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

C. Wendt
R. ナ嗟iwa
Somos, Inc.

4 November 2025

VESPER - Framework for VErifiable STI Personas
draft-wendt-stir-vesper-06

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 on the telephone network. 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 identifiable entities and 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 the entity 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 responsible for its use. This stronger linkage is especially important as misuse (i.e., the illegimate spoofing and impersonation) tied to 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 well established in the financial industry. Through a defined process and as an adjunct to the authoritative telephone number assignment process involving Responsible Providers or Organizations and the jurisdictional Numbering Administrator, an Entity is issued a TNAuthList Authority Token defined in [RFC9448], establishing their right to use a telephone number. Beyond establishing the authority of the telephone number, optionally additional information an entity may like to assert to a called party, such as Rich Call Data (RCD) [RFC9795], 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 [RFC9795]) to enhance the ability to protect the privacy of information when desired or required. These Authority Tokens are used in challenges toward the issuance of delegate certificates which can be transparently recorded in a transparency log, which can act as a set of neutral eco-system registrar points for representing asserted claims associated with telephone numbers with or without exposing underlying data as 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.

In addition to supporting call authentication of the originating party, the VESPER framework can also extend to the validation of the called party through the use of connected identity as defined in [I-D.ietf-stir-rfc4916-update]. In this model, the same authority token and delegate certificate mechanisms that bind an originating telephone number to a vetted entity can be applied in the reverse direction, enabling a called party to assert its validated identity via signed PASSporTs included in SIP responses. This optional capability broadens the scope of accountability and transparency to both ends of the communication session while maintaining the privacy-conscious design principles of VESPER.

This VESPER trust model and profile is enhanced using eco-system wide accountability. Transparency logs formalize and announce 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 and auditability, 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 for issuance and certificate transparency for eco-system auditing. 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 claim and 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 from a centralized jurisdictional Number Administrator. This token is issued following the assignment or delegation of a number. The issuance of the delegate certificate is recorded in a transparency log providing relying parties an eco-system wide verification of the association between a number and its authorized entity, authorized by the regulated Responsible Provider or Organization that is authorized to assign numbers via jurisdictional regulatory policies over telephone numbers.

Beyond the association of telephone numbers, JWTClaimConstraints [RFC8226] and EnhancedJWTClaimConstraints [RFC9118] play a critical role in delegate certificates issued under the VESPER framework. They provide a standardized mechanism for Certification Authorities to explicitly constrain any additional claims a delegate certificate holder is permitted to assert in communications. This constraint mechanism ensures that even if a certificate is misused or presented outside its intended scope, the relying party can verify whether the claims presented are authorized by the issuer. Certification Authorities derive these constraints from Authority Tokens issued by vetted Claim Agents, which serve as cryptographic proof of the claim validations. By limiting the scope of claims to those proven and

approved during the certificate issuance process, using JWTClaimConstraints Authority Tokens provided by trusted Claim Agents that take responsibility for vetting those additional claims makes VESPER extensible just as PASSporT claims are intended to do to protect both the telephone number and other assertions made through PASSporTs.

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 for what the relying party should do with this information. Instead, it focuses on standardizing how vetted results and right-to-use associations are asserted, recorded, and presented within the STIR ecosystem focused on the telephone number first and additional claims and assertions second.

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 or mis-issuance issues.

VESPER implementations MUST support short-lived delegate certificates and SHOULD use "x5c" to convey certificates inline. Transparency logging remains required.

4. Vesper Architectural Overview

4.1. The VESPER Framework Architecture

The VESPER framework 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 person 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 Numbering Administrator (NA), both jurisdictional to a country code and neutral to the eco-system, that represents authoritative policies for number uses within that jurisdiction and facilitates a minimum tie of telephone numbers to entity identifiers and ensures transparency, traceability, and auditability within the ecosystem.

Participation in the VESPER framework requires a shared set of policies 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 optionally and where applicable, additional claims and associated attributes (i.e. PASSporT type defined claims, like Rich Call Data). Claims beyond the telephone number are structured representations of verified information, issued by authorized or accepted Claim Agents. Each claim type is standardized via PASSporT type specifications [RFC8225] 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 Organization follows the numbering assignment process but additionally authorizes an TNAuthList Authority Token to be used by a Certification Authority in the issuance of a delegate certificate that minimally includes a TNAuthList extension that corresponds ot the telephone number.

