Secure Telephone Identity Revisited
Internet-Draft
Intended status: Standards Track
Expires: 8 January 2026

C. Wendt
R. Sliwa
Somos, Inc.

7 July 2025

VESPER - Framework for VErifiable STI Personas
draft-wendt-stir-vesper-04

Abstract

This document formalizes a profile and a framework for the use of delegate certificates and authority tokens to strengthen the association between telephone number assignments and the entities that have the authoritative right to use them. It defines a model in which the TNAuthList Authority Token serves as a trusted representation of telephone number assignment and right-to-use (RTU), anchored by a Notary Agent that logs these associations through verifiable transparency mechanisms. The framework also extends the use of authority tokens to support other PASSporT claims like Rich Call Data (RCD) by defining a role for JWTClaimConstraints Authority Tokens. These tokens are issued by authoritative or recognized and vetted claim agents within the ecosystem to assert information associated with the entity assigned a telephone number. The Notary Agent plays a critical role in recording these claims and their provenance, enhancing transparency and accountability. Delegate certificates encapsulate and incorporate both the telephone number and associated information validated via authority tokens to the certification authority issuing them, binding them to the authenticated telephone number of the calling party. These certificates are published to a certificate transparency log, enabling relying parties to independently verify the integrity and legitimacy of number use and related claims. The VESPER (Verifiable STI PERsona) approach utilizes STIR protocols and the ACME authority token to formalizing a verifiable, auditable, and privacy-conscious foundation for associating telephone numbers with vetted entities and validated assertion of associated metadata.

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 Secure Telephone Identity (STI) architecture, based on STI certificates [RFC8226], PASSporTs [RFC8225], and the SIP Identity header field [RFC8224], define the foundational use of digital signatures and tokens to protect the integrity of calling information, particularly the telephone number, during a communications session. While these mechanisms help validate call signaling, they do not directly establish who is authorized to use a given telephone number. This document provides a profile of the STI architecture by formalizing the use of delegate certificates and authority tokens to more clearly and verifiably associate a telephone number with the entity-person or business-responsible for its use. This stronger linkage is especially important as misuse of telephone numbers by unauthorized parties continues to undermine trust in communications networks.

To address this, the VESPER framework introduces roles and interactions that mirror proven practices from other trust-based industries, such as Know Your Customer (KYC) and Know Your Business (KYB) procedures in finance. Through a defined process and as an adjunct to the telephone number assignment process involving Responsible Providers or Organizations and the Notary Agent, an Entity is issued a TNAuthList Authority Token defined in [RFC9448], establishing their right to use a telephone number. Additional information an entity would like to assert to a called party, such as Rich Call Data (RCD) [I-D.ietf-stir-passport-rcd], can be asserted and authorized using JWTClaimConstraints Authority Tokens [I-D.wendt-acme-authority-token-jwtclaimcon]. JWTClaimContraints have the interesting property that they can be used to assert either direct values or the integrity hashes of values (e.g., using "rcdi" claims defined in [I-D.ietf-stir-passport-rcd]) to enhance the ability to protect the privacy of information when desired or required. These tokens are used in challenges toward the issuance of delegate certificates which can be transparently recorded by a Notary Agent ecosystem role, which acts as a neutral registrar of these claims associated with telephone numbers without exposing underlying private data unless explicitly authorized or desired. Transparent declarations of claim assertions have the potential beneficial property of enhancing the trust of the asserted claims based on monitoring of these claims to avoid fraudulent impersonation that the STI framework is intended to solve.

This VESPER trust model and profile is enhanced using eco-system wide accountability. Transparency logs formalize the issuance of certificates and the relationship between telephone numbers, associated claims and their rightful users, helping detect and prevent fraudulent or conflicting claims by interested parties and

auditing mechanisms. By shifting from implicit trust in digital signatures alone to an explicit framework of vetted identities and transparent claims, this approach builds a foundation for enhanced verifiable communications. It enables the responsible use of telephone numbers, discourages impersonation, and strengthens enforcement against abuse, ultimately fostering greater confidence in telephone number-based communications.

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

This document defines a framework for the authoritative association of telephone numbers to the entities responsible for their use, using delegate certificates and authority tokens. Within this framework, referred to as VESPER (VErifiable STI PERsonas), entities are represented through verifiable claims that establish their right to use a telephone number and, optionally, their asserted claim attributes such as Rich Call Data (RCD) or other claims defined via PASSporT type specifications. These claims are issued by trusted responsible parties and are anchored through transparency mechanisms to support trust, auditability, and privacy as appropriate.

