



VESPER Framework: A Path to RTU and Verifiable Trust for Telephone Numbers

Chris Wendt

VP, System Engineering, Somos, Inc.

Co-Chair - IPNNI, STI-GA-TC, IETF vcon WG,
CFCA TTWG

Board Director, SIP Forum

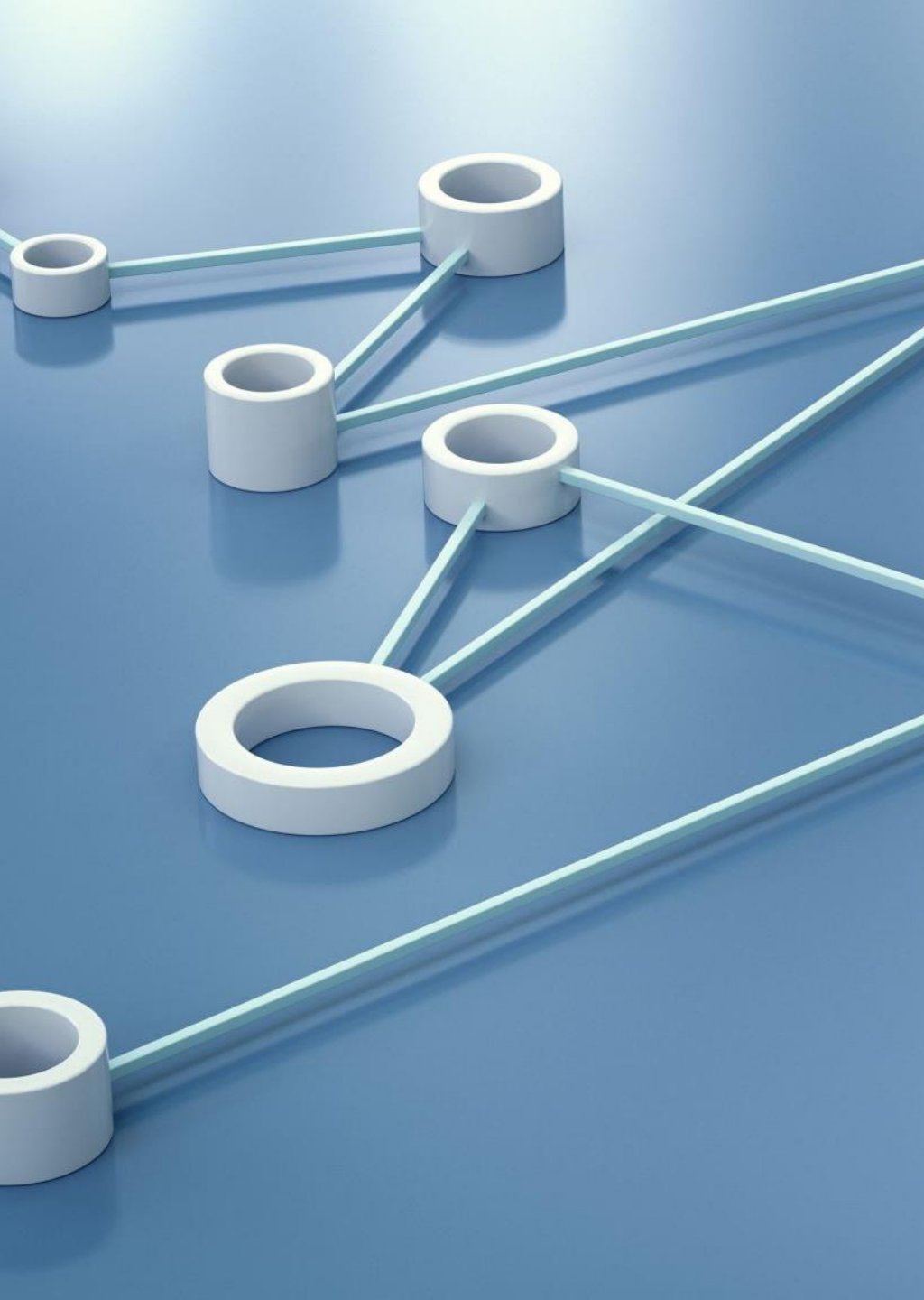
Defense without Offense Does Not Win Games

Scoring Points Requires Offense

- Blocking bad calls is necessary, but insufficient.
- We must enable **trusted communications end-to-end**.
- We must enable **trusted RTU and KYC end-to-end**.
- Trust needs to be **provable** and **linked to the end entities**

Use of telephone numbers is a privilege with responsibilities.