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).

Claim Agents provide JWTClaimConstraints Authority Tokens to validate inclusion of these constrainted claim assertions to the issuance of delegate certificates to the valid Entities. 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. Juridictional Number Administrator Responsibilities

The Number Administrator (NA) serves as the ecosystem's neutral 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. Coordination of eco-system Transparency Logs, which issues cryptographic receipts to confirm and timestamp the existence of each claim.

While this document does not define a dispute resolution process, any conflicts or misclaims discovered through transparency should be escalated through a neutral ecosystem-specific mechanisms, likely coordinated by the NA role in communication with relevant Responsible Providers or Organizations or Claim Agents.

4.3. Claim Agents and Claim Information Privacy

Privacy is a foundational principle of the VESPER framework. Claim Agents are not required to expose or publish sensitive data about 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 potential claim assertions relevent to identifying the calling party, Claim Agents may choose to constrain the direct values of the claims 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 or not at all. This approach ensures that the claim's authenticity can still be verified without compromising the Entity's privacy, if and when required. 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 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 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 as is typical in a Number Administration assignment system, but additionally via an associated opaque and unique identifier. This could be globally unique identifier or a public-key that is provably associated to the entity and establishes 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 but allows for non-repudiation throughout the ecosystem. Thus, when potential policy violations occur, the Entity identifier provides an indisputable path to the corresponding Responsible Providers and Organizations and to the Entities assigned the telephone number via the delegated certificate in question.

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 to an authorized CA that requires that proof to issue a delegate certificate.

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 their preferred 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 of the Authority Tokens required, the CA issues a delegate certificate to the Entity.

CAs SHOULD issue short-lived certificates with brief validity intervals. Entities SHOULD automate renewal to avoid service interruptions.

This certificate MUST include:

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

This certificate, if additional claims and assertions are made beyond the base PASSporT claims defined in [RFC8225], MUST include:

* 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.

4.5. VESPER Certificate Profile (Short-Lived & Inline Conveyance)

VESPER delegate certificates MUST support the short-lived certificate profile in [I-D.ietf-stir-certificates-shortlived]. PASSporTs MUST include the certificate chain using the "x5c" header. Verification Services SHOULD prefer "x5c" over "x5u" if included, and MUST NOT dereference "x5u" if "x5c" is present and valid. Short-lived certificates reduce the need for revocation infrastructure and eliminate external certificate fetches.

4.6. Use of VESPER 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, as defined in [RFC8224] 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 in the PASSporT, ensuring that claims cannot exceed those vetted and authorized by the corresponding Claim Agent.

As defined in [RFC8224], 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.

* If the PASSporT includes an "x5c" header, the certificate chain must be validated from the inline header; "x5u" must not be dereferenced.

* If "x5c" is absent, "x5u" MAY be used to retrieve the certificate chain.

* 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.

Senders SHOULD include "x5c"; relying parties SHOULD prefer "x5c" when both are available.

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.

4.7. VESPER Authentication and Verification Procedures

This section outlines the expected behavior of Authentication Services (AS) and Verification Services (VS) in deployments utilizing VESPER delegate certificates. These procedures extend the baseline STIR authentication and verification models defined in [RFC8224], [RFC8225], and [RFC8226] by incorporating validation of transparency-backed delegate certificates and associated claims.

4.7.1. Authentication Service Behavior

When originating a call, the Authentication Service performs the following steps:

* Constructs a PASSporT for the session containing the required claims (e.g., orig, dest, iat), as well as any optional authorized claims (e.g., Rich Call Data).

* Signs the PASSporT using a VESPER delegate certificate that:

  - Contains a valid TNAuthList extension authorizing the orig telephone number.

  - Optionally includes JWTClaimConstraints or EnhancedJWTClaimConstraints extensions consistent with the asserted claims.

  - Is backed by a Signed Certificate Timestamp (SCT) from a transparency log.

