stir
Internet-Draft
Intended status: Informational
Expires: 4 February 2026

C. Wendt
Somos, Inc.

3 August 2025

Verifiable STI Persona (VESPER) Use Cases and Requirements
draft-wendt-stir-vesper-use-cases-01

Abstract

This document discusses a set of use cases and requirements for an extension to Secure Telephone Identity Revisited (STIR) called Verifiable STI PERsona (VESPER). VESPER fundamentally enhances STIR by establishing an authoritative and cryptographically verifiable Right-to-Use (RTU) relationship between telephone numbers and their assigned entities, business organizations or individuals, through digital signatures that bind an entity to a set of asserted claims, delegate certificates that govern the assertion of those claims to a responsible party, and Authority Tokens that prove the validitation of those claims by authoritative parties. This cryptographic binding ensures explicit non-repudiation, removing ambiguity around who is accountable for calls or messages originating from specific telephone numbers, significantly deterring spoofing and fraud.

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 4 February 2026.

Copyright Notice

Table of Contents

1. Introduction

The Secure Telephone Identity Revisited (STIR) framework ([RFC8224], [RFC8225], and [RFC8226]) has established a robust foundation for mitigating caller ID spoofing by cryptographically associating telephone numbers with the entities responsible for originating telephone calls and other forms of real-time communications. However, STIR primarily focuses on authenticating the calling number itself or the responsible network provider, without fully validating the underlying individual or business entity claiming the right-to-use (RTU) that telephone number or clearly establishing how and by whom such validation occurred. Consequently, ambiguities remain regarding the actual entity responsible for calls, the authenticity of caller attributes, and the caller's consent or authorization.

The VESPER framework [I-D.wendt-stir-vesper] extension to the STIR framework directly addresses these gaps by establishing an authoritative, cryptographically verifiable relationship between telephone numbers and their legitimate assignees,responsible businesses or individuals, using digital signatures, delegate certificates [RFC9060], and Authority Tokens [RFC9447], [RFC9448], [I-D.wendt-acme-authority-token-jwtclaimcon]. By explicitly linking telephone numbers to validated entities through these cryptographic proofs, VESPER provides robust non-repudiation, conclusively identifying the entity accountable for calls or messages and significantly reducing, if not virtually eliminating, when verified by relying parties, opportunities for number spoofing and related fraudulent activities for the telephone numbers represented by and in the VESPER framework roles and elements.

A central principle of VESPER is privacy-preserving transparency. It utilizes independent Notary Agents defined in [I-D.wendt-stir-vesper] and public, tamper-evident transparency logs [I-D.wendt-stir-certificate-transparency] to securely publish cryptographically verifiable assertions of RTU and entity attribute claims including associated call and caller metadata. These transparency mechanisms typically employ privacy-protecting opaque identifiers to safeguard confidentiality and protect personally identifiable information (PII), except when explicitly required for lawful enforcement or voluntarily disclosed by the entity itself. Importantly, the VESPER framework explicitly allows telephone number

holders, particularly businesses, to publicly disclose their verified identities, telephone number associations, and validated claims. This level of transparency significantly enhances public trust and accountability, while still respecting privacy preferences and confidentiality requirements in other circumstances.

VESPER also clearly delineates liability and accountability within the telecommunications ecosystem, providing objective safe-harbors to telecommunications providers with proper delegation to entities that utilize those Responsible Providers and Organizations that follow the framework for their telecommunications services. Providers verifying delegate certificates [RFC9060] and transparency log receipts can objectively demonstrate a defined standard of reasonable diligence, aligning directly with recognized legal frameworks for digital signatures. The legal foundation for the use of digital signatures is well established, with precedents such as the U.S. E-SIGN Act [US.E-SIGN] and the EU eIDAS Regulation [EU.eIDAS] recognizing their validity and enforceability. Providers can demonstrate a high standard of due diligence by relying on cryptographic proofs issued by vetted entities, whether corporate or individual, whose identities have been verified through Know Your Customer (KYC) and identity-proofing procedures aligned with leading international and regulatory frameworks, including [FATF.KYC], [FinCEN.CDD], [NIST.SP.800-63A], and [EU.eIDAS]. This enables them to achieve explicit legal protections and regulatory safe-harbors against undue liability. Moreover, by combining these upfront checks with continuous public transparency and monitoring mechanisms, the ecosystem can rapidly detect and correct any inadvertent mis-issuance or deliberate malfeasance by trusted parties.

Ultimately, by integrating deeper levels of identity assurance, transparent public verification, and clear accountability, VESPER significantly enhances trust, compliance clarity, and regulatory efficiency within jurisdictionally regulated telephony services, complementing and extending the foundational STIR framework toward a high-assurance telecommunications ecosystem.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. The Telephone Number as an Authoritative, Jurisdictionally Regulated, and Accountable Digital Identity Anchor

In a digital landscape increasingly crowded with unverified email addresses, anonymous app handles, and transient digital identities, the telephone number remains uniquely positioned as a robust and regulated identity anchor. Although originally created for legacy telecommunications infrastructure as a globally unique routing identifier, similar to an IP address, the telephone number continues to benefit from well-established jurisdictional frameworks that mandate clear accountability, regulated access, and explicit responsibilities assigned to responsible communications service providers. Unlike, IP addresses, a telephone number is often considered a lasting communications identity, often advertised publically in the case of many businesses. This distinctive regulatory context uniquely positions the telephone number to serve as a foundational anchor for trustworthy digital identity, examples described in [NIST.SP.800-63], particularly in contexts where accountability is mandated by law and clear identification of responsible entities is essential.

