers as account identifiers or recovery mechanisms, yet there is no standard way to verify that a number presented by a domain or application is legitimately associated with the entity operating that service.

Under VESPER, service operators authorized for a telephone number can present cryptographic proof of that authorization, optionally bound to a domain-controlled origin. Relying services can validate this before granting elevated access, enabling callbacks, or trusting embedded contact references, reducing abuse by attackers who reference well-known telephone numbers without authorization.

3.6. Public Sector and Emergency Communications Integrity

Public safety communications and official notifications are vulnerable to spoofing, particularly when attackers combine fraudulent calls, messages, and web content to simulate official communications with coordinated credibility.

VESPER enables authorized public entities to assert cryptographic control over designated telephone numbers and bind those numbers to official domain-controlled contexts. Receiving networks or applications can validate this authorization before elevating trust treatment in emergency or public safety communications.

3.7. Carrier-Backed Consumer Identity

Individual consumers do not directly hold the Right-to-Use for their telephone numbers; that authorization rests with the telephone service provider that assigned the number to them. When a consumer places a call, it is their carrier that backs the legitimacy of that number’s use. Today there is no cryptographically verifiable way for the called party to confirm that the originating number is actively backed by a legitimate carrier assignment rather than a spoofed or fraudulently used number.

VESPER enables carriers to issue delegate certificates covering the telephone numbers assigned to their consumers, with the carrier’s RTU authority forming the trust chain. The carrier’s domain serves as the corroborating identity signal, providing the called party verifiable evidence that the number is legitimately assigned and actively backed by a responsible provider. This model applies equally in B2C contexts: a business receiving a call from a consumer can validate that the number is carrier-backed and legitimately assigned, and a consumer receiving a call from a business can benefit from the same verification in reverse. Connected identity extends

this further, enabling each party's carrier to independently assert and verify the other's number authority, establishing mutual trust in the call.

3.8. Bidirectional Identity Verification

In many communication contexts, particularly B2B interactions such as a financial institution calling a business customer or two enterprises coordinating a transaction, a single direction of identity proof is insufficient. The called party has no cryptographic mechanism to verify that the entity calling them is the legitimate holder of the telephone number being presented, and the calling party has no way to confirm the called party is who they expect.

VESPER supports bidirectional identity verification through Connected Identity [I-D.ietf-stir-rfc4916-update]. Both parties can hold delegate certificates authorized for their respective telephone numbers. The called party can return a signed PASSporT asserting their number authority, and the calling party can validate it. The result is a mutually authenticated communication transaction where both parties' telephone number authority is cryptographically verified.

3.9. Credential Retrieval Across Communication Channels

In many communication environments a relying party cannot rely on the signaling path to carry VESPER credentials inline. This includes PSTN/TDM interconnects where SIP Identity headers are stripped, messaging platforms that have no equivalent header mechanism, web-based interactions where a telephone number is referenced but no call is in progress, and asynchronous contexts where verification happens after the communication event.

VESPER addresses this through two complementary mechanisms. A domain-hosted certificate repository provides a stable, publicly resolvable HTTPS location under the entity's domain where delegate certificates can be retrieved and validated independently of how the communication arrived. A portable RTU Token provides a signed JWT proof of right-to-use that can be conveyed in any channel, presented in a message, embedded in a web interaction, or delivered asynchronously, as verifiable evidence of telephone number authority outside of SIP signaling. Together these mechanisms decouple credential verification from any specific transport, making VESPER applicable wherever telephone numbers are used [I-D.wendt-stir-vesper-oob].

3.10. Platform and Multi-Tenant Number Authorization

Communication platforms, CPaaS providers, and ISVs commonly control telephone number pools on behalf of multiple tenants, customers, or automated systems. In these deployments the platform holds RTU for the number pool but originates communications through many different downstream parties. Today there is no standard way for a terminating network or relying party to verify that a given tenant's use of a platform number was explicitly authorized by the RTU holder, or to distinguish authorized tenant traffic from misuse by unauthorized parties.

VESPER enables the platform RTU holder to declare, via SPC entries in the TNAuthList of their delegate certificate, which originating providers are authorized to place calls from those numbers on the platform's behalf. Individual tenants interact with the platform's calling infrastructure without needing to establish independent RTU or certificate relationships. The platform's delegate certificate serves as the auditable authorization record for the entire number pool, making the authorization chain verifiable end-to-end regardless of how many layers exist between the RTU holder and the originating call.

