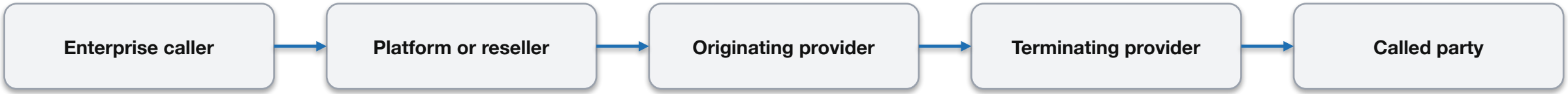
SIPNOC 2026
Accountable end to end

VESPER and DNO+ — right-to-use, domain identity, and authorization-first origination



DNO+ scopes who may originate

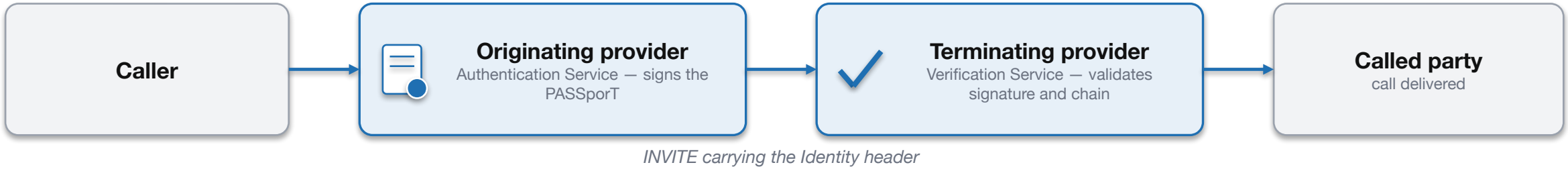
VESPER carries what the provider cannot

both have to arrive

Chris Wendt
Somos, Inc.
IETF STIR · IETF vCon WG co-chair · ATIS/SIP Forum IP-NNI · CFCA Trust and Transparency Working Group · US STI-GA Technical Committee

SHAKEN, briefly

Deployed across the US since 2019, and it does the job it was built for.



What it establishes

- The calling number was not modified in transit
- The call was signed by a provider holding a credential for that number or SPC
- The signing provider is identified, on every call, to everyone downstream

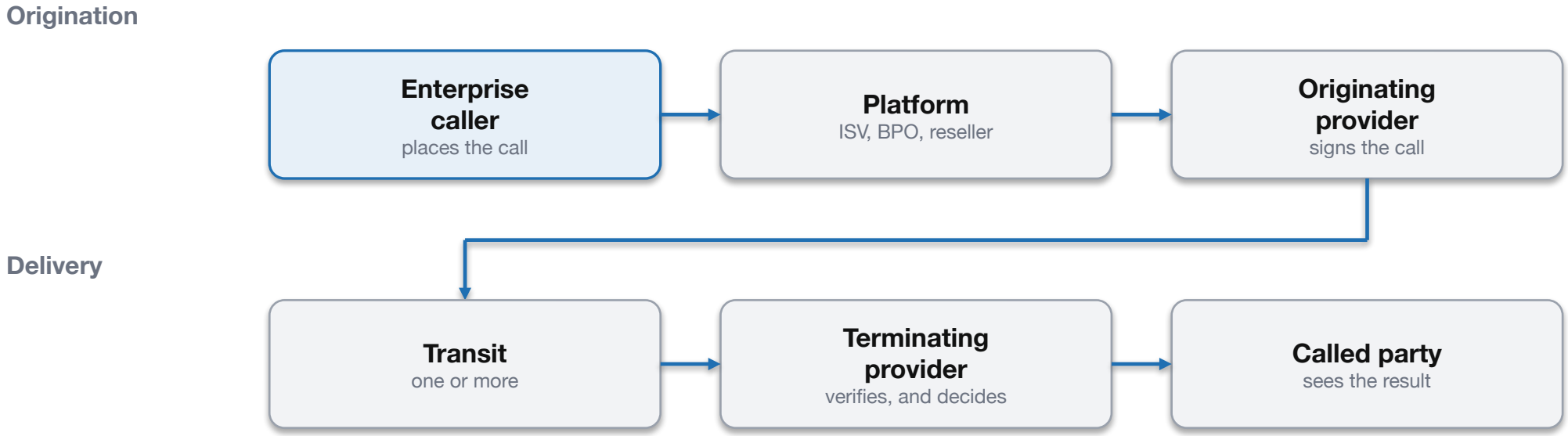
Where it started — the provider level

- A TNAuthList (RFC 8226) holds either a service provider code or telephone numbers
- SHAKEN deployed the SPC form, so the credential identifies the provider that signed
- The TN form was in the design from the start, and is the part not yet deployed

SHAKEN authenticates the provider, not the caller. That was the starting point, not the limit of the design. What this talk is about is the move from provider-level to TN-level authentication.