Unlike freely created digital identifiers, telephone numbers are strictly administered resources, assigned and managed under explicit regulatory oversight. For instance, in the United States, the Federal Communications Commission (FCC), together with designated neutral numbering administrators, governs allocation, assignment, and portability under the North American Numbering Plan [NANPA.Plan]. The NANP [NANPA.Plan] operates within the global E.164 numbering structure defined by the ITU [ITU.E164]. This structured oversight ensures that every telephone number maintains an unambiguous link to an authorized, regulated carrier-of-record, creating a traceable, auditable chain of authority that, if properly accounted for and enforced, should not easily be bypassed or manipulated.

The regulated carrier relationship introduces critical legal and operational accountability into digital interactions anchored by telephone numbers. Even when the human or business entity utilizing a particular number remains anonymous to the broader public, the service provider managing that number retains a clearly defined legal obligation for compliance, privacy protection, portability rules, and responsiveness to lawful investigation. This provider-level accountability significantly differentiates telephone numbers from other digital identifiers, providing regulatory authorities with a clearly identifiable, legally accountable intermediary whenever misuse or fraudulent activity is suspected.

Recently, the STIR framework, has significantly enhanced this inherent accountability through the addition of cryptographic authentication and verification mechanisms. STIR employs digital signatures using a corresponding certificate issued to authorized repsonsible providers and organizations defined in [RFC8225] and [RFC8226]. The delegation of certificates, defined in [RFC9060] allows responsible providers when they assign numbers to their customers to provide a delegate certificate for use in the STIR ecosystem. The VESPER framework's purpose and intent is to further extend and deepen this concept by explicitly binding the telephone numbers and process of delegation to verified and legally accountable business entities or individuals through the use of cryptographically secured Authority Tokens that validate the issuance of delegate certificates. The use of digital signatures corresponding to the issued delegate certificate ensures non-repudiation and offer a strong deterrent against fraudulent usage or spoofing, transforming telephone numbers adhearing to the VESPER framework into robust identity anchors.

The use of the VESPER enhanced trust framework not only clarifies accountability but also introduces clear, objective allocation of liability across multiple stakeholders:

* Individuals and businesses explicitly asserting and accepting accountability by digitally signing communications, binding themselves cryptographically to their assigned telephone number. This creates unequivocal non-repudiation, an explicit digital admission of responsibility.

* Telecommunications service providers bear explicit responsibility for issuing, validating, revoking, and attesting delegate certificates on behalf of their customers. Downstream carriers and other relying parties which verify certificate chains and audit transparency-log receipts gain a legally defensible safe harbor against undue liability, thereby incentivizing robust compliance and governance practices.

* Transparency mechanisms and governance frameworks, such as independent, tamper-evident transparency logs, offer continuous public oversight and rapid detection of inadvertent mis-issuance or deliberate malfeasance. These mechanisms establish clear paths for enforcement, dispute resolution, and accountability, further reinforcing the overall integrity and reliability of the ecosystem.

This structured model mirrors familiar legal frameworks governing accountability in the physical world: individuals and entities clearly bear responsibility for their actions; providers act as

regulated custodians with duties to both customers and authorities; and regulatory bodies and law enforcement enforce accountability through structured due process.

By integrating longstanding regulatory oversight with advanced cryptographic assurance anchored by the core STIR authentication and verification protocols, the telephone number emerges as a uniquely effective anchor of digital trust, one that reliably balances accountability and privacy within a clear legal and technical framework.

4. VESPER: A Telecommunications-Based Trust Framework

The continued erosion of public trust underscores the critical need for such a balanced model, one that simultaneously safeguards individual and corporate freedoms and rights, strengthens digital integrity, and ensures effective accountability. Telecommunications infrastructure, uniquely regulated and identity-anchored through telephone number assignments, is optimally positioned to lead this transition toward a more trustworthy and accountable digital communications ecosystem.

4.1. Foundational Goals of the Framework

This trust framework is structured around four foundational principles:

* Authoritative Verifiability: Each participant in a digital interaction can cryptographically verify the legitimacy of the counterparty’s asserted identity and their explicit Right-to-Use (RTU) specific telephone numbers without necessarily knowing the counterparty’s personal identity.

* Explicit Accountability and Non-Repudiation: Digital actions linked to telephone-number-based identities are cryptographically signed, establishing unambiguous non-repudiation. Entities accepting and asserting accountability through digital signatures can therefore be legally traced, under appropriate due process, to responsible individuals or business entities.

