What Does Telco Need? Requirements for Organizational Identity Evidence

Daniel Hardman

2026-03-11

Abstract

Before engineers choose steel or concrete, they agree on what a bridge must carry. This paper applies the same discipline to organizational identity in telecommunications: instead of comparing candidate architectures, it sets out what the problem actually demands, so any proposal can be measured against a fair test. It argues for five essential properties — evidence over keys (portable, inspectable proof of relationships and authority, not just present-tense key validity); historical provability (answering 'what was valid then?', not only 'what is valid now?'); first-class support for complex, constrained, cooperative delegation; jurisdictional diversity, so verifiers can evaluate evidence without a single national root of trust; and cryptographic agility for key rotation, recovery, and post-quantum migration without a global flag day. An appendix expands these into detailed technical requirements, non-goals, and evaluation questions. The point is not to crown a winner, but to agree on the requirements first.

Before debating whether a bridge should be steel or concrete, engineers agree on what it must carry, how far it must span, and what earthquakes it must survive. Only then do materials matter.

The same principle applies to identity evidence in telecommunications. Before comparing candidate architectures, we need to agree on what the problem actually demands. This essay proposes requirements for an evidence layer that supports organizational identity, authority, and accountability in telco and adjacent real-time communications. The goal is not to pick winners, but to establish a fair test.

The Problem

Modern telco ecosystems need reliable accountability for communications that involve enterprises, service providers, call centers, bots, AI agents, and delegates acting across organizational and jurisdictional boundaries.

Verifiers — whether network operators, regulatory bodies, or end users — must be able to answer questions like these:

- Which legal or accountable party stands behind this communication?
- Does that party have the right to use this phone number or channel identifier?
- Does that party have the right to assert this brand or role?
- Is this call center or intermediary authorized to act on behalf of the principal?
- What evidence supported these conclusions at the time of the interaction?

These aren't hypothetical edge cases. They're core to preventing vishing, brand impersonation, unauthorized delegation, and a dozen other fraud patterns that cost billions annually and erode public trust in telecommunications.

The system must answer these questions in a way that remains meaningful under key rotation, cryptographic compromise, algorithm migration, partial connectivity, and long audit horizons. That's a tall order. But it's the actual requirement.

Five Essential Properties

Any architecture proposed for this space should be evaluated against these five properties.

1. Evidence Over Keys

A courthouse doesn't just check whether your ID is valid today. It maintains a record — affidavits, filings, receipts, transcripts — that can be reviewed later by appeals courts, journalists, or historians. The record isn't about present-tense access. It's about *accountability*.

Telco identity is the same. We don't just need to know that a cryptographic key validates right now. We need portable, inspectable evidence about relationships, authority, and rights.

Who attested to what? What was the scope of that attestation? What source of authority backed each claim — a legal registry, a numbering authority, a trademark office, a delegating principal? How do these pieces of evidence connect?

This evidence must be verifiable without depending on hidden institutional state, unverifiable assertions, or bilateral side agreements. If you can't see the reasoning, you can't trust it. And if the reasoning is scattered across opaque silos, you can't meaningfully audit it years later when a dispute arises.

Present-tense key validation is important. But it's not enough. Evidence comes first.

2. Historical Provability

Suppose your bank calls you about suspected fraud on your credit card. You authorize them to reverse three specific charges. Two years later, the bank produces a signed authorization from you, but you don't remember signing it, and the amount seems wrong.

Can you prove what you actually authorized *then*? Or can the bank only prove that your signature validates *now*?

This is the difference between historical provability and present-state validation. It matters in telco just as much as it matters in banking.

When a regulatory investigation asks "was this call center authorized on March 15, 2024?", the answer can't be "well, they're authorized today". When an enterprise rotates its cryptographic keys — maybe because of a compromise, maybe because of routine maintenance, maybe because of a post-quantum migration — the evidence about past communications must remain verifiable.

Keys rotate. Algorithms change. Delegates are added and removed. Organizational structures evolve. The identity of the organization must remain stable through all of this, and historical evidence must remain checkable. Routine cryptographic maintenance should not erase history.

A system optimized only for present-tense checks — "does this key validate?" — cannot answer historical questions without bolting on extensive side machinery. By then, you're not using the architecture's native features; you're compensating for its gaps.

3. Complex Delegation

A multinational enterprise doesn't make all its own phone calls. It authorizes call centers, marketing partners, customer support vendors, and regional offices to act on its behalf. These arrangements aren't simple parent-child relationships. They have constraints.

A call center might be authorized to originate calls using the enterprise's brand, but only for customer service, not sales. A marketing partner might be authorized during a specific campaign window, and only in certain regions. An emergency services provider might be authorized only when specific criteria are met. A business process outsourcer might require two-party approval for high-value actions.

This is not a hierarchy. It's a graph with weighted edges, conditional logic, time windows, geographic constraints, and spend limits. The authorization semantics are rich because real-world authority is rich.