The call path is not two parties

Caller, provider, provider, called party is the mental model. The calls that matter are longer.



What each hop can do

- See the call, alter what it carries, and hand it onward
- The provider that signs may have no view of the party that placed the call
- Anything travelling with the call has to survive every hop to the decision point

Three things get authenticated

Only one of them is the party placing the call.

The caller

- **What** — the entity placing the call, and its right to use the number
- **Mechanism** — delegate certificate — the number holder's own STI certificate, RFC 9060
- **Asserted by** — the entity that holds the number
- **Scope** — carried end to end
- **Where** — in the IETF now

The provider

- **What** — which provider originated the call, and what it knows about its customer
- **Mechanism** — SHAKEN PASSporT — attestation A, B or C
- **Asserted by** — the originating provider, about itself
- **Scope** — carried end to end
- **Where** — deployed since 2019

The network

- **What** — the connection between two providers, and the routing it carries
- **Mechanism** — mutual TLS between session border controllers
- **Asserted by** — the peer operating the interface
- **Scope** — one hop
- **Where** — being specified now for all-IP interconnection

Agreement-less IP interconnection

SHAKEN is the middle column. It travels end to end, and what it asserts is about the provider — not about the caller.

An attestation is an opinion, not a proof

Start from the Commission's own definition. Three things it leaves open, and all three sit at the caller level.

> *“a voice service provider’s assertion about the knowledge it has of its customer and the customer’s right to use a telephone number”*
> Know Your Upstream Provider FNPRM, FCC 26-32, ¶ 54

- **Nothing downstream can check it** — an assertion about knowledge is an opinion. The right-to-use behind even a properly applied A is confirmed inside the provider, and no evidence of it travels with the call
- **Nothing says which providers were authorized** — an enterprise using five providers has no way to say which five, and no way to say a sixth is not one of them
- **Nothing guarantees it arrives** — a credential can be verified at the first hop and silently dropped. Any TDM segment in the path removes the Identity header outright — every credential, of every kind

Codifying the levels raises the floor. A right-to-use credential raises the ceiling — proof that a named entity holds the number, carried to the decision point.

What each level commits to, and who answers

Read as grades they are a ranking. Read as what they say, A and B are a commitment, C is an honest refusal to make one, and a certificate is a third party stepping forward.

A and B — I vouch for this customer

- "Knows the customer" means an authenticated UNI — a session the provider authenticated to a known account
- **A** — and the provider has itself confirmed right-to-use
- **B** — but it cannot confirm authority over that number
- Traceback comes to it, and for an A it is offering its own name

C — I am a conduit

- The call arrived over an NNI or peering interface, or from an unauthenticated UE
- No authenticated session ties the call to a known account
- Accurate, and not a deficiency — but it leaves nobody on the call to answer for it

Delegate certificate present

- The caller self-identifies, cryptographically
- Traceback goes directly to that entity
- And to the TNSP that issued the credential, which decides whether it keeps being issued

A certificate does not dilute accountability. It routes it to the party best placed to answer, and to the one that can withdraw the credential.

Why right-to-use is hard to establish

The number took its own path to the party using it, and it is not the call path.

How a number reaches the caller

- Allocated to a carrier out of the numbering plan
- Assigned to that carrier's customer — often a reseller
- Sublet onward to a platform, ISV or BPO
- Provisioned to the enterprise or call centre that places the call
- Every step is a commercial relationship, not a registry entry

What nobody has

- An authoritative record of where the number ended up
- The assigning carrier knows its own customer, not that customer's customers
- Numbers port, churn and get reassigned, so any snapshot is stale

What passes for proof

- A letter of authorization, or a copy of a phone bill
- Both are trivially forged, and checked by eye when they are checked at all
- Never revisited once filed
- No relying party outside the transaction ever sees either one

Right-to-use is the fact that most directly prevents spoofing. Both open FCC proceedings circle it — KYC (FCC 26-27) on what a provider must establish about its customer, KYUP (FCC 26-32) on what it must establish about the provider handing it traffic. Both impose process, and process does not travel past the organization that performs it.