* Attaches the signed PASSporT in a SIP Identity header using the "x5c" header parameter to convey the certificate chain inline.

* Ensures that the certificate is valid, unexpired, and issued by a CA compliant with the VESPER certificate issuance profile.

4.7.2. Verification Service Behavior

Upon receiving a SIP request containing an Identity header, the Verification Service:

* Validates the PASSporT signature and parses the included claims.
* Validates the VESPER delegate certificate by checking:
  - Trust chain validity and issuer compliance with STI and VESPER certificate policies.
  - The presence and accuracy of the TNAuthList extension corresponding to the orig telephone number.
  - The presence and SCT validation of the certificate’s transparency log inclusion.
  - Any JWTClaimConstraints [RFC8226] and EnhancedJWTClaimConstraints [RFC9118] extensions, ensuring claimed values conform to constraints.
* Rejects the PASSporT if any of the above validations fail.

This delineation ensures that only calls with properly issued and verifiable delegate certificates are authenticated and accepted under the VESPER framework, reinforcing accountability and integrity within the STIR ecosystem.

4.7.3. Connected Identity Authentication and Verification

A similar verification process applies when VESPER is used in deployments that support Connected Identity as defined in [I-D.ietf-stir-rfc4916-update]. In this model, the destination party may return a PASSporT of type ’rsp’ within a SIP response, signed using a delegate certificate authorized for the ’dest’ telephone number in the original call.

4.7.3.1. Authentication by the Destination Party

When acting as an Authentication Service, the destination party performs the following steps to generate and sign the ’rsp’ PASSporT:

Constructs a PASSporT of type ’rsp’ including:

* The original ’orig’ and ’dest’ values from the incoming call.
* The ’iat’ claim representing the issuance time.

* Optionally, include other claims to convey attributes of entity including "vper", if appropriate.

Sign the PASSporT using a valid VESPER delegate certificate containing a TNAuthList extension authorizing use of the ’dest’ telephone number (i.e., the destination party’s number).

Include the "x5c" header in the PASSporT, conveying the certificate chain used for signing.

Ensure the certificate is valid, unexpired, includes a valid SCT, and that the certificate corresponds to the ’dest’ claim.

Attach the signed PASSporT to a SIP 200 OK response using the Identity header as described in [I-D.ietf-stir-rfc4916-update].

4.7.3.2. Verification by the Originating Party

To verify the ’rsp’ PASSporT, the originating party (or an upstream Verification Service acting on its behalf) MUST perform the following checks:

* The ’rsp’ PASSporT MUST be signed using a valid VESPER delegate certificate with a TNAuthList value matching the ’dest’ number.

* The certificate MUST:

  - Be issued by a Certification Authority compliant with [RFC8226] and the VESPER profile;

  - Include a valid SCT and be within its validity period.

* The PASSporT signature MUST be validated using the provided ’x5c’ header.

* The ’orig’ and ’dest’ claims MUST match those of the original PASSporT that initiated the call.

* The ’iat’ claim MUST be within an acceptable freshness interval.

* The Verification Service SHOULD validate the certificate’s inclusion in a transparency log using the SCT.

These procedures confirm that the destination party has authenticated and cryptographically asserted its identity using a VESPER delegate certificate, extending mutual identity validation to the terminating side of the call. This process supports bi-directional trust, enhances accountability, and enables privacy-aware identity assertion.

5. PASSporT Claim: "vper" (Verifiable Persona Entity Representation)

This section defines a new PASSporT claim, "vper" (Verifiable Persona Entity Representation), intended to encapsulate structured, extensible metadata about an entity authorized to use a telephone number. The "vper" claim enables verifiable, privacy-conscious assertion of real-world entity attributes bound to a delegate certificate and associated number via the VESPER framework.

5.1. Claim Format

The "vper" claim is a JSON object containing the following REQUIRED fields:

```
"vper": {
  "id": "string",              // Globally unique NA identifier
  "glue": ["string", ...],     // Array of GLUE URNs
  "name": "string",            // Registered legal business name
  "domain": "string"           // Domain associated with the entity
}
```

Field Definitions

* id (REQUIRED): A globally unique identifier for the entity associated via Number Assignment process. This MAY be a UUID, a public key thumbprint, or another opaque identifier that supports global uniqueness and non-repudiation. The identifier serves as a persistent reference to the entity across authority tokens and certificates.