Any evidence architecture that models delegation as simple parent-to-child chains will be stretched and stressed when faced with the actual requirements. Extensions, side registries, and bolt-on overlays will proliferate. These aren't signs of a flexible system. They're signs of structural mismatch.

Moreover, delegation introduces accountability risks. If a delegate can act unilaterally on the delegator's behalf, how does the delegator know when that authority is being exercised? How can abuse be detected and prevented? Cooperative delegation models — in which the delegate's actions require cryptographic cooperation from the delegator, or at least transparent reporting that the delegator can audit — provide stronger accountability than purely unilateral delegation. The delegate receives authority, but accepts an explicitly enforced duty to keep the delegator informed. Similarly, preventing unauthorized sub-delegation — where a delegate passes authority to yet another party — requires the system to track and enforce whether further delegation is permitted.

First-class support for complex delegation — including the ability to verify rich constraints, enforce cooperative models, prevent unauthorized sub-delegation, and trace authority back to appropriate roots — is a requirement, not a nice-to-have.

4. Jurisdictional Diversity

A certificate authority in one country may not be trusted in another. A governance regime mandated by US regulators is not accepted in Europe or Asia. A telco standard designed around a single national root of trust cannot scale globally without fragmenting into a patchwork of incompatible regional silos.

This is not a hypothetical problem. STIR/SHAKEN in North America uses a certificate-based model with US-specific governance. European and Asian operators have not adopted it, not because they don't care about call authentication, but because the trust model doesn't cross borders cleanly.

The requirement is this: verifiers in any jurisdiction must be able to evaluate evidence, even when the enterprise, the numbering authority, the communication provider, and the verifier all operate under different governance frameworks. Evidence must be portable.

This doesn't mean eliminating governance. Governance is necessary. But it does mean that governance outcomes — who attested to what, and why it should be trusted — must be inspectable and verifiable without requiring all parties to recognize the same nationally bounded root authority.

Incremental deployment matters, too. It must be possible for one enterprise or one verifier to adopt the system and gain value, without waiting for a global flag-day migration or a regulatory mandate. Systems that require universal prior agreement never deploy.

5. Cryptographic Agility

Cryptographic algorithms have lifespans. MD5 was once standard, then broken. SHA-1 followed the same path. RSA is robust today, but vulnerable to quantum computers tomorrow. Every major organization should be planning post-quantum migrations now, even though commercial quantum computers don't yet exist.

The threat isn't distant. Attackers are already harvesting encrypted sessions, knowing that future quantum computers will let them decrypt the contents and access secrets, IP, M&A plans, and sensitive communications that seemed safe when encrypted. This is called "harvest now, decrypt later", and it's happening today.

Migration to post-quantum algorithms is not optional. But it also cannot happen as a synchronized global flag day. Organizations will migrate at different speeds. Verifiers will support new algorithms on different schedules. Some legacy systems will lag by years.

An evidence architecture must support cryptographic agility — the ability to rotate keys, migrate to new algorithms, and recover from compromise — without requiring simultaneous upgrades across the entire ecosystem. Identifiers and evidence artifacts should survive these transitions.

Equally important: compromise of a key should not mean permanent loss of control. Recovery mechanisms must exist. Transparency about key state changes — rotations, compromises, recoveries — must be verifiable, not just asserted.

If an architecture cannot handle cryptographic change gracefully, it will age poorly, and the cost of maintaining it will compound.

What This Means

These five properties — evidence over keys, historical provability, complex delegation, jurisdictional diversity, and cryptographic agility — are not wishlist items. They are what organizational identity in telco actually requires.

Proposed architectures should be evaluated by asking: How does this system address each property? Which capabilities are native, and which require extensive retrofitting?

Some architectures will fit these requirements naturally. Others will need bolt-on registries, side protocols, and governance workarounds to approximate the same outcomes. That difference matters. It determines cost, complexity, interoperability, and long-term viability.

The point is not to declare a winner in advance. The point is to agree on a fair test. These are the requirements. Let's see what fits.

Appendix: Detailed Requirements

The five essential properties above map to the following detailed technical requirements, organized by theme.

Evidence Over Keys

1. Accountable-Party Binding The system must support cryptographically verifiable binding between a communication and an accountable party whose legal or formally recognized identity can be established.

2. Channel-Right Binding The system must support proof that the accountable party, or a valid delegate, has the right to use the asserted communication channel or endpoint identifier (phone numbers, messaging handles, etc.).

3. Attribute-Right Binding The system must support proof that asserted attributes (brand, logo, trade name, role, settlement, human-vs-AI) are authorized for use by the accountable party.

4. Portable Verification The system must allow verification decisions to be based primarily on portable, inspectable evidence rather than hidden institutional state, unverifiable assertions, or bilateral side agreements.

5. Source Authority Traceability The system must support tracing each material assertion back to an appropriate source of authority (legal registries for identity, numbering authorities for channels, trademark offices for brands, delegating principals for delegation).

6. Evidence Composability The system must support composition of multiple evidence artifacts into a verifier-meaningful whole without losing provenance, integrity, or relationship semantics.