* Privacy and Consent: Personal identity remains protected by design. User information is only revealed upon explicit consent or when legally mandated. Selective disclosure mechanisms ensure minimal exposure of personally identifiable information (PII), preserving privacy while enabling regulatory oversight.

* Provider and Infrastructure Responsibility: Telecommunications service providers issuing identifiers (telephone numbers and associated authority tokens) have clearly defined legal obligations to responsibly manage issuance, attestation, validation, and compliance with lawful inquiries. Providers following rigorous cryptographic validation processes gain clear legal safe-harbors, incentivizing broad compliance.

4.2. Framework Architectural Overview

Central to this framework is the concept of cryptographically secure identity assertions, leveraging delegate certificates and Authority Tokens as described within the VESPER extension of STIR [I-D.wendt-stir-vesper]. These cryptographic set of eco-system credentials explicitly represent verified RTU for telephone numbers, along with validated entity attributes in the form of claims. Entities digitally sign actions, such as placing calls or sending messages, creating explicit, legally recognized evidence of accountability that significantly reduces fraud and spoofing.

Key architectural elements include:

* Vetted Entity Assertions: Trusted responsible telecommunications providers or authorized agents explicitly attest to an entity’s verified RTU of specific telephone numbers and any validated claims or attributes through standardized cryptographic mechanisms.

* Tamper-Evident Transparency Logs: Every issuance of authorized delegate certificates is recorded in eco-system avilable, independently and/or neutrally maintained, append-only transparency logs. Cryptographic receipts allow third parties, including regulators and providers, to verify proper issuance and rapidly detect mis-issuance or malfeasance.

* Delegation and Controlled Presentation: Entities may securely be delegated to and delegate usage rights to authorized representatives (e.g., call centers, CPaaS platforms, individual devices) while maintaining accountability and traceability to credentials that can be revoked by authoritative and responsible parties.

4.3. Legal Interface and Process Compatibility

Explicit integration with legal frameworks ensures regulatory and procedural compatibility:

* Compliance with Subpoenas and Warrants: As with longstanding telecommunications practices, lawful subpoenas or court orders can be used to reveal the entity behind pseudonymous tokens when harm or illegality is credibly alleged. This supports attribution through due process and preserves judicial oversight while respecting end-user privacy until a legal threshold is met.

* Clear Provider Obligations and Defined Safe-Harbors: Those that issue delegate certificates under the VESPER framework are required to submit to auditable transparency logs. Proviers and relying parties that performing cryptographic validation steps, such as verifying the certificate chain and transparency receipt correspondingly demonstrate "reasonable diligence."

* User Rights and Disclosure Boundaries: The framework gives users granular control over what entity information is disclosed and when, supporting public transparency where desired (e.g., by enterprises) while still protecting personally identifiable information (PII) by default. Entity disclosure only occurs under lawful process or user consent, and users retain the right to seek redress for misuse, impersonation, or unauthorized exposure of their credentials.

4.4. A Layered Trust and Accountability Model

This telecommunications-based trust framework supports a layered approach to identity, balancing user privacy, enterprise transparency, and systemic accountability:

* Anonymous or Pseudonymous Participation: Individuals may engage in digital communications without exposing personal identity by default. Pseudonymous tokens that use verifiable hashes and opaque identifiers allow users to maintain privacy while proving authorized access and use of a telephone number.

* Transparent Entity Disclosure for Trust Enhancement: Business entities or individuals may choose to publicly disclose their validated entity claims, including right-to-use (RTU) assertions and related metadata, as part of transparency efforts. This opt-in disclosure, published via tamper-evident transparency logs, builds verifiable public trust in their communications and associated claims such as Rich Call Data (RCD) defined in [RFC9795].

* Explicit Legal Accountability for Malicious Actors: Cryptographic non-repudiation ensures that entities who misuse verified certificates or tokens inherently self-incriminate. If abuse or impersonation occurs, providers and regulatory authorities can

rely on transparency receipts, audit logs, and signature trails to identify the responsible party through lawful process, protecting the broader ecosystem from fraud and reinforcing deterrence through enforceable consequences.

This structured, tiered model preserves individual autonomy while embedding strong legal and cryptographic safeguards. It allows entities to selectively expose identity when it enhances credibility, and enables regulators and providers to clearly allocate roles and responsibilities. By anchoring these functions to the globally recognized and jurisdictionally governed telephone number, the framework fosters a scalable and lawful model of digital trust.

4.5. Privacy by Design Rather than Policy

Many contemporary digital platforms rely primarily on internal terms of service to define privacy expectations, resulting in weak guarantees that can be altered unilaterally or undermined by external demands. In contrast, this telecommunications-based trust framework incorporates explicit privacy-by-design principles embedded directly into its technical architecture through cryptographic mechanisms, including:

* Purpose-Specific Tokenization: Identity assertions (Authority Tokens and delegate certificates) are explicitly bound to specific usage contexts and authorized purposes, preventing unauthorized secondary use.

* Independent, Tamper-Evident Transparency Logs: Issuance of cryptographic identity credentials and tokens is publicly logged in independently maintained, cryptographically secure transparency logs. These logs provide auditability and accountability without compromising user privacy or exposing personally identifiable information when desired.