The core premise is that a telephone number, when used as a communications identifier, must be explicitly bound to the real-world party authorized to use it. While telephone numbers have long served as identifiers in global communications, the absence of a strong binding between a number and a responsible party has allowed for abuse-most notably through number spoofing and impersonation fraud. In many cases, bad actors exploit the lack of accountability to mislead call recipients, avoid traceability, or impersonate legitimate businesses and individuals. To address this, the VESPER framework introduces a standardized method for expressing and publishing the right-to-use (RTU) of a telephone number through the issuance of a TNAuthList Authority Token. This token is issued following the assignment or delegation of a number and is registered via a Notary Agent, which records the issuance event in a transparency log. This notarization provides independent verification of the association between a number and its rightful user, without requiring public disclosure of sensitive identity data. Additional claim information can be represented and protected within the delegated certificate using JWTClaimConstraints [RFC8226] and

EnhancedJWTClaimConstraints [RFC9118]. During the delegate certificate issuance process a JWTClaimConstraints Authority Token is used to validate the inclusion of these in the delegated certificate. The resulting delegate certificates are recorded by the Notary Agent, enabling verifiable, ecosystem-wide awareness of valid claims associated to a telephone number. This provides confidence to a relying party and through a verification service that both the entity and the associated claim metadata has been validated through an authorized process and that the calling party has both the right to use the number and, if applicable, has been vetted by a recognized authority.

Unlike prior models that rely on implicit trust in the caller or the STI signer, this approach provides an explicit, auditable, and standards-based path to associate communications with a known and authorized party. The VESPER framework does not define how vetting (e.g., KYC/KYB) is performed, nor does it prescribe specific policy requirements. Instead, it focuses on standardizing how vetted results and right-to-use associations are asserted, recorded, and presented within the STIR ecosystem. By reinforcing the accountability of number usage and enabling the trusted presentation of related identity claims, this architecture enhances integrity, supports privacy, and enables enforcement mechanisms to deter misuse-ultimately restoring trust in telephone-based communications.

4. Vesper Architectural Overview

4.1. The VESPER Trust Framework Architecture

The VESPER Trust Model establishes a structured framework for asserting and verifying the association between a telephone number and the entity authorized to use it. This model supports a broad range of communications use cases, from fully attributed business communications with rich identity information to privacy-conscious scenarios that require only verification that the number is in legitimate use by a real validated entity.

At its core, the model is built on a trust structure with the following key roles:

1. Entities (e.g., individuals or organizations) seeking to assert their right to use a telephone number and assert claims about themselves or a set of communications,

2. Responsible providers and organizations that are authorized to allocate and assign numbers within a jurisdictional numbering plan,

3. Claim Agents that are authorized and recognized for validating and issuing claims about those entities, and

4. A Notary Agent that records claim issuance events and ensures transparency and traceability within the ecosystem.

Participation in this trust model requires a shared set of policies and standards governing how entities are vetted and how claims are created and validated. These policies define the requirements for asserting an entity's identity, the right to use a telephone number, and, where applicable, additional claims and associated attributes (i.e. PASSporT type defined claims, like Rich Call Data). Claims are structured representations of verified information, issued by Claim Agents. Each claim type is standardized via PASSporT type specifications in the STIR working group, with clearly defined required and optional key-value pairs, ensuring interoperability and consistency across the ecosystem. Through this model, VESPER provides a scalable and transparent foundation for building trust in telephone-based communications, with the flexibility to support both fully attributed and privacy-respecting use cases.

4.2. Roles and Responsibilities in the VESPER Framework

The VESPER trust framework defines a set of roles that work together to assert and validate claims about telephone numbers and the entities authorized to use them. At the core of this ecosystem are two primary roles: Entities and Claim Agents. Entities are individuals or organizations that wish to establish their authority to use a telephone number and, optionally, present additional vetted identity attributes. Claim Agents are responsible for validating this information and issuing standardized, structured claims.

4.2.1. Entity

An Entity is the individual or organization seeking to assert its authority to use a specific telephone number and, optionally, to present additional vetted claims such as business name or purpose. The Entity is the central actor around which the claims and trust relationships are formed.