Historical Provability

7. Historical Provability The system must support verifiable reconstruction of evidence and authority relationships that were valid at an arbitrary point in the past. It must be possible to distinguish what was valid then from what is valid now.

8. Stable Identity Across Key Change The system must preserve continuity of accountable identity across key rotation, algorithm migration, and routine cryptographic maintenance. Routine maintenance must not require a change in the underlying identity.

9. Verifiable Event Ordering The system must support cryptographically meaningful reasoning about how signing, issuance, revocation, and key-state changes relate in time. The system must not depend solely on present-tense status checks when historical validity questions are in scope.

10. Revocation with Defined Freshness The system must support revocation or invalidation of evidence and authority relationships with freshness properties appropriate to real-time communications. Freshness assumptions must be explicit so verifiers can determine whether the system meets their operational risk thresholds.

Complex Delegation

11. Delegation Semantics The system must support delegation of authority across organizational boundaries. The delegation model must support identification of delegator and delegate, scope of delegated authority, multiple constraint types on delegated authority including purpose, geography, jurisdiction, time, protocol/role, and proof requirements, composition semantics for multiple constraints, revocation or expiration of delegated authority, and verifier inspection of the delegation chain or graph.

12. Cooperative Delegation The system should support cooperative delegation models in which the delegate's exercise of authority can be cryptographically bound to the delegator's awareness or endorsement. Such models minimize the risk of undetected misuse of delegated authority and provide stronger accountability than purely unilateral delegation.

13. Sub-Delegation Control The system should support explicit control over whether a delegate can further delegate (attenuate) the authority they have received. When sub-delegation is prohibited, the system must prevent delegates from granting portions of their delegated authority to additional parties.

14. Multi-Party Control The system should support control models stronger than single-key ownership, including threshold control, weighted approval, separation of duties, and other multi-party authorization schemes appropriate for high-value organizational identities.

Jurisdictional Diversity

15. Cross-Jurisdiction Operability The system must function across jurisdictional boundaries and trust domains without requiring all participants to share a single nationally bounded root-of-trust regime. Verifiers must be able to evaluate evidence even when the issuer, subject, verifier, and communication providers operate under different governance frameworks.

16. Incremental Deployability The system must be deployable incrementally. Adoption by one enterprise or one verifier must create value without requiring prior universal rollout, national mandates, or global flag-day migrations.

17. Compatibility with Existing Transports The system must be usable over existing communication channels and protocols with reasonable transport overhead. Where compact real-time messages are needed, the system may separate lightweight in-band evidence references from richer out-of-band evidence retrieval, provided integrity and binding remain verifiable.

18. Performance and Scalability The system must scale to large numbers of organizations, delegates, and verifiers without requiring constant high-cost reissuance, excessive online lookups, or brittle centralized bottlenecks.

19. Privacy and Selective Disclosure The system should support variable evidence disclosure so that verifiers can receive the minimum information necessary for their role, jurisdiction, and purpose. The architecture should permit distinct verifier views when required by privacy or regulatory constraints.

20. Data Locality and Regulatory Adaptability The system must be capable of deployment in ways compatible with locality, retention, erasure, and sector-specific regulatory requirements. Where requirements conflict, the architecture should make these tensions explicit and manageable.

Cryptographic Agility

21. Compromise Detection and Recovery The system must support transparent detection of key compromise or control anomalies and must support recovery procedures that preserve or re-establish legitimate control. Recovery mechanisms must minimize the risk that an attacker can obtain permanent control simply by compromising a currently active key.

22. Cryptographic Agility The system must support migration to new cryptographic algorithms, including post-quantum algorithms, without requiring synchronized global upgrades by all ecosystem participants. The system should allow long-lived identifiers and evidence artifacts to survive such transitions.

Cross-Cutting Concerns

These are operational goals, not architectural requirements. However, they color or constrain many of the requirements listed above.

Compact Real-Time Signaling Real-time communications should carry only compact evidence or evidence references in-band.

Low-Latency Verification Verification workflows should support latency (including revocation latency) appropriate to real-time call or message handling.

Manageable Cost Issuance, maintenance, rotation, recovery, and verification costs should be low enough for broad adoption by enterprises, service providers, and downstream verifiers.

Non-Goals

The following are explicitly not universal design assumptions:

- A single global root authority
- A single governance body for all jurisdictions
- Online contact with a central service for every verification decision
- A requirement that every verifier process all evidence at maximal depth
- Elimination of governance (the goal is to make governance outcomes inspectable and portable, not to eliminate governance)

Evaluation Questions

When evaluating candidate architectures, ask:

1. What evidence does this architecture preserve natively?
2. What crucial properties must be reconstructed by side systems?
3. What happens when keys rotate, are compromised, or must migrate to new algorithms?
4. Can it answer "what was valid then?" as well as "what is valid now?"
5. Does it model delegation and rights as first-class semantics, or only as bolted-on conventions?
6. Can verifiers in different jurisdictions evaluate the same evidence, or is trust fragmented by national boundaries?