From Network Trust to Entity Trust

STIR/SHAKEN – Got Us Started

- Verifies who put the call on the network.
- Assists traceback and accountability.
- Attestation is subjective and inconsistently applied.

VESPER

- Builds on STIR using delegate certificates.
- Authenticates the actual entity calling.
- Enables trusted branding and caller identity.

VESPER doesn't replace STIR/SHAKEN – it builds **on top**




Offense + Defense wins games

Why VESPER?

KYC is essential at the Responsible Provider level:

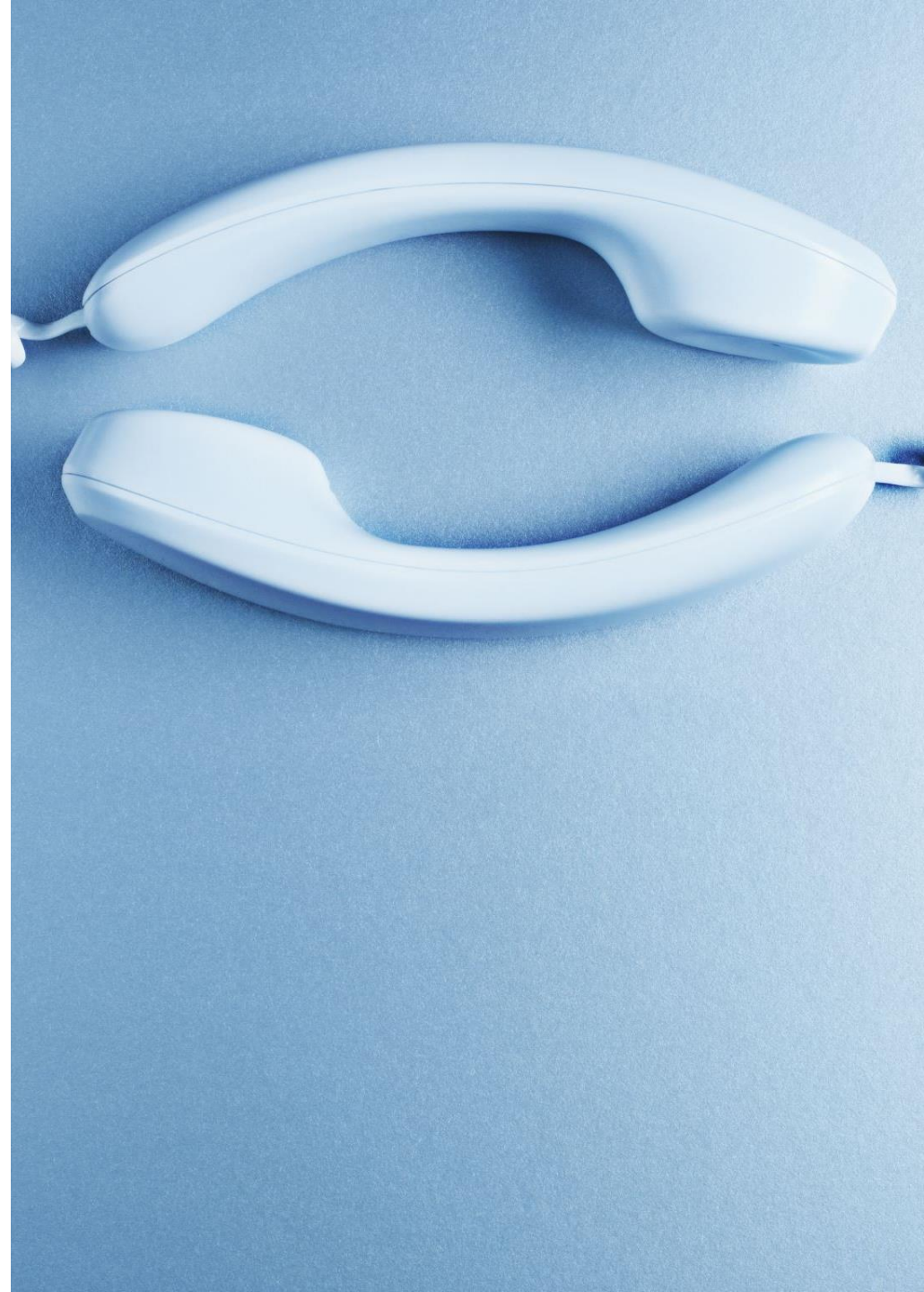
- Confirms: *“They are who they say they are”*
- Provides: A pathway for law enforcement accountability
- Enables: Onboarding metadata and Rich Call Data (RCD)

But for the telephone network KYC alone isn’t enough...