* Competitive and Distributed Responsible Issuance: Following existing competitive communications service provider business models, identity verification and token and certificate issuance processes are distributed and conducted by regulated telecommunications providers or authorized entities freely chosen by end users of telecommunications services that adhere to clear compliance and auditability standards, thus eliminating dependence on centralized or decentralized identity repositories managed by single parties that risk privacy compromise or choice of trusted provider or enable trust across transparent jurisdictional boundaries.

By embedding these explicit privacy safeguards directly into the technical design, entities and users gain robust, cryptographically enforceable control over their personal data disclosures, far beyond the limited protections offered by privacy policies or contractual terms of service alone.

4.6. Due Process and Lawful Identity Attribution

A central benefit of anchoring digital identities in jurisdictionally regulated telephone numbers is the availability of established legal processes for lawful identity attribution. Lawful identity attribution is supported by existing frameworks such as the U.S. Stored Communications Act [US.SCA], the EU ePrivacy Directive [EU.ePrivacy], and international conventions like the Budapest Convention [COE.Cybercrime]. Technical compliance with identity proofing standards like NIST SP 800-63 [NIST.SP.800-63] ensures verifiability in regulated digital environments. Similar to how telecommunications subscriber records are currently accessed through legally authorized subpoenas, warrants, or court orders, the telecommunications-based trust framework provides clear processes for legally valid identity resolution.

Authority Token or delegate certificate issuers, such as regulated telecommunications providers or authorized credential issuers, maintain comprehensive and auditable logs enabling explicit, lawful compliance with subpoenas or judicial requests. Crucially, this targeted identity attribution process remains strictly limited, legally controlled, and fully transparent with privacy guarentees, avoiding mass surveillance or arbitrary identity disclosures. By employing established legal thresholds and due process standards upheld by the responsible providers or organizations, this framework ensures law enforcement and regulatory authorities obtain identity information solely through clear, judicially sanctioned pathways of entities chosen responsible provider or organization.

4.7. Balancing Individual Rights with Explicit Accountability

In addressing contemporary digital accountability challenges, this telecommunications-based framework provides explicit clarity regarding liability allocation and responsibilities across all participants:

* Individuals and Entities: Users are directly accountable for actions taken under their cryptographically secured identity tokens. Digital signatures represent explicit legal admissions of responsibility, supported by long-standing precedents like the U.S. E-SIGN Act [US.E-SIGN] and EU eIDAS Regulation [EU.eIDAS], ensuring strong non-repudiation and deterrence of malicious behavior.

* Telecommunications and Service Providers: Providers issuing and validating cryptographic identity assertions have clear regulatory obligations, including appropriate verification, auditability, and compliance with lawful disclosure requests. Providers adhering to these explicit due-diligence standards benefit from clear legal safe-harbors, incentivizing rigorous compliance and robust identity management practices.

* Government and Regulators: Regulatory bodies bear the responsibility of defining clear and legally enforceable thresholds for lawful identity attribution, safeguarding against government overreach, and ensuring appropriate mechanisms for redress in cases of mistaken identity attribution or procedural abuse.

Through this structured balance of rights and responsibilities, the framework promotes a rights-respecting digital ecosystem where individual privacy is preserved, lawful accountability is enforceable, and regulatory clarity is maintained without increasing centralized control or expanding surveillance powers. In doing so, this telecommunications-based trust framework provides a legally sound, privacy-preserving approach to digital identity, one fundamentally aligned with individual digital protections and norms.

5. Use Cases and Scenarios

A trust framework demonstrates its true value through practical application to real-world problems. The telecommunications-based identity model proposed here is not theoretical, it addresses critical and widespread issues in digital communications today. The scenarios below illustrate concrete benefits for consumers, enterprises, communications platforms, and regulatory bodies, effectively balancing privacy, accountability, and legal clarity.

5.1. Trusted Caller ID and Verified Messaging

Problem: Consumers are inundated with fraudulent and deceptive phone calls and messages. Malicious actors regularly spoof trusted identities, banks, government agencies, healthcare providers, to exploit victims financially or extract sensitive information. Traditional caller ID systems and messaging channels currently offer minimal assurance of sender authenticity, undermining public trust.

Solution: Using the proposed VESPER-based trust framework, businesses or individuals can present cryptographically signed delegate certificates during calls or message exchanges. The associated digital signatures, tied explicitly to authorized telephone numbers, are verified in real-time by receiving networks or relying applications, ensuring that the caller is explicitly authorized to represent the asserted identity.

Privacy Benefit: Tokens, certificates and corresponding transparency logs need not expose personal identities, only responsible provider and organizational affiliation or proof of verification status, preserving consumer privacy while enhancing trust.

Accountability Benefit: Malicious use is directly traceable through cryptographically logged issuance events, enabling lawful attribution and regulatory enforcement.

5.2. Preventing Impersonation and Business Communication Fraud

Problem: Fraudsters frequently impersonate executives, support agents, or trusted representatives, deceiving employees and customers into transferring money, credentials, or sensitive data. Current communication methods make it difficult to verify genuine business-originated calls or messages, significantly exacerbating risks.