* glue (REQUIRED): An array of GLUE URNs defined in [I-D.ietf-spice-glue-id] that bind the entity to one or more standardized, jurisdiction-specific or globally recognized business identifiers (e.g., DUNS number, EIN, LEI, VAT ID). These enable interoperability across business registries and aid in regulatory traceability.

* name (REQUIRED): A string containing the legal business name as registered with the relevant jurisdictional authority or business registry. This MUST match the name associated with the provided GLUE identifiers.

* domain (REQUIRED): A string representing the canonical domain name associated with the business, typically used for its public website and/or authorized communication addresses (e.g., email). This value MUST be DNS-resolvable and under the administrative control of the asserting entity.

The "vper" claim may be used in full or in hashed form to support privacy-conscious deployments, as guided by the next section.

Extensibility

The "vper" claim is designed to be extensible. Future specifications may define optional fields for additional structured entity metadata. Such extensions MUST be registered via the IANA PASSporT claim registry under this base claim or defined via new claim types.

6. JWTClaimConstraints for Transparent Claims

This section defines how VESPER uses JWTClaimConstraints [RFC8226] and EnhancedJWTClaimConstraints [RFC9118] to announce claims through the certificate that is submitted to a transparency log, while preserving privacy when desired or required. In this model, a Claim Agent validates an Entity’s desired claims and issues a JWTClaimConstraints Authority Token [I-D.wendt-acme-authority-token-jwtclaimcon] to a Certification Authority (CA). The CA includes a corresponding constraints extension in the delegate certificate, and that certificate is logged for ecosystem transparency. Three privacy modes are supported:

1. Transparent-Value 寰the constraint fixes the exact value to be asserted (fully transparent).

2. Semi-Private (Unsalted Hash) — the constraint fixes a hash of the value (guessable by an observer who can test likely values).

3. Private (Salted Commitment) — the constraint fixes a salted hash commitment; verification requires out-of-band salt disclosure from the Entity to an explicitly authorized relying party (RP).

6.1. Goals and Non-Goals

* Binding: Relying parties MUST be able to verify that a presented claim value is one authorized by the certificate.

* Transparency: Observers MUST be able to audit which claims are authorized for a number, without necessarily learning the private values.

* Transparent Privacy Choice: Entities and Claim Agents MUST be able to choose per-claim whether values are public, semi-private, or private.

* Simplicity: All modes use widely deployed primitives (SHA-2) and reuse deterministic serialization similar to RCD integrity [RFC9795] mechanism.

This section does not redefine the syntax of the JWTClaimConstraints/ EnhancedJWTClaimConstraints extensions; it profiles their content to carry clear values or integrity artifacts for values.

6.2. Addressing Claims in PASSporTs

When Claims appear in PASSporTs, constraints refer to claims by claim name and, for structured claims, by JSON Pointer (RFC6901) into the claim value.

However, even if the PASSporT does not include an explicit claim as part of the signed object in the context of a call or message, an important property of the transparency in the VESPER framework is if the relying party wants to validate claims made as part of transparency validation outside of PASSporT verification, it can look at the JWTClaimsConstraints objects to validate claims.

6.3. Constraint Encodings (Three Privacy Modes)

For each constrained claim (or claim path), the JWTClaimConstraints Authority Token and the certificate extension MUST carry exactly one of the following encodings.

6.3.1. Transparenct-Value Constraint

The claim value is directly constrainted to be the value in open text.

Verification: The VS compares the presented PASSporT claim value (after deterministic serialization if structured) for equality with value.

6.3.2. Semi-Private Constraint (Unsalted Hash)

Intended use: Values where limited hiding is acceptable, understanding that guessing is possible (e.g., logo URL or short labels).

Semantics: The certificate fixes a digest D over the canonicalized value without a salt.

Computation:

V_bytes = deterministic_serialize(V) D = SHA-256(V_bytes)

Verification: The VS computes D′ over the received value and accepts if D′ == digest.