-  It proves trust *to the provider* – not the entire ecosystem
-  It doesn’t scale trust across multiple carriers or verifiers
-  It lacks a public, cryptographically verifiable representation

VESPER answers these challenges:

- Extends KYC outcomes via **notarized Right-to-Use (RTU)** claims
- Leverages **Authority Tokens + Certificates**
- Makes trust *external, provable, and auditable* by anyone via transparency
- Integrates into **existing certificate-based call authentication**



The Opportunity: Trust at Scale

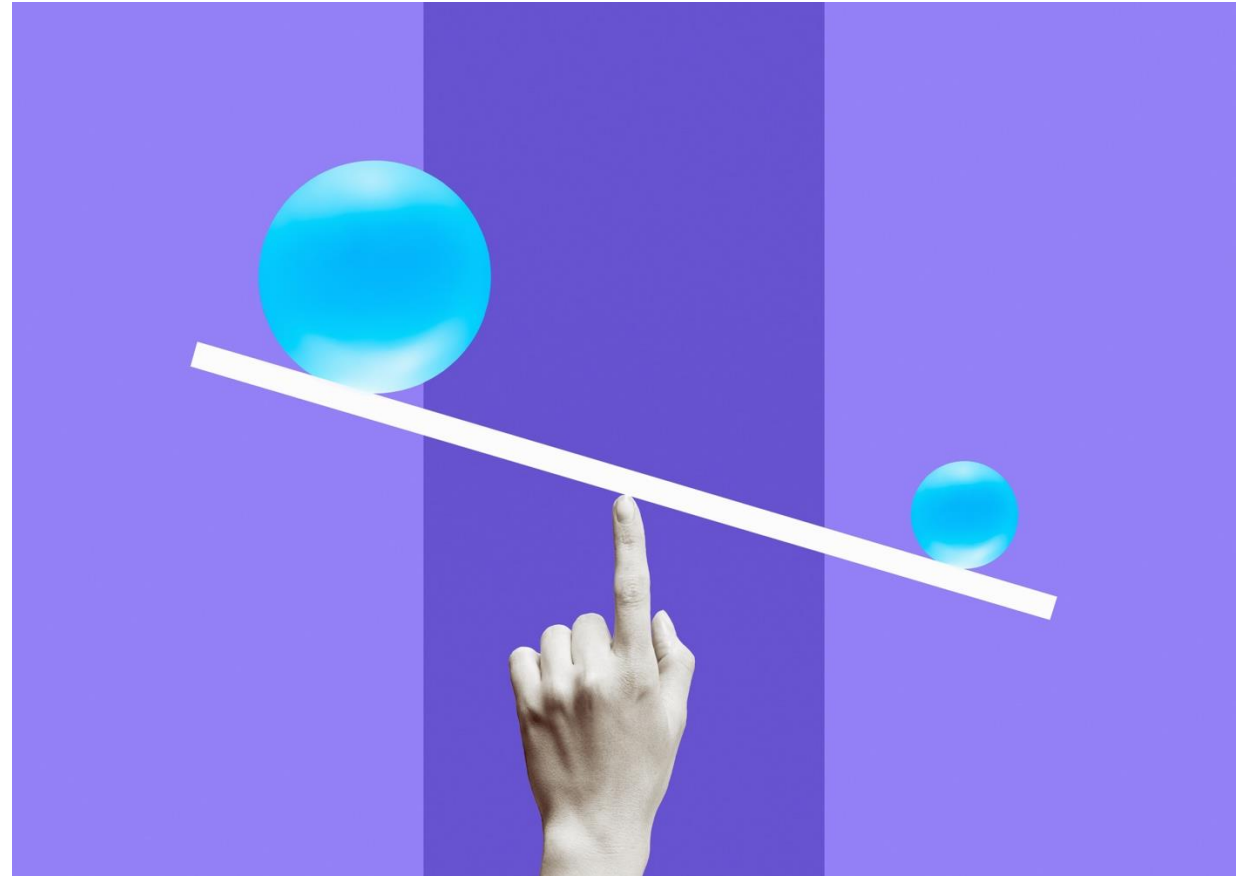
I'm not proposing we need to apply VESPER to all calls