Where the caller has to carry its own proof

The multi-hop cases, now as a requirement.

Where the provider cannot vouch

- The enterprise is behind a platform, ISV, BPO or reseller — more than one hop from the signing provider
- Multi-homed across providers, or moving between them
- The call crosses a border, where no foreign provider holds US numbering authority
- There is no call at all — porting, onboarding, provisioning

Where the provider will not vouch

- It knows its customer, but will not take sole responsibility for that number
- B or C is the honest answer, and the certificate carries what the provider will not
- Its own name stays off a commitment it cannot keep
- That determination stays the provider's own

VESPER

What the caller presents is proof of right-to-use — an authenticated claim on the number, made by the party that holds it, rather than a provider vouching for what it cannot check.

VESPER — a profile of STIR building blocks

RFC 9060 defined the delegate certificate in 2021. What it left open — who issues one, on what evidence, and how a relying party knows the entity behind it — is what VESPER supplies.

TN ⇄ Domain Binding
draft-wendt-stir-tn-domain-binding-02
New — standalone draft

Certificate Transparency
draft-ietf-stir-certificate-transparency-04
With the IESG — AD evaluation

Short-lived Certificates
draft-ietf-stir-certificates-shortlived-06
With the IESG — IESG evaluation

Delegate Certificates
RFC 9060
Existing STIR

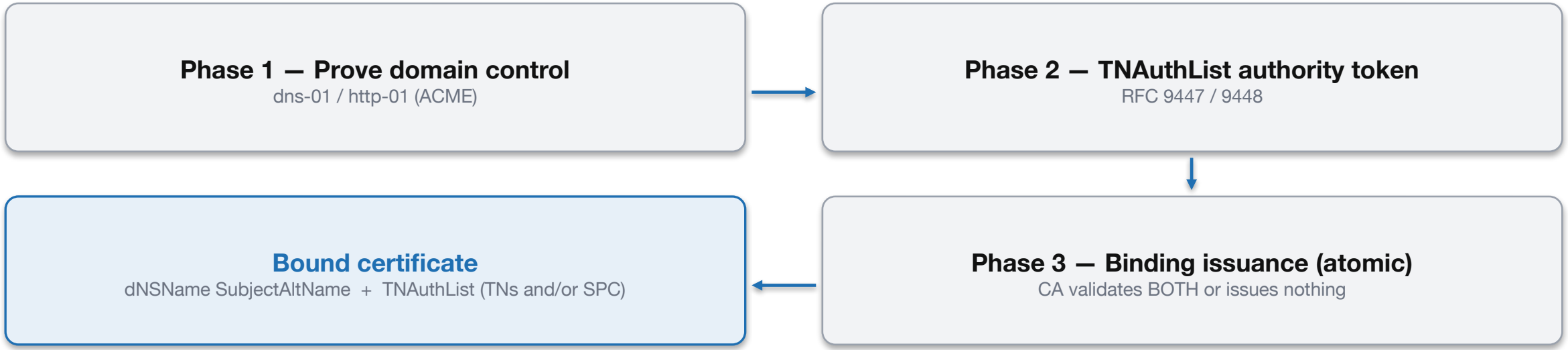
Authority Tokens (ACME)
RFC 9447 / 9448 · JWTClaimConstraints
Existing STIR

Connected Identity
RFC 9970
Existing STIR

What VESPER supplies is the issuance story — who issues the credential (an RTU Authority, through ACME authority tokens), on what evidence (KYC of the entity and of its right to use, performed once at issuance), and how a relying party that had no part in that KYC can still check its result (the domain binding, publicly logged).

TN ⇄ domain binding

A domain name in the certificate SubjectAltName, validated with existing ACME domain validation and co-validated with telephone-number authority into a single certificate.



Neither chain is derivable from the other. Compromising the binding requires both.

KYC establishes the entity. The domain makes it provable.

Both are needed and they do different jobs. The working group's objection to earlier approaches was that business identifiers are jurisdictionally variable, and tying a protocol to national registration policy is out of IETF scope.