Solution: Enterprises utilize cryptographically secured delegate certificates and tokens to authorized personnel, call centers, or automated business systems. These tokens and certificates carry clearly defined assertions, such as "Authorized Support Agent" or "Verified Collections Department," validated via vetted Know-Your-Customer (KYC) processes and recorded transparently in public, tamper-evident logs.

Privacy Benefit: Individual employee identities can remain protected; only the desired organizational authorization status is explicitly disclosed.

Accountability Benefit: Delegated misuse creates a cryptographic audit trail traceable to individual agents or systems, enabling swift traceable investigation and clear external legal attribution.

5.3. Reputation-Based Access and Moderation on Digital Platforms

Problem: Social media platforms and online services that utilize user asserted identifiers face ongoing challenges differentiating authentic, good-faith participants from malicious users or automated accounts. Malicious actors repeatedly create new, anonymous accounts to evade moderation and conduct harmful activities.

Solution: Users register on digital platforms using pseudonymous but cryptographically verified identity tokens tied to authorized phone numbers or vetted entities. Over time, these tokens accumulate positive reputational signals, enabling services to provide tiered access levels, moderation privileges, or other trust-based incentives.

Privacy Benefit: Users avoid disclosing sensitive personal data to individual platforms; instead, they present proof of a trusted identity anchor without revealing unnecessary personal details.

Accountability Benefit: Malicious actors can no longer evade moderation by repeatedly creating unverified identities; misuse is cryptographically traceable, enabling efficient, targeted enforcement actions when legal thresholds are met.

5.4. Public Sector and Emergency Communications Integrity

Problem: Public emergency alerts, health updates, and official notifications are susceptible to spoofing, risking dangerous confusion, panic, or exploitation by malicious actors. Current dissemination methods lack reliable authentication mechanisms to assure recipients of message authenticity.

Solution: Government agencies and authorized entities issue cryptographically signed delegate certificates and Authority Tokens tied explicitly to recognized telephone numbers or trusted service codes. Network providers and applications validate these cryptographic signatures in real-time before delivering critical messages, ensuring authenticity and trustworthiness.

Privacy Benefit: Recipients receive verifiably authentic communications without needing to disclose or collect additional personal information.

Accountability Benefit: Only explicitly authorized entities can successfully issue validated tokens. Any misuse or impersonation leaves clear cryptographic evidence in transparency logs, enabling swift regulatory and legal action.

5.5. Why These Use Cases Matter

These examples illustrate the profound versatility and real-world applicability of the telecommunications-based trust framework. By leveraging cryptographically assured telephone-number-based assertions, the framework achieves significant improvements in consumer protection, enterprise security, public safety, and civic integrity. It explicitly balances user privacy with robust accountability, enabling clear legal attribution through transparent due-process mechanisms. Ultimately, this blend of authoritative verification, privacy-preserving transparency, and explicit legal accountability addresses precisely the challenges and complexities inherent in modern digital communications.

6. Deployment and Governance

Implementing a privacy-preserving, legally accountable trust framework anchored in telephone numbers is not merely a technical endeavor, it requires ecosystem coordination and a governance structure to coordinate and manage responsible participants to provide clear alignment across telecommunications, technology providers, enterprises, regulatory authorities, and policy-making bodies. In current STIR/SHAKEN deployments, this to a large extent exists providing a trust anchor and certificate policy that aligns with the fundamental STIR architecture. Successful deployment of VESPER framework extensions with that governance in place does not necessitate additional centralized control or extensive new regulatory mandates; rather, it can evolve organically through established roles and existing jurisdictional frameworks, facilitated by interoperable standards and transparent accountability mechanisms that can enable VESPER. There are however some new roles and responsibilities required as discussed above. The following section describes those new roles or responsibilities for eco-system participants.

6.1. Roles and Responsibilities

6.1.1. Responsible Telephone Service Providers, Responsible Organizations, and Numbering Authorities

Responsible telephone service providers, Responsible Organizations, and numbering authorities currently operate under explicit regulatory oversight, managing number allocation, portability, subscriber records, and responding to lawful inquiries. Traditional delegation via Letters of Authorization (LoAs) [ATIS.LoA], traditional Toll-Free Number LOA practices defined by ATIS SNAC [ATIS.TFLOA], and used for number portability and RTU transfers [FCC.NumberPorting], lack cryptographic enforceability or public auditability or transparency. Under this enhanced trust framework, these entities assume additional, clearly defined responsibilities:

* Issuance of Cryptographic Right-to-Use (RTU) Assertions: Providers and numbering authorities issue authoritative cryptographic attestations (Authority Tokens and delegate certificates) explicitly verifying entities' legitimate Right-to-Use specific telephone numbers.

* Revocation and Audit Management: Providers manage token revocation processes, or in the case of sufficiently short-lived certificates [I-D.ietf-stir-certificates-shortlived] simply removing the ability to request fresh tokens, and publish issuance and revocation events to independent, tamper-evident transparency logs, ensuring auditability, compliance, and immediate detection of mis-issuance or fraud.