Not everyone expects/needs/wants branding

But those that want it need **verifiable ties to trusted telephone numbers** at telecom scale

Transparency that only they can rightfully initiate calls

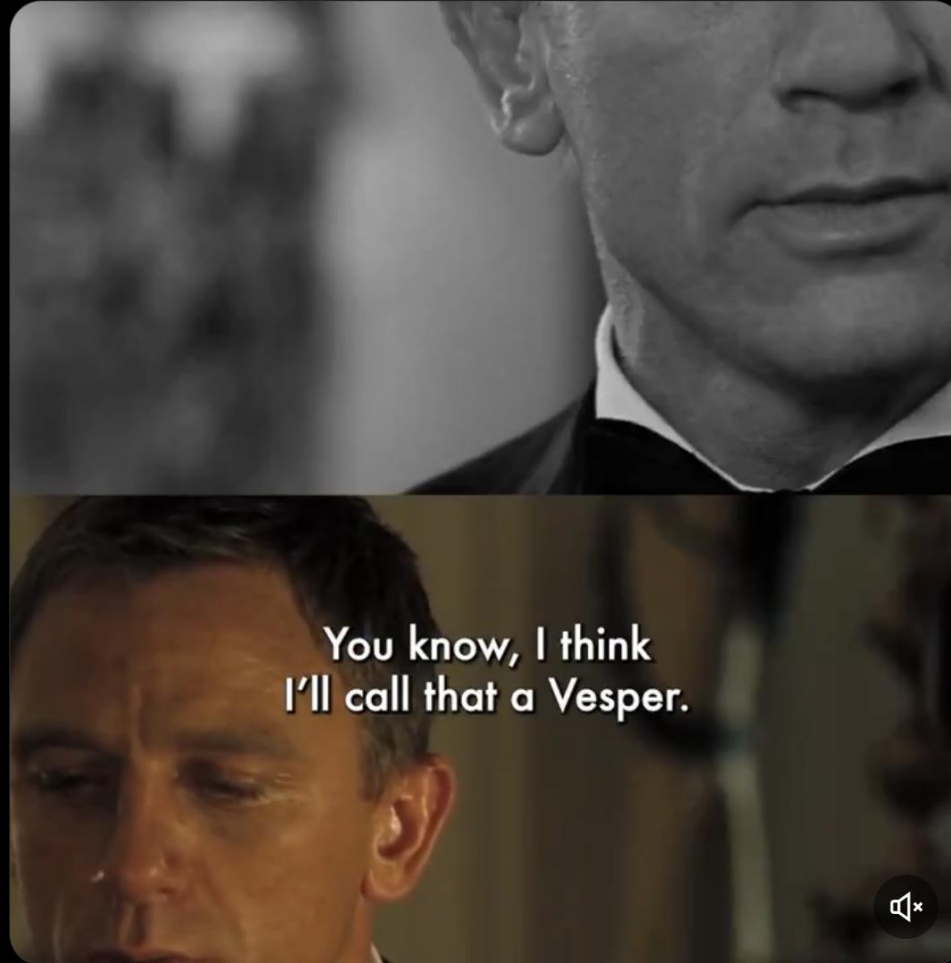
signed with RTU established or with vetted Rich Communications information



James Bond  @007 · 14h ...

007 The Vesper Martini. Once you've tasted it, it's all you want to drink.

[#NationalMartiniDay](#) [#CasinoRoyale](#)
[#JamesBond](#) [#DanielCraig](#)



 21  295  1.6K  55K  

VESPER: Extending Trust Beyond KYC

KYC and Entity validation is critical

- VESPER builds on KYC by enabling **ecosystem-wide, transparent trust**.
- Right-to-Use (RTU) claims are notarized and verifiable.
- **Trust becomes portable and visible.**
- Verified associations between telephone numbers and entities are **made visible to all parties**, not just a single provider.
- **Supports both transparency and privacy.**
 - Businesses, governments, and public entities can **publicly declare** identity and RTU.
 - Individuals retain **control and privacy** over their identity disclosures.