KYC — once, at issuance

- Before any certificate exists, someone verifies who the entity is and that it holds the numbers
- That is necessary work, and nothing here replaces it
- It is a judgment made once, by one party, inside one organization — so it does not travel

The domain — every time, by anyone

- The verified entity is bound to a name anyone can resolve
- The certificate is publicly logged, so the binding is checkable in real time
- A relying party that had no part in the KYC can still check its result
- No bilateral trust, no new registry, nothing to ask the originating provider

KYC is required, and its result is what has to travel. Binding the verified entity to a globally unique, publicly verifiable identifier is what makes that verification transitive.

Two trust anchors, bound in one certificate

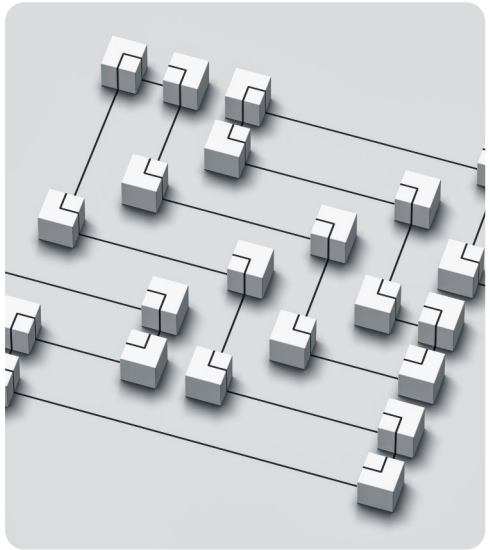
Both are already deployed at production scale, and both already have mature governance. VESPER binds them rather than replacing either.

STIR trust anchor

- Anchored by telephone-number authority — FCC-overseen, STI-GA governance
- In production since 2019 across the US voice ecosystem
- Jurisdictionally bound to the NANP and national numbering plans

WebPKI trust anchor

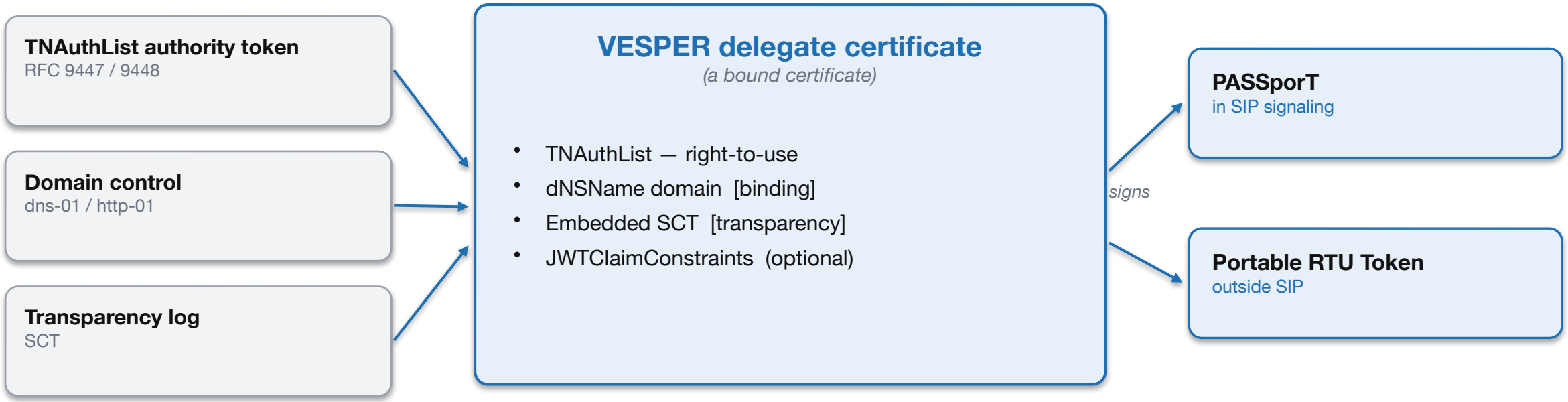
- Anchored by domain authority — CA/Browser Forum governance, Certificate Transparency
- Deployed globally; billions of verifications a day
- Globally federated — works across jurisdictions without bilateral agreements



Binding them inside the same certificate produces one verifiable assertion: this telephone number is authorized to this entity at this domain.

How VESPER composes the blocks

Everything a relying party needs is encapsulated in one certificate.