4. Requirements for Origination Authorization

The use cases above motivate a standardized, verifiable mechanism allowing the responsible RTU holder to declare which signing identities are authorized to originate communications for a given telephone number. The following requirements capture the intended properties of such a mechanism:

* Verifiable Enablement: It should be possible to verify that the RTU holder explicitly enabled a specific signing identity (e.g., a delegate certificate or SPC-authorized originator) to originate communications for the telephone number.

* Lifecycle Management: It should be possible to update and revoke origination eligibility declarations in a timely manner, consistent with RTU state and certificate lifecycles.

* Transparency and Auditability: Enablement and revocation events should be observable through transparency mechanisms, enabling independent audit without requiring centralized enforcement control.

* Cross-Channel Applicability: The mechanism should support both voice and messaging use cases and should accommodate scenarios where telephone numbers are referenced within domain-controlled contexts.

* Policy Separation: The mechanism defines verifiable authorization inputs but does not prescribe enforcement, blocking, presentation, or regulatory policy decisions, which remain local to relying parties.

* Attestation Grounding: Where the mechanism supports SPC-based origination authorization, it should be possible for a relying party to determine whether an originating provider's STIR/SHAKEN attestation is backed by an explicit RTU-holder declaration, providing an objective basis for evaluating attestation claims rather than relying on self-certification. This is particularly important in the common case where the originating provider is different from the responsible provider or organization that assigned the telephone number to the entity.

5. Roles and Responsibilities

Deploying VESPER builds on existing STIR/SHAKEN operational roles and trust anchors. The following functional roles are relevant to VESPER deployment. Governance, policy, and regulatory considerations remain external to the protocol.

Telephone service providers, responsible organizations, and numbering authorities ground RTU validation in existing number assignment and delegation practices. Within the VESPER framework, these entities issue cryptographic RTU evidence (e.g., Authority Tokens) that enables STI Certification Authorities to issue TNAuthList-constrained delegate certificates, and manage revocation and lifecycle controls for those assertions.

Application-layer communications providers, including CPaaS and UCaaS platforms, integrate cryptographic identity assertions and delegate certificates into their voice, messaging, and API-based services. They provide token management capabilities for their enterprise customers and implement operational controls for token issuance, expiration, delegation, and revocation.

Business and enterprise entities are the RTU holders responsible for issuing and managing delegate credentials for their telephone numbers. They define which originating providers or internal systems are authorized to use those numbers, and are accountable for monitoring and revoking credentials in response to misuse.

Transparency log operators maintain independently operated, publicly accessible logs that record certificate and authorization artifacts in a tamper-evident, append-only manner [I-D.ietf-stir-certificate-transparency]. They issue Signed Certificate Timestamps (SCTs) proving log inclusion and support ecosystem-wide auditability without centralizing control. The effectiveness of this model is well established through the CA/ Browser Forum's mandate for Certificate Transparency [CABF.CT] in the Web PKI ecosystem [RFC6962].

6. Security Considerations

This informational use-case document defers security considerations to the resulting technical specifications.

7. IANA Considerations

This document has no IANA actions.

Acknowledgments

The author acknowledges the years of industry interactions and innovations that contributed to the technical approaches described here.

References

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-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>.

[I-D.wendt-stir-vesper]
Wendt, C. and R. ナ嗟iwa, "VESPER - Verifiable STI Presentation and Evidence for RTU", Work in Progress, Internet-Draft, draft-wendt-stir-vesper-07, 31 March 2026, <https://datatracker.ietf.org/doc/html/draft-wendt-stir-vesper-07>.

[I-D.wendt-stir-vesper-oob]
Wendt, C. and R. ナ嗟iwa, "VESPER Out-of-Band OOB", Work in Progress, Internet-Draft, draft-wendt-stir-vesper-oob-01, 4 November 2025, <https://datatracker.ietf.org/doc/html/draft-wendt-stir-vesper-oob-01>.

[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>.

[RFC6962] Laurie, B., Langley, A., and E. Kasper, "Certificate Transparency", RFC 6962, DOI 10.17487/RFC6962, June 2013, <https://www.rfc-editor.org/rfc/rfc6962>.

[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>.

[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>.

[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>.

Informative References

[CABF.CT] CA/Browser Forum, "Baseline Requirements for TLS Server Certificates", CABForum CA-Browser-Forum TLS BR 2.1.6, 2025, <https://cabforum.org/working-groups/server/baseline-requirements/documents/>.

Author’s Address

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