Privacy: An observer who can guess candidate values can compute digests and test them. Use only when this risk is acceptable or values have sufficient entropy. This mirrors the integrity mechanism in [RFC9795].

6.3.3. Private Constraint (Salted Commitment with Selective Disclosure)

Intended use: Sensitive values (e.g., opaque IDs, PII) where the Entity wants verifiability only for explicitly authorized RPs.

Semantics: The certificate fixes a commitment C that incorporates a secret, per-claim salt S. Only C (and optionally a hash of S) is published. The Entity may later disclose S (and, if needed, V) out-of-band to an RP of its choosing for verification.

Data Items

V: value to be proven (octets after deterministic serialization). S: secret random salt (128 bits from a CSPRNG). H: a collision-resistant hash (MUST support SHA-256).

Computation:

V_bytes = deterministic_serialize(V) C = H(S || V_bytes) (optional) S_hash = H(S)

Publication: The certificate and transparency log include only commit (and optional salt_hash). S and V are not published.

Salt Disclosure: The Entity MAY disclose S (and, if required, V) to an authorized RP via an authenticated, confidential channel (e.g., a compact JWE encrypted to the RP’s public key). Disclosure is per-RP and per event at the Entity’s discretion.

Verification by RP: 1. Obtain (V, S) from the Entity. 2. Compute C′ = H(S || deterministic_serialize(V)). 3. Accept if and only if C′ == commit (and, if salt_hash present, H(S) == salt_hash).

6.4. Certificate and Transparency Log Requirements

The CA MUST copy the constraints from the JWTClaimConstraints Authority Token into the certificate’s JWTClaimConstraints/ EnhancedJWTClaimConstraints extension without widening them.

The issued certificate MUST be submitted to a transparency log; the log therefore reveals: * the existence of each constrained claim/ path, and * for each, either the clear value, an unsalted hash, or a salted commitment (but never the salt). * For mode commit, implementations MUST NOT include the salt in the certificate or log.

6.5. Authority Token Requirements

A JWTClaimConstraints Authority Token MUST:

* identify the Claim Agent and the Entity,

* enumerate the constrained claims/paths and, for each, one of the three encodings above,

* specify the hash algorithm where applicable ("alg": "sha-256" RECOMMENDED),

* be time-bounded and bound to the TN(s) (e.g., via TNAuthList) authorized for the Entity.

The CA MUST verify the token per [I-D.wendt-acme-authority-token-jwtclaimcon] and issue a certificate that does not exceed the token’s scope.

6.6. Verification by a Relying Party (VS)

When verifying a PASSporT:

* For value mode: ensure the presented claim equals the constrained value.

* For hash mode: recompute the digest over the presented claim and compare.

* For commit mode: if the RP has received S (and V if needed) out-of-band, recompute and compare the commitment. If S is not available, the RP MUST treat the constraint as "authorized but not presently verifiable" and apply local policy (e.g., defer validation, request disclosure, or treat as unauthenticated attribute).

7. Security Considerations

TBD

8. IANA Considerations

New PASSporT Claim: "vper"

This document requests that the IANA add a new entry to the "PASSporT Claims" registry as follows:

Claim Name	Claim Value Type	Reference
vper	JSON object	RFCthis

Table 1: PASSporT Claims registry entry for "vper

9. Acknowledgments

The authors would like to acknowledge Jon Peterson for valuable feedback into the concepts and framework for this document. This work is mainly based on the many years of inputs and specifications developed in the STIR working group and the larger telephone industry which the authors acknowledge as a critically important feedback and influence toward the development of the VESPER framework.

10. Normative References

[I-D.ietf-spice-glue-id]
Zundel, B., Dingle, P., and M. B. Jones, "GLobal Unique Enterprise (GLUE) Identifiers", Work in Progress, Internet-Draft, draft-ietf-spice-glue-id-02, 20 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-spice-glue-id-02>.

[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-03, 6 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-stir-certificates-shortlived-03>.

[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-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-03, 7 July 2025, <https://datatracker.ietf.org/doc/html/draft-wendt-acme-authority-token-jwtclaimcon-03>.

[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>.

[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 liwa
Somos, Inc.
United States of America
Email: robjsliwa@gmail.com