Core Principles of VESPER

Grounded in Trust and Privacy

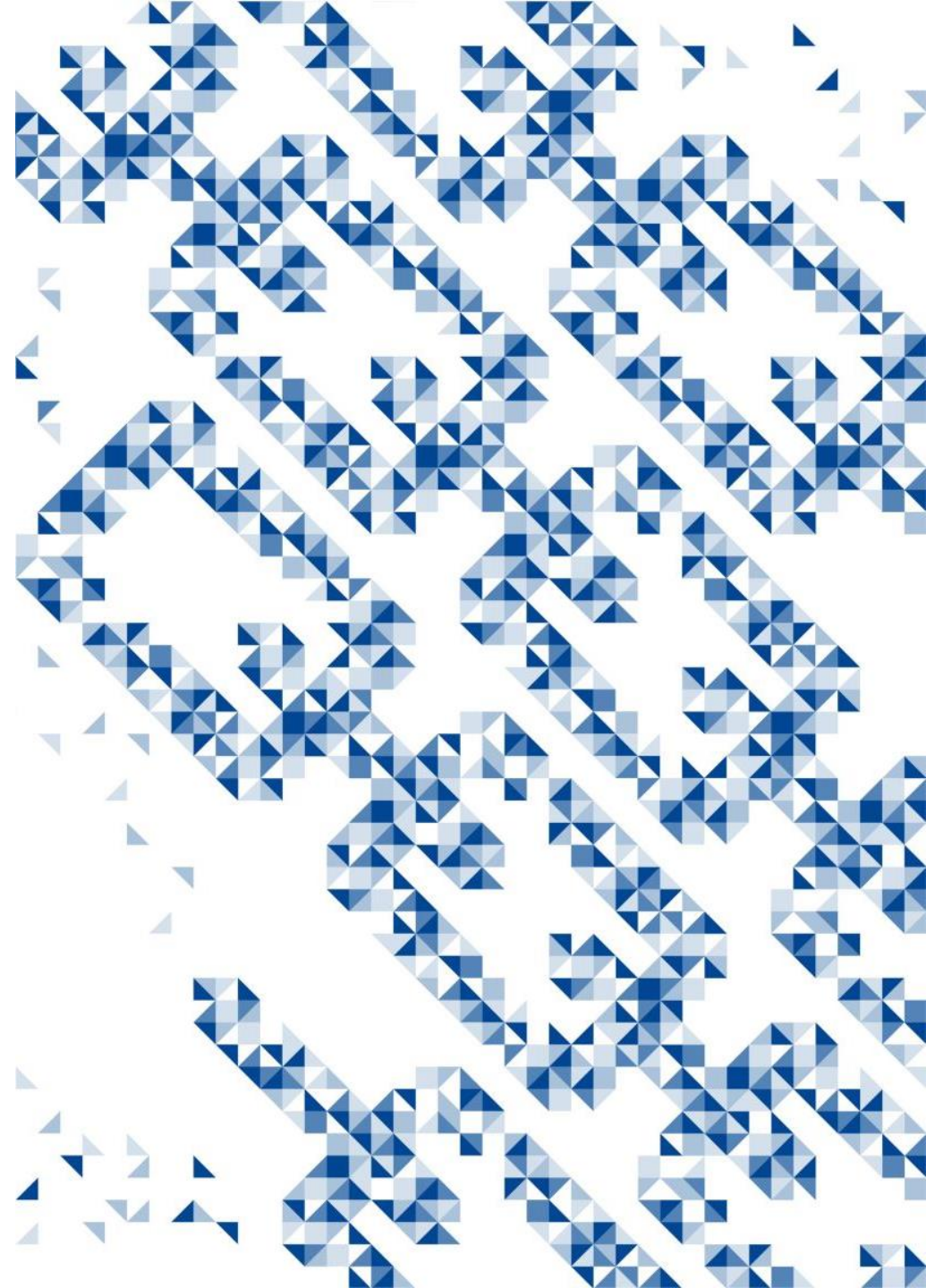
- **Right-to-Use (RTU) – Entities** utilize verifiable proof they're authorized to use a number tied to assignment.
- **Responsible Organizations and Providers** - Validate and safeguard number assignments to **Entities**
- **Vetting/KYC + Transparent Notarization** - Everything logged and verifiable by the eco-system that depends on it.
- **Privacy by Design** - Disclosure only when needed, but privileges may be limited depending on policies.