Relying party verifies chain to an STI trust anchor · TNAuthList authorizes orig · embedded SCT · binding rule: x5u domain = dNSName · claim constraints

Authentication and verification profile

Standard PASSporTs, standard X.509 chain validation, plus one binding rule.

Authentication Service (originating)

- Construct PASSporT: orig, dest, iat, optional claims
- Sign with a VESPER delegate cert whose TNAuthList authorizes orig
- Convey the chain inline via x5c
- x5u → the certificate at its domain-hosted repository

Verification Service (terminating)

- Validate signature; chain to an STI trust anchor
- Confirm TNAuthList authorizes orig
- Validate the embedded SCT; check claim constraints
- Binding rule: x5u domain matches the dNSName SubjectAltName

Optional Connected Identity: the destination returns a rsp PASSporT signed by a delegate certificate authorized for dest — mutual verification of both parties.

The portable RTU Token

A JWT signed by the delegate certificate's private key, chain in the x5c header. The one genuinely new normative item in the draft.

Claims

- **iss** — the entity's domain, matching the dNSName
- **iat / exp** — short-lived by design
- **orig** — the telephone number being asserted
- **optional** — claims where JWTClaimConstraints authorizes them

Where it is used

- Number-portability and porting validation
- Onboarding an enterprise to a new originating provider
- Registry, RespOrg and platform provisioning checks
- Anywhere there is no call to carry a PASSporT

The replacement for the letter of authorization — the same question, answered by a credential instead of a PDF.

DNO today — and the tier that is missing

Do Not Originate is a default-deny mechanism on calling-number provenance, codified at 47 CFR § 64.1200(o) and extended by the Eighth Report and Order from gateway providers to every provider in the call path. It already works. It just does not reach the numbers that matter most.

Tier 1 — cannot originate
invalid, unallocated and unassigned numbers
deployed

Tier 2 — will not originate
subscriber-requested DNO; the IRS taxpayer assistance line is the canonical example
deployed

Tier 3 — originate only under declared conditions
the numbers an enterprise does use, through the providers it chose
DNO+ — proposed

- Most high-value telephone identity falls outside both existing tiers — numbers that do legitimately originate, but only under conditions the holder can state
- Same distribution mechanism, enhanced per-number records — no new infrastructure

It changes the question from "who signed this call?" to "was that provider authorized to sign it?"

What a DNO+ record says

Per number, declared by the right-to-use holder, distributed on the existing DNO mechanism.

Never originate

- Classic DNO, unchanged
- The number does not place calls, from anyone

These providers may sign

- The SPCs of the originating providers the holder authorized
- What an A-level attestation should be measured against