4.2.2. Responsible Provider or Responsible Organization

A Responsible Provider, sometimes called a Telephone Number Service Provider (TNSP), or Responsible Organization (RespOrg) plays both their traditional well-defined role in the allocation and assignment of telephone numbers in accordance with national or international numbering plans generally followed internationally via e.164 and e.164.1 but also a foundational role in the VESPER ecosystem by

validation of the association of telephone number assignments to Entities. These entities operate under regulatory authority and are responsible for administering number resources associated with a specific country code or region.

Their responsibilities include:

* Number Assignment: Allocating telephone numbers to Entities under the rules of an authorized numbering plan.

* Entity Association: Establishing and maintaining a record that links each assigned telephone number to a specific, uniquely identified entity. This includes assigning a persistent identifier or account reference to the Entity to which a number is assigned providing an opaque identifier. This identifier can be used by the Entity to reference themselves in an opaque way for accessing assignment relevant information including TNAuthList Authority Tokens or also referenced during any disputes or disclosures when necessary.

The Responsible Provider or RespOrg coordinates with the Notary Agent to issue proof of assignment or participate in the claim transparency process, their role, even as it currently exists, is essential in grounding the trust framework in authoritative number assignment data. Other ecosystem participants, such as Claim Agents and Notary Agents, can and should reference assignment records governing the Right to Use (RTU) maintained by Responsible Providers or RespOrgs to validate issuance of delegate certificates to the valid Entities.

4.2.3. Claim Agent Responsibilities

Claim Agents are trusted parties in the ecosystem responsible for validating information about Entities and issuing authoritative or verified claims. These claims cover claims associated with PASSporT defined claims including identity details or Rich Call Data (RCD).

Each Claim Agent is uniquely identified within the VESPER ecosystem and should be registered with a Notary Agent (NA) (CW: should it?). Once a Claim Agent performs its vetting process, it issues signed JWTClaimConstraints Authority Tokens containing the validated claim information or integrity hashes for those claims for the Entity depending on privacy preferences.

4.2.4. Notary Agent Responsibilities

The Notary Agent (NA) serves as the ecosystem’s registrar and transparency authority. It performs three critical functions:

1. Registration of Responsible Providers and Responsible Organizations that correspond to the traditional roles in accordance with a national or international numbering plans.

2. Registration of Claim Agents, ensuring each is uniquely identifiable and authorized to issue specific types of claims.

3. Operation of a Transparency Log, which issues cryptographic receipts to confirm and timestamp the existence of each claim.

Notarization can be privacy-preserving, where only cryptographic hashes of claims are logged, or fully transparent, allowing public visibility of claim contents to detect conflicts or impersonation attempts. This optional public disclosure enables monitoring of duplicate or unauthorized claims across the ecosystem.

While this document does not define the dispute resolution process, any conflicts or misclaims discovered through transparency can be escalated through ecosystem-specific mechanisms, likely coordinated by the Notary Agent in communication with relevant Claim Agents.

4.3. Claim Agents and Claim Information Privacy

Privacy is a foundational principle of the VESPER trust model. Claim Agents are not required to expose or publish sensitive data about Subject Entities when recording claims. Instead, claims can be privacy-protected by logging only the cryptographic hashes of the claim content in the transparency log, preserving proof without revealing the underlying details.

4.3.1. Public vs. Private Disclosure

For claim information that is public by nature-such as business names, logos, or other branding elements-Claim Agents may choose to log the data in full within certificates for public visibility. This public transparency helps the ecosystem identify conflicting or fraudulent claims and reinforces trust through open scrutiny.

Conversely, for private or sensitive claims (e.g., internal identifiers or personally identifiable information), Claim Agents may choose to log only a hash of the data. This approach ensures that the claim’s authenticity can still be verified without compromising the Entity’s privacy. Disclosure of such claims remains at the discretion of the Entity or may occur in limited cases where legal or regulatory obligations apply.

4.4. Delegate Certificate Issuance Process

In the VESPER trust framework, the issuance of a delegate certificate to an Entity involves the multiple roles defined and referenced in this document, including the Responsible Provider or Responsible Organization, Claim Agents, the Notary Agent, and a trusted Certification Authority (CA) operating under the STIR eco-system certificate policy governing STIR certificates defined in [RFC8226].

The process begins when a Responsible Provider or Responsible Organization assigns a telephone number to an Entity. As part of that assignment, the Entity is formally associated with the number in the Notary Agent’s system via an opaque and unique identifier, establishing an auditable relationship between the number and the right-to-use holder. The opaque unique identifier helps to uphold the privacy of the eco-system as part of normal telephone number allocation and assignment has traditionally followed. When potential policy violations occur the Notary Agent systems using the Entity identifier provides an indisputable path to the corresponding Responsible Providers and Organizations and then to the Entities assigned the telephone number and delegated a certificate in question that can respond to policy and legal requests as part of their responsibilities to the STIR eco-system should govern.