RTU + Transparent Notarization

Adding the Missing Layer of Verifiable Accountability

1. **TN Authority Token** - Confirms that an entity has the right to use a specific telephone number. (like issuing a license to use a resource)
2. **Claim Constraint Authority Token** – Based on vetted association of claims (beyond telephone number) to the Entity
3. **Transparent Notarization** - Cryptographically signs and timestamps the claim, linking it to the asserting party. (like notarizing a legal claim or filing)
4. **Auditable Transparency Log** - Logs the claim in a tamper-evident, verifiable log. (like a public land or title record)

This framework creates external visibility into what would otherwise be internal, unobservable KYC decisions – providing a critical check against weak or misused vetting.



Certificate Transparency

Well-established framework already mandated by CABrowser Forum in WebPKI

Public Logging of Certificates

- Every VESPER-issued certificate must be recorded in a tamper-evident transparency log.

Signed Certificate Timestamps (SCTs)

- SCTs act as cryptographic receipts proving the certificate has been logged properly.

Defense Against Mis-issuance

- Prevents unnoticed or fraudulent issuance of certificates – any misbehavior is publicly visible.

Ecosystem-Wide Auditability

- Anyone (verifiers, regulators, watchdogs) can monitor CT logs for anomalies or abuse.

Accountability at Scale

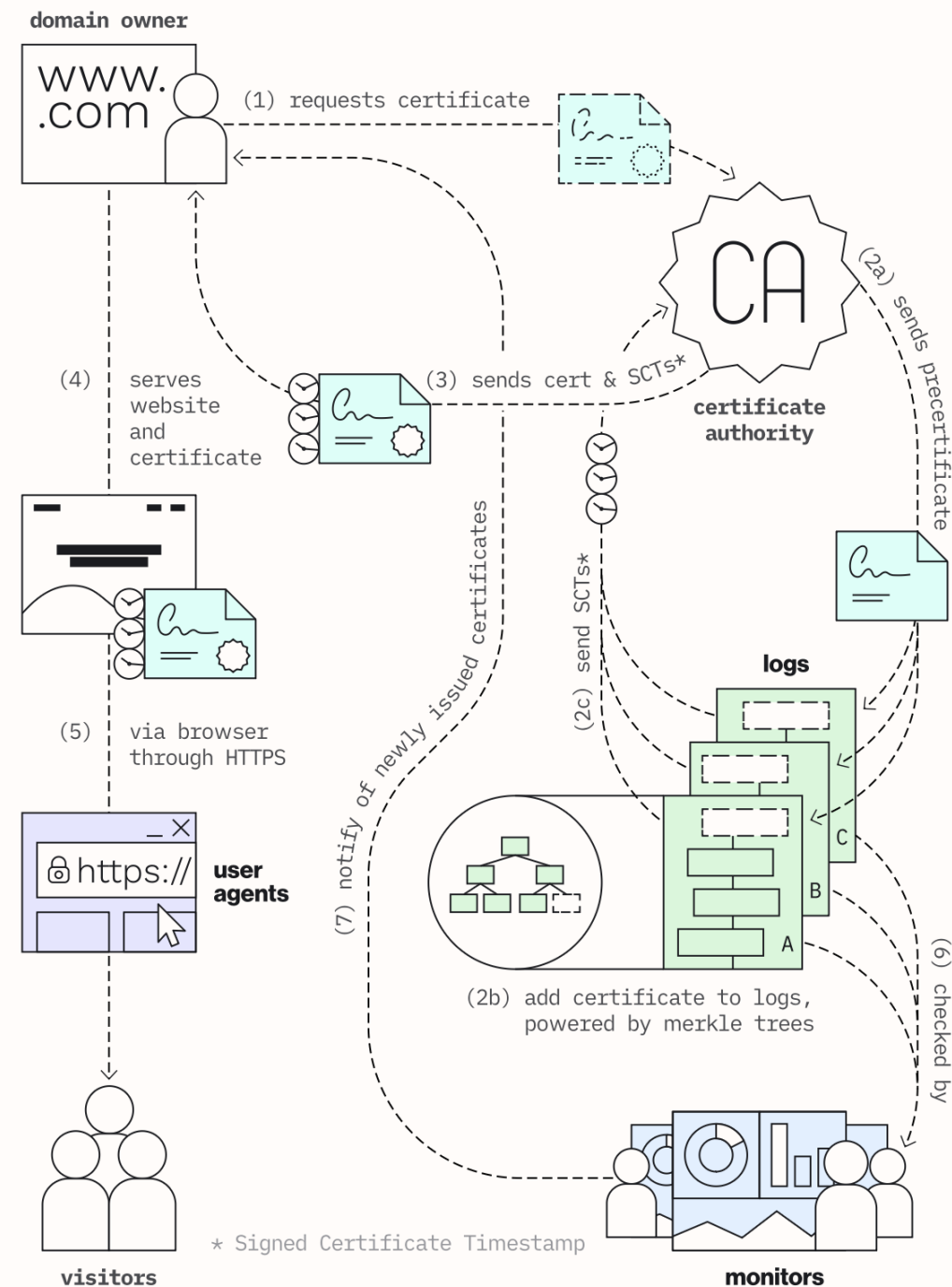
- Supports decentralized trust by removing reliance on any single authority – logs are append-only and verifiable by anyone.

