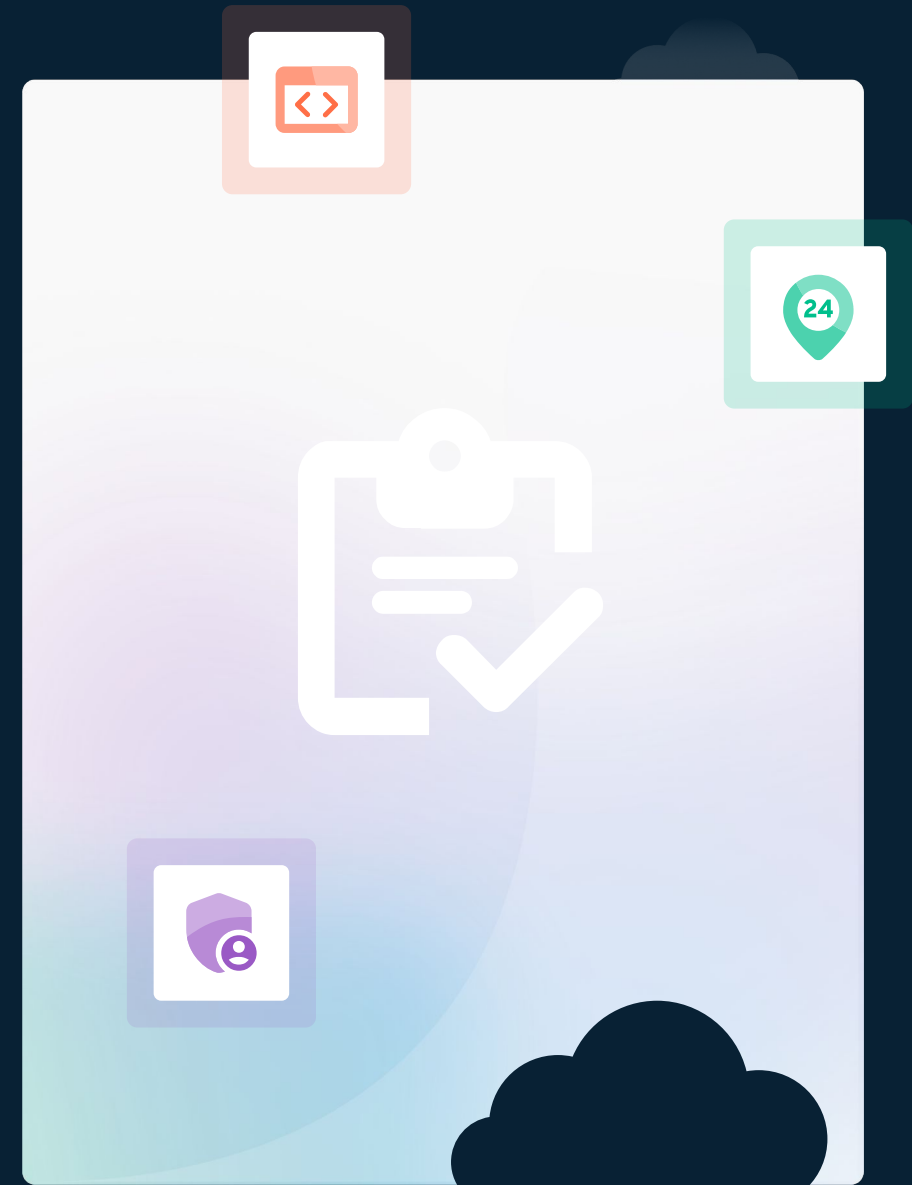


The FCC is writing your vendor's product roadmap

Product strategy for the all-IP transition

Mark R. Lindsey | SIPNOC 2026



Three product questions will have hard deadlines

01

Which technologies could have a proposed federal sunset, and what should we do whether or not it holds?

02

What replaces the bilateral agreement, and who sells it?

03

What should we build before the institutions exist?

Your TDM product line has a proposed federal sunset date

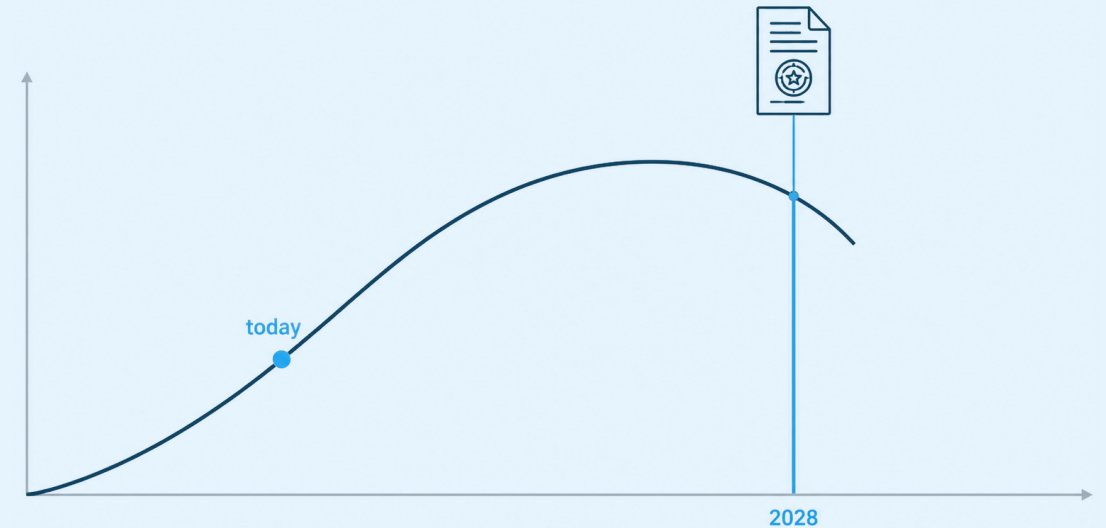
End-of-life notice: TDM interconnect, its billing machinery, and PRI gateways now have a planning date.