Additionally, following this association, a TNAuthList Authority Token can be issued to the Entity. This token authoritatively represents the Entity’s Right-To-Use the telephone number and can serve as cryptographic proof of assignment.

In parallel, a Claim Agent may be used to validate additional attributes that the Entity wishes to assert when originating calls, such as Rich Call Data (RCD). These validated attributes are encoded in a JWTClaimConstraints Authority Token, which governs what claims the Entity is authorized to present in communications. The Claim Agent may also use the TNAuthList Authority Token as proof of assignment and the Right-to-Use the telephone numbers being asserted by the Entity. This should also be utilized to govern the constraint of the "orig" claim to only the valid associated numbers to the Entity.

Once both tokens have been obtained, the Entity initiates a Certificate Signing Request (CSR) to a CA authorized to issue certificates within the STIR ecosystem. As per the mechanisms outlined in [RFC9447], [RFC9448], and [I-D.wendt-acme-authority-token-jwtclaimcon], the TNAuthList and JWTClaimConstraints tokens are presented as ACME challenge responses to prove the Entity’s authority over the number and its validated claims.

Upon successful validation, the CA issues a delegate certificate to the Entity. This certificate includes:

* A TNAuthList extension [RFC8226], representing the telephone number(s) the certificate holder is authorized to use.

* A JWTClaimConstraints extension [RFC8226] and/or EnhancedJWTClaimConstraints extension [RFC9118], representing the constraints on claims the certificate holder is permitted to assert.

The issued certificate is then submitted to a certificate transparency log. A corresponding transparency receipt is returned to the Entity and/or CA to provide verifiable proof of publication. This transparency mechanism enables ecosystem-wide monitoring and validation of certificate issuance and claim legitimacy.

4.5. Use of Delegate Certificates for Signing Communications

Once an Entity has received a delegate certificate containing validated right-to-use and claim constraints, it can use this certificate to sign communications associated with the authorized telephone number.

For example, when the Entity initiates a SIP call, it generates a PASSporT object containing session-specific details such as "orig", "dest", and "iat". The Entity then signs the PASSporT using its delegate certificate, which binds both the telephone number and any authorized claims (e.g., RCD elements) to the communication.

Critically, the JWTClaimConstraints extension in the certificate enforces the set of claims the Entity is permitted to assert, ensuring that claims cannot exceed those vetted and authorized by the corresponding Claim Agent.

The signed PASSporT is then attached to the SIP Identity header and transmitted with the call. The Verification Service (VS) on the receiving side performs STIR verification, checking:

* That the PASSporT signature is valid.

* That the delegate certificate is trusted, unexpired, and issued by a recognized CA.

* That the certificate includes a valid TNAuthList extension for the telephone number in use in the "orig" claim.

* That any asserted claims conform to the JWTClaimConstraints and/or EnhancedJWTClaimConstraints in the certificate.

* That a corresponding transparency receipt exists, proving the certificate was publicly recorded.

If all verifications succeed, the relying party can trust that the call is both authorized and attributable, and that all claims have been validated by responsible participants in the ecosystem.

Should questions arise, such as disputes over the legitimacy of the claims, the identity of the calling Entity, or the integrity of the Claim Agent, the Notary Agent serves as the central authority for managing escalation and disclosure. This includes providing access to Responsible Party information via a privacy-preserving and legally compliant resolution process, aligned with ecosystem governance and policy enforcement.

5. Security Considerations

TODO Security

6. IANA Considerations

None

7. Acknowledgments

TODO acknowledge.

8. Normative References

[I-D.ietf-stir-passport-rcd]
Wendt, C. and J. Peterson, "PASSporT Extension for Rich Call Data", Work in Progress, Internet-Draft, draft-ietf-stir-passport-rcd-26, 5 June 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-stir-passport-rcd-26>.

[I-D.wendt-acme-authority-token-jwtclaimcon]
Wendt, C. and D. Hancock, "JWTClaimConstraints profile of ACME Authority Token", Work in Progress, Internet-Draft, draft-wendt-acme-authority-token-jwtclaimcon-02, 7 July 2025, <https://datatracker.ietf.org/doc/html/draft-wendt-acme-authority-token-jwtclaimcon-02>.

[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>.

[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>.

Authors' Addresses

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

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