* Compliance with Lawful Attribution Requests: Providers respond promptly to lawful subpoenas or judicial orders requiring disclosure of subscriber identities associated with specific cryptographic tokens, adhering strictly to established legal standards of due process and privacy protections.

6.1.2. CPaaS, UCaaS, and Enterprise Communications Providers

Application-layer communications providers, including Communications Platform as a Service (CPaaS) and Unified Communications as a Service (UCaaS) providers, facilitate enterprise and end-user interaction with telephone numbers and identity tokens, fulfilling essential integration roles by:

* Embedding Cryptographic Verification: Integrating cryptographic identity assertions and delegate certificates directly into their voice, messaging, and API-based services, ensuring real-time verification and enhanced call authentication.

* Providing Token Management Tools: Offering enterprise customers and individual users intuitive tools to manage and present authority tokens and delegated certificates for communications, preserving privacy while ensuring authenticity.

* Enforcing Policies and Compliance: Implementing and maintaining rigorous policies regarding token issuance, expiration, delegation, revocation, and lawful compliance, enabling proactive response to misuse or fraudulent activities.

6.1.3. Business and Enterprise Entities

Businesses and enterprise entities act as critical identity providers for their employees, contractors, or automated systems. Within this framework, enterprises assume explicit responsibility to:

* Properly Manage Delegated Certificates and Credentials: Properly issue and delegate credentials tied explicitly to enterprise-controlled telephone numbers for clearly defined use cases (e.g., outbound call centers, support teams, automated messaging systems).

* Define Authorization Policies and Assertions: Clearly specify attributes, roles, and use permissions associated with assertion specific credentials, such as "Authorized Support Agent" or "Verified Financial Representative", enabling recipients to validate authenticity without, if applicable, exposing individual user identities.

* Respond to Misuse and Enable Accountability: Actively monitor and revoke misused or compromised token or certificate credentials, cooperating fully with legal investigations and regulatory compliance efforts by providing auditable, transparent records of usage.

6.1.4. Transparency Log Operators and Notary Agents

Integral to the accountability and auditability of the proposed trust framework are independent, publicly accessible transparency logs, [I-D.wendt-stir-certificate-transparency]. The effectiveness of transparency logs as a public accountability mechanism has been proven through their adoption in the Web PKI ecosystem [RFC6962], where the CA/Browser Forum and major browser vendors mandate Certificate Transparency [CABF.CT] for publicly trusted TLS certificates, ensuring that all issued certificates are publicly logged and auditable to detect mis-issuance or compromise. Transparency log operators have clear responsibilities to:

* Maintain Tamper-Evident, Publicly Accessible Logs: Independently record all cryptographic token issuance, revocation, and delegation events in append-only logs without compromising user privacy.

* Provide Cryptographic Proof of Valid Issuance: Issue Signed Certificate Timestamps (SCTs) and cryptographic receipts for approved Certification Authorities, enabling third parties, such as regulators, service providers, or independent auditors, to verify the legitimacy and proper issuance of identity assertions.

* Ensure Distributed, Transparent Accountability: Facilitate ecosystem-wide oversight without centralizing control or exposing personally identifiable information (PII), allowing rapid detection and remediation of mis-issuance or malicious behavior.

6.2. The Benefits of Federated Governance

Aligning with the existing telephone number administration governance models of ITU-T e.164 [ITU.E164], as a globally adopted standard, this federated governance model follows existing regulatory frameworks and jurisdictional sovereignty, avoiding the pitfalls of centralized or single-party identity management. By clearly defining stakeholder roles, embedding explicit privacy protections, and establishing transparent accountability processes, the framework ensures trustworthiness, regulatory alignment, and balanced liability distribution across the entire telecommunications ecosystem.

Ultimately, deployment through federated governance, guided by cryptographic accountability, clear liability allocation, and user-controlled privacy, creates a sustainable, scalable, and legally robust telecommunications-based digital identity system. This collaborative approach effectively aligns stakeholder incentives, enhances public trust, and provides a comprehensive solution to the complex identity and accountability challenges inherent in modern digital communications.

7. Deployment Models

Implementing a robust telecommunications-based trust framework is both practically achievable and highly compatible with existing infrastructure, regulatory environments, and industry practices. It is designed specifically for incremental deployment, federated governance, and interoperability, balancing innovation, competition, privacy, and accountability within clearly defined legal parameters.

7.1. Incremental Integration with Existing Infrastructure

The proposed trust framework can be incrementally deployed atop established telecommunications systems, leveraging existing infrastructure and call-authentication technologies. Specifically:

* STIR Extensions: Existing STIR protocol supporting infrastructure can readily integrate the use of delegate certificates. By explicitly verifying and documenting Right-to-Use (RTU) through numbering authority-managed processes, the existing framework can be significantly enhanced without wholesale infrastructure replacement.

* Messaging Integration: Messaging platforms and gateways can incorporate cryptographic verification of identity tokens into their existing workflows. Verified identity assertions ensure trustworthiness in messaging applications and services, significantly enhancing fraud prevention and user confidence.