Expect slippage: The date may move. Plan against it anyway.

The exit has value: Customers trapped in TDM already pay for a way out.

It could be as early as December 31, 2028

Source: FCC, comment sought on transitioning voice services to all-IP



Voice Quality across the Internet is solvable, but...

One Study Measured Voice over Internet:

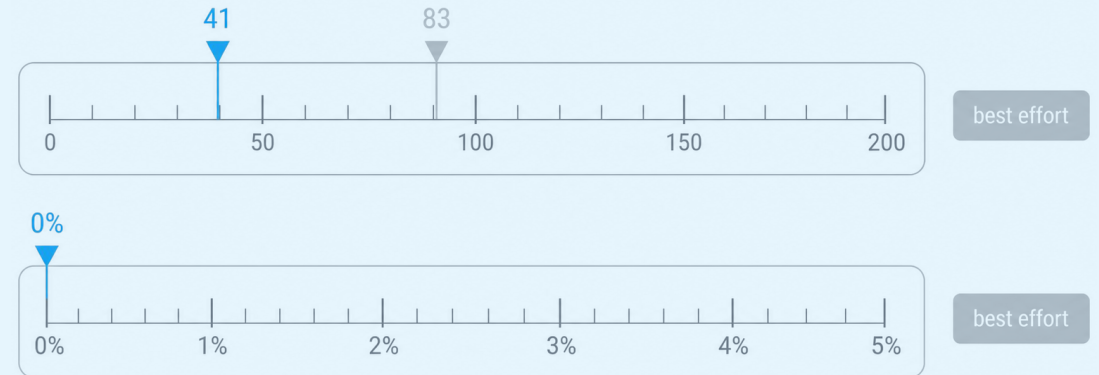
41 ms median latency, 83 ms at the 90th percentile, & averaging 0.008% packet loss.

Best effort: Unprioritized QCI-8 on AT&T LTE, with no prioritization once traffic reaches the internet.

What the study means is debated, but it's not an outlier: About half of Bandwidth's traffic already crosses the public internet.

Well-engineered public paths carry production voice.

Source: AT&T letters, May 21 and July 14, 2026 · WC Dkt. 25-304



ALIII and IcP, defined

ALIII

Agreement-less IP Interconnection over the Internet

- Carriers send interconnection traffic across the public internet.
- Carriers agree to one shared set of rules.
- No bilateral contract sits behind the connection.
- The rulebook does the work the agreement used to do.

IcP

Interconnection provider

- One provider connects to carriers across the country.
- An IcP can connect any carrier to any other carrier.
- Private, engineered bandwidth is available.
- The IcP sets the rules and answers for performance.
- Close to the NTP idea

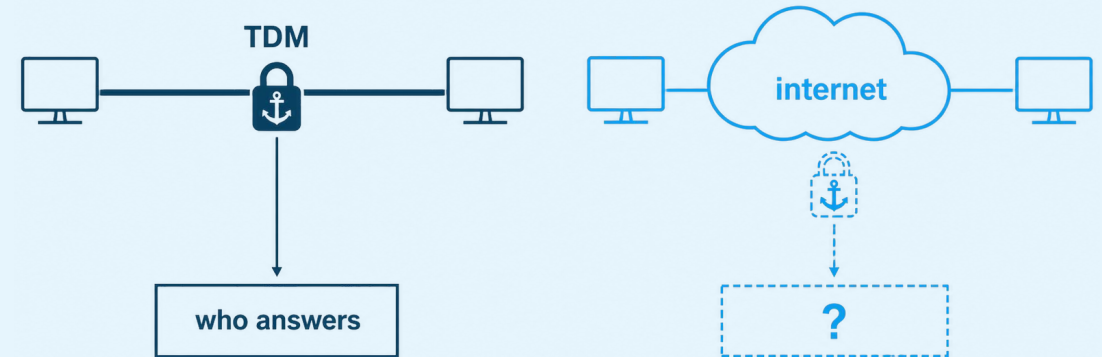
The gap is accountability, not quality

Quality: An engineering problem with mature tools and measurable performance.

Accountability: An unclaimed product surface, and the objection you actually hear.

The opening: SBC vendors, carriers, and local exchange carriers all feel the same unmet need.

When it breaks, who answers for it?