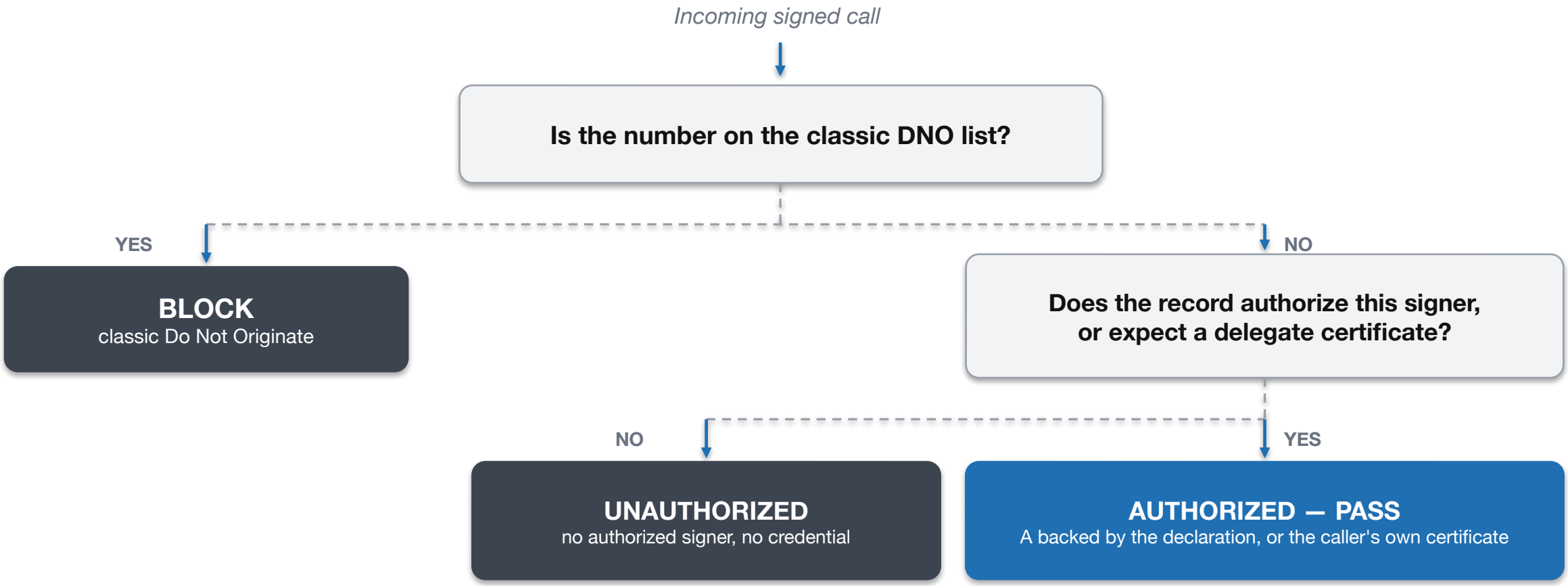
Expect a delegate certificate

- The enterprise signs for itself, or its credential travels with the call
- A call from this number arriving without one is suspect on its face

The third entry is an extension to the framework as written — the white paper names an enterprise credential as a permitted originating identity; stating that one is expected is the proposal.

The DNO+ origination check

Two questions, asked in order, on a call that is already signed.



What DNO+ does for Attestation A

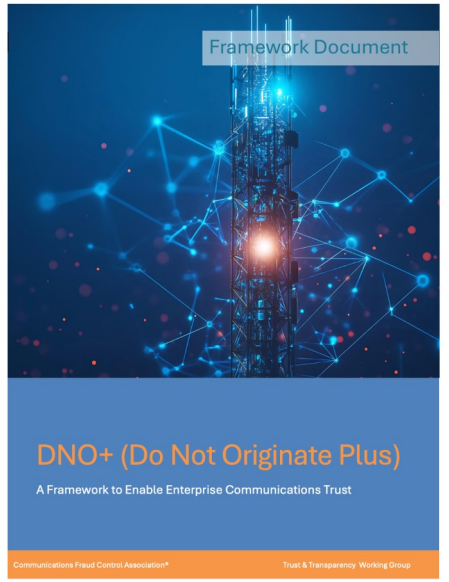
Attestation A asserts a direct customer relationship and that the customer is authorized to use the number. Today the second half is self-certified with no external validation.

Listed in the declaration

- The OSP has the number holder's own cryptographic authorization behind its A
- Its A is verifiably grounded rather than self-asserted
- A positive reason to participate, not a compliance cost

Not listed

- **Should not have originated** — an A or B without that relationship with the responsible party
- **Should be blocked, and it can be dropped** — whatever attestation level the call carries
- **Objective evidence of improper attestation** — inconsistent with what the provider must have known



CFCA Trust and Transparency Working Group

cfca.org · DNO+ framework document

DNO+ does not set attestation policy. It constrains on the number holder's authorization — a different party, deciding a different thing.

The whole picture

The record, the attestation, and the party who answers.

THE DNO+ RECORD SAYS	THE CALL CARRIES	WHO ANSWERS
The record lists this signer's SPC	→ A — grounded in the holder's authorization	→ the OSP: it vouched, and it answers
Expect a certificate — one arrived	→ B or C, plus the caller's certificate	→ the enterprise, and the TNSP that issued it
Expect a certificate — none arrived	→ suspect on its face	→ **no one for the caller; an A here is improper attestation**
No record for this number	→ the attestation stands on its own	→ unchanged from today

DNO+ is per number and opt-in. Where the holder has declared a record, the attestation becomes checkable against it; where there is none, nothing changes.

Artifact and declaration

Two mechanisms, two parties, two questions — and neither is the network answering for itself.