* Broad Application Integration: Other digital applications, such as social media, authentication services, or financial applications can adopt authority tokens and delegate certificates credentials as authoritative proofs of telephone number ownership and verified entity assertions, enhancing security and accountability beyond telecommunications alone.

7.2. Federated Trust Ecosystem

The framework deliberately avoids centralized identity control, instead promoting a federated, interoperable trust ecosystem composed of multiple authorized entities. This federated approach ensures:

* Innovation and Competition: Diverse providers can independently associate verified telephone numbers with business entities and individuals, fostering competition and driving innovation in identity verification and management services.

* Resilience and Ecosystem Diversity: Distributed and federated governance enhances systemic resilience, reducing dependency on any single provider or centralized entity, thereby ensuring robust continuity and adaptability.

* Local Policy Autonomy within Interoperable Standards: Jurisdiction-specific legal and regulatory requirements can coexist seamlessly within an interoperable, global framework, allowing tailored implementations that respect local privacy, data protection, and transparency norms.

7.3. Standards-Based Approach

Core technical components, including token and certificate formats, transparency logs, and verification tools, should be standardized via open, consensus-driven processes and made broadly available through interoperable implementations. This approach promotes:

* Industry and Community-Driven Adoption and Auditability: Open standards based on internationally recognized industry consensus-driven process facilitate broad adoption, rigorous security audits, and continuous community-driven improvements, strengthening overall system integrity and trustworthiness.

* Accessibility for Smaller Providers and End-Users: Clear standards and competitive and accessible implementations enable smaller providers and end-users to rapidly integrate solutions, leveling competitive playing fields and fostering widespread adoption.

* Transparency and Trust in Technical Mechanisms: Publicly available standards and implementations reassure users, regulators, and service providers that the underlying identity verification mechanisms are secure, privacy-preserving, and independently verifiable.

8. Conclusion: The Case for VESPER as the Future of Trusted Digital Identity

Throughout this document, we have explored the urgent challenges facing digital communications today; rampant caller impersonation, ambiguous accountability, fragmented privacy protections, and inconsistent regulatory environments. The current landscape leaves consumers vulnerable, enterprises exposed, providers burdened, and regulators struggling to enforce accountability effectively. The VESPER framework, as outlined, directly addresses these challenges by fundamentally strengthening trust and accountability through authoritative and cryptographically verifiable identity assertions anchored explicitly in telephone numbers.

Reflecting on the core foundations and principles, VESPER achieves four critical objectives essential for robust trusted digital identity:

* Authoritative Assignment and Non-Repudiation: By cryptographically binding telephone numbers directly and explicitly to their legitimate assignees through digital signatures and delegate certificates, VESPER establishes undeniable proof of Right-to-Use (RTU). This directly deters fraud and spoofing, clarifies responsibility, and significantly simplifies regulatory enforcement by eliminating ambiguity.

* Privacy-Preserving Transparency: VESPER uniquely integrates Authority Tokens and independent Notary Agents managing publicly verifiable, tamper-evident transparency logs. This provides robust accountability without sacrificing user privacy. End-user personally identifiable information (PII) remains protected and confidential, disclosed only through explicitly authorized legal processes. Users maintain control over identity disclosures, achieving privacy by design rather than merely policy.

* Clear, Objective Allocation of Liability and Regulatory Safe-Harbor: Telecommunications providers performing verification steps, checking delegate certificate chains, Authority Tokens, and transparency receipts, objectively demonstrate due diligence consistent with established digital-signature legal frameworks. Providers thus gain clear regulatory safe-harbors, incentivizing broad adoption, promoting fairness, and significantly reducing liability risk and compliance burdens.

* Accountability and Regulatory Confidence via Non-Repudiation: Digital signatures and immutable transparency logs enable precise legal attribution, explicitly identifying responsible entities whenever misuse occurs. Non-repudiation ensures malicious actors inherently self-incriminate, greatly simplifying legal investigations and restoring regulatory confidence and effectiveness.

Moreover, through the illustrative use cases provided, trusted caller ID, secure enterprise communication, reputation-based digital services, and public safety alerts and communications, VESPER demonstrates its practical versatility. The framework directly enhances consumer protection, enterprise security, public confidence, and regulatory efficacy, effectively balancing privacy and accountability across multiple scenarios.

Deployment models discussed emphasize incremental integration with existing STIR/SHAKEN infrastructures, federated governance preserving innovation and autonomy, and open standards promoting transparency and adoption. Legal and regulatory compatibility is explicitly preserved, respecting established telecommunications laws, international privacy standards, and due process rights. Explicit mechanisms ensure lawful attribution is tightly controlled, auditable, and compliant with legal and digital rights norms.