Real-Time Monitoring

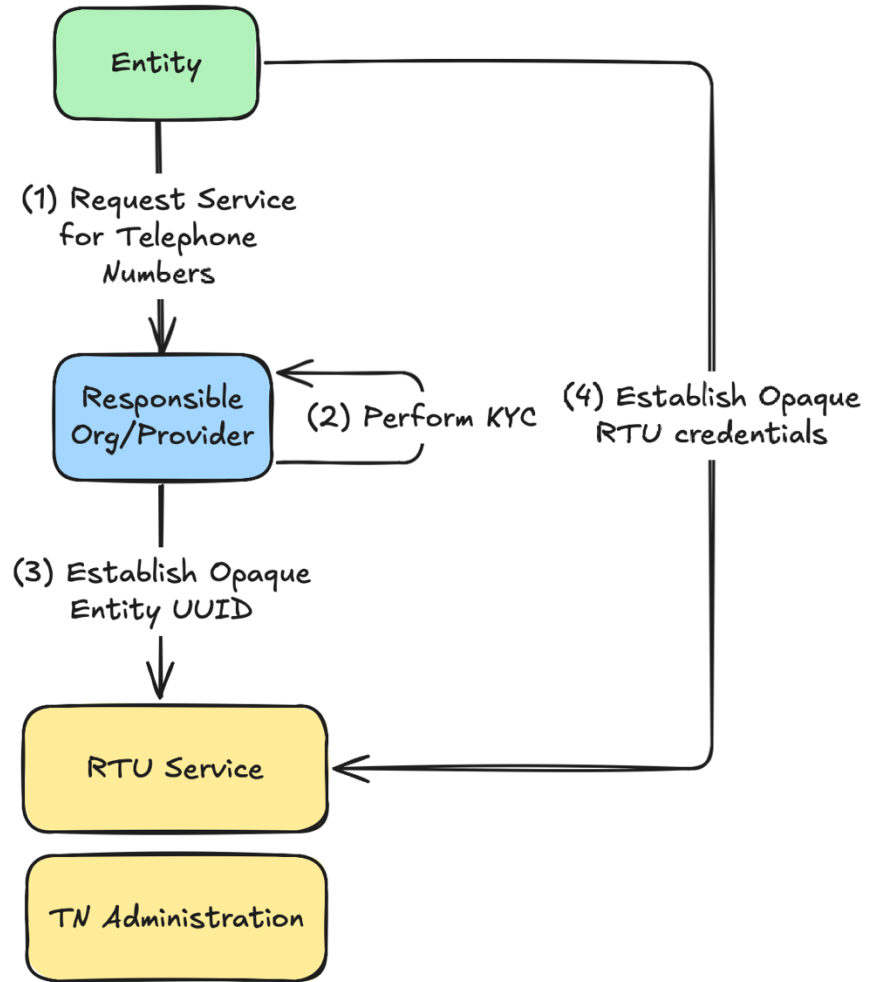
- Transparency monitors continuously scan CT logs for suspicious or misused certificates.

Foundation for Ecosystem Trust

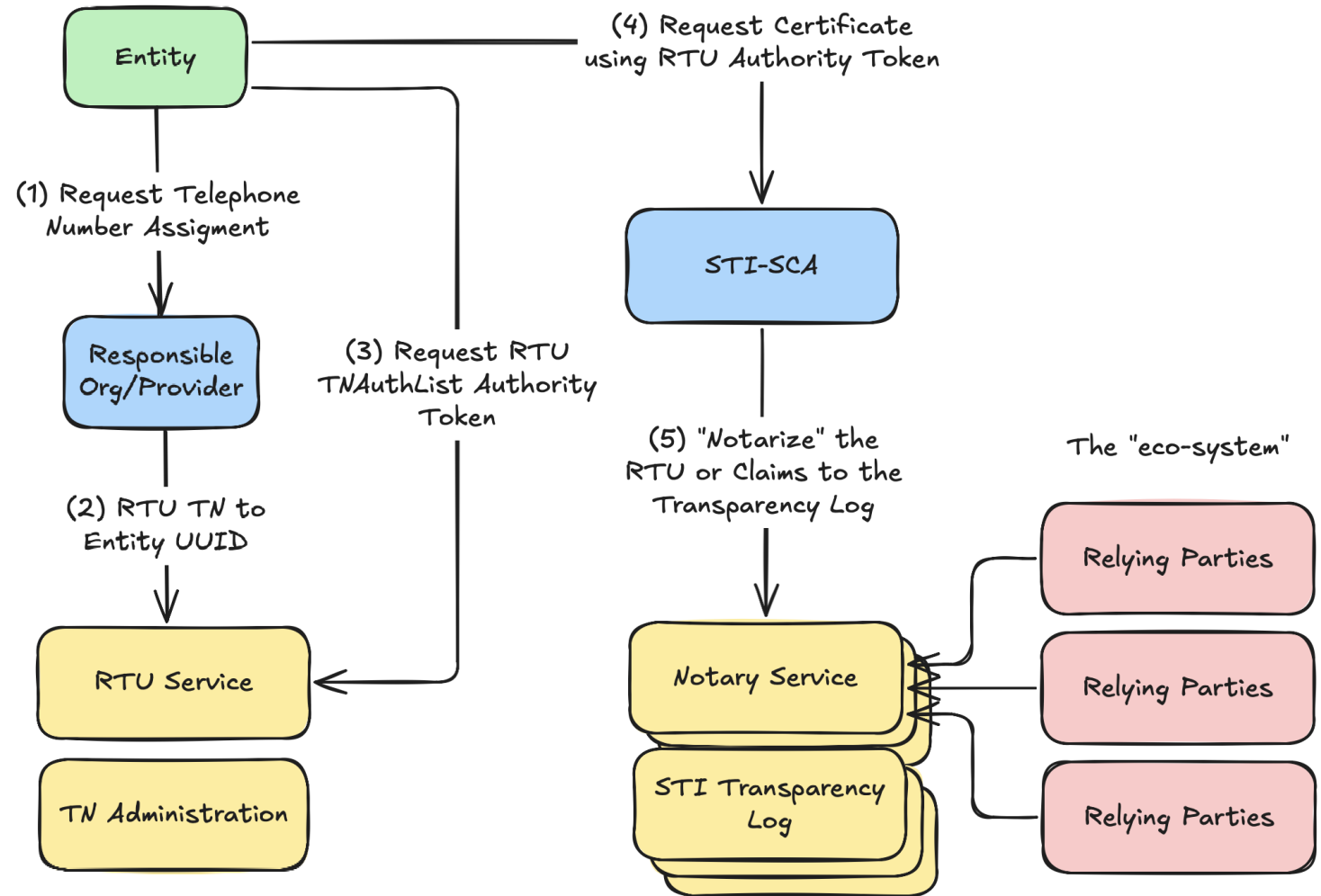
- Enables public proof of identity assertions and RTU claims, not just private onboarding validation.



How does it work?



Onboarding



RTU Establishment and "Notarization"



Play Ball!

- Vesper is a **proposed** set of protocol specifications that represent a trust framework that **wraps** what we've established with STIR authentication, certificates, and authority tokens
- Create a scalable, verifiable path for governing the distribution of trust across an eco-system based on widely used well-establish transparency mechanisms used in WebPKI for domain certificates
- Looking to collaborate to take the best of what we have started in various parts of the industry into a consensus single path forward