DNO+ — the declaration

- Who may originate from this number, declared by the entity that holds it
- Per number, on a distribution mechanism that already exists

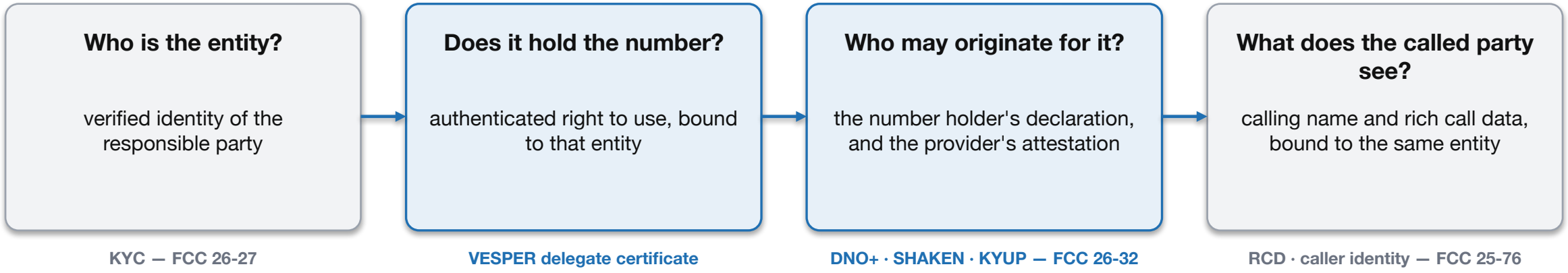
VESPER — the artifact

- Who holds this number, proved by the entity itself
- A certificate the caller presents when the provider cannot answer for it

Neither depends on a provider's internal judgment transferring to anyone else.

The visible end of a validated chain

The name on the handset is not a free-standing claim. It is the last link of something that starts at origination — when every link is verified.



- Each of these was its own proceeding. Each answered one link, and none of them closes the chain alone
- One verification at origination can support all of them, rather than being repeated for each

The more of these factors are independently verified and consistent with one another, the stronger the evidence behind the identity on the handset.

Where the work stands

Post-IETF 126, with the recharter through working-group consensus.

- **STIR recharter** — went to the IESG with WG consensus; review comments worked through, awaiting formal approval
- **vesper-10** — a profile framework composing existing STIR tools, with the normative mechanism work split out
- **tn-domain-binding-02** — separated from the core framework and from certificate transparency
- **certificate-transparency-04** — past the working group and with the AD
- **certificates-shortlived-06** — past IETF last call and balloted; DISCUSSes to clear
- **DNO+** — published as a CFCA Trust and Transparency Working Group white paper, 3 September 2026

Adoption calls for vesper and tn-domain-binding once the charter clears. The drafts are open, and the working group is the place to argue with them.

Takeaways

Three things get authenticated
the caller, the provider and the network — and SHAKEN is the middle one, not the first

The move is provider-level to TN-level
TNAuthList was specified to carry numbers as well as service provider codes; SHAKEN started at the carrier level by choice

The provider and network levels are converging
mutual TLS proves which provider on the connection; the attestation's distinct half narrows to the knowledge claim

An attestation is a commitment
A and B say the provider will answer for the caller; C honestly says it will not

DNO+ scopes origination, VESPER carries proof
one says who may originate, the other says who holds the number

Both have to arrive
the framework measures who may sign, never whether the signature survives the path

Let's build a definitive profile for TN-based certificate authentication using STIR tools.

References

Everything on these slides is public. Please cite the primary sources.

Standards work

- draft-wendt-stir-vesper-10
- draft-wendt-stir-tn-domain-binding-02
- draft-wendt-stir-vesper-use-cases-04
- draft-ietf-stir-certificate-transparency-04
- draft-ietf-stir-certificates-shortlived-06
- RFC 8224 · 8225 · 8226 · 8946 · 9060 · 9447 · 9448 · 9795 · 9970
- datatracker.ietf.org/wg/stir

Framework and record

- CFCA TTWG — DNO+ (Do Not Originate Plus): A Framework to Enable Enterprise Communications Trust, 3 September 2026 — cfca.org
- FCC 26-32 — Know Your Upstream Provider FNPRM, WC 17-97 / CG 17-59
- FCC 26-27 — Enhancing Know-Your-Customer Requirements, CG 17-59 / 02-278
- FCC 25-15 — Eighth Report and Order, CG 17-59
- 47 CFR § 64.1200(o) — Do Not Originate · § 64.6302(b) — unaltered caller ID
- ATIS-1000074 · 1000092 · 1000085