In summary, the telecommunications-based trust framework represented by VESPER offers a clear, scalable path forward. It resolves longstanding tensions between anonymity and accountability, aligns legal clarity with cryptographic security, and balances individual privacy with regulatory effectiveness. By explicitly tying telephone numbers to authoritative, cryptographically verifiable identity proofs, VESPER delivers the high-assurance, privacy-preserving trust model that today’s digital ecosystem urgently requires. It is not merely an enhancement; it represents the logical evolution of digital identity, built upon existing regulatory foundations and strengthened through advanced cryptographic assurance, providing the trust, accountability, and transparency essential to the future of digital communications.

9. Security Considerations

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

10. IANA Considerations

This document has no IANA actions.

Acknowledgments

The author of this document acknowledges and wants to thank the years of industry interactions and innovations that led to this framework, it is the contribution of many that helped to form the fundamentals for how the legal and policy frameworks meet the use of the technical frameworks involved.

References

Normative References

[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.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>.

[I-D.wendt-stir-certificate-transparency]
Wendt, C., ナ嗟iwa, R., Fenichel, A., and V. A. Gaikwad, "STI Certificate Transparency", Work in Progress, Internet-Draft, draft-wendt-stir-certificate-transparency-06, 11 June 2025, <https://datatracker.ietf.org/doc/html/draft-wendt-stir-certificate-transparency-06>.

[I-D.wendt-stir-vesper]
Wendt, C. and R. ナ嗟iwa, "VESPER - Framework for VErifiable STI Personas", Work in Progress, Internet-Draft, draft-wendt-stir-vesper-04, 7 July 2025, <https://datatracker.ietf.org/doc/html/draft-wendt-stir-vesper-04>.

[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>.

[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>.

Informative References

[ATIS.LoA] Alliance for Telecommunications Industry Solutions (ATIS), "ATIS Inter-Carrier Call Processing (ICCP) Letter of Authorization (LOA) Best Practices", ATIS ATIS-0300251, 2016, <https://access.atis.org/apps/group_public/download.php/33136/ATIS-0300251.pdf>.

[ATIS.TFLOA] Alliance for Telecommunications Industry Solutions (ATIS), SMS/800 Number Administration Committee (SNAC), "Toll-Free Number (TFN) Access Guidelines", ATIS ATIS-0300112, 2017, <https://access.atis.org/apps/group_public/download.php/41219/ATIS-0300112.pdf>.

[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/>.

[COE.Cybercrime] Council of Europe, "Convention on Cybercrime (Budapest Convention)", Treaty ETS No.185, 2001, <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>.

[EU.eIDAS] European Parliament and Council, "Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)", EURegulation Regulation (EU) No 910/2014, 2014, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910>.

[EU.ePrivacy] European Parliament and Council, "Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive)", EUDirective Directive 2002/58/EC, 2002, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002L0058>.

[FATF.KYC] Financial Action Task Force (FATF), "Customer Due Diligence for Financial Institutions", FATF CDD Guidance (Recommendation 10), 2017, <https://www.fatf-gafi.org/content/dam/fatf-gafi/images/guidance/Updated-2017-FATF-2013-Guidance.pdf.coredownload.pdf>.

[FCC.NumberPorting] Federal Communications Commission (FCC), "Number Portability: Rules and Orders", FCC Porting Rules, 2023, <https://www.fcc.gov/general/number-portability>.

[FinCEN.CDD] Financial Crimes Enforcement Network (FinCEN), "Customer Due Diligence Requirements for Financial Institutions", FederalRegister 81 FR 29397, 2016, <https://www.fincen.gov/resources/statutes-and-regulations/cdd-final-rule>.

[ITU.E164] ITU-T, "The International Public Telecommunication Numbering Plan", ITU-T E.164, 2010, <https://www.itu.int/rec/T-REC-E.164/en>.

[NANPA.Plan]
North American Numbering Plan Administrator (NANPA), "North American Numbering Plan (NANP)", NANPA NANP Overview, 2025, <https://www.nanpa.com/about>.

[NIST.SP.800-63]
Temoshok, D., Proud-Madruga, D., Choong, Y.-Y., Galluzzo, R., Gupta, S., LaSalle, C., Lefkovitz, N., Regenscheid, A., and National Institute of Standards and Technology (NIST), "Digital Identity Guidelines", NIST SP 800-63-4, 2025, <https://doi.org/10.6028/NIST.SP.800-63-4>.

[NIST.SP.800-63A]
Temoshok, D., Abruzzi, C., Choong, Y.-Y., Fenton, J., Galluzzo, R., LaSalle, C., Lefkovitz, N., Regenscheid, A., Vachino, M., and National Institute of Standards and Technology (NIST), "Digital Identity Guidelines: Enrollment and Identity Proofing Requirements", NIST SP 800-63A, 2025, <https://doi.org/10.6028/NIST.SP.800-63a-4>.

[US.E-SIGN]
United States Congress, "Electronic Signatures in Global and National Commerce Act", USCode Title 15, Chapter 96, 2000, <https://www.govinfo.gov/content/pkg/USCODE-2022-title15/html/USCODE-2022-title15-chap96.htm>.

[US.SCA] United States Congress, "Stored Communications Act (SCA), 18 U.S. Code Chapter 121", USCode 18 U.S.C. 2701-2712, 1986, <https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121>.

Author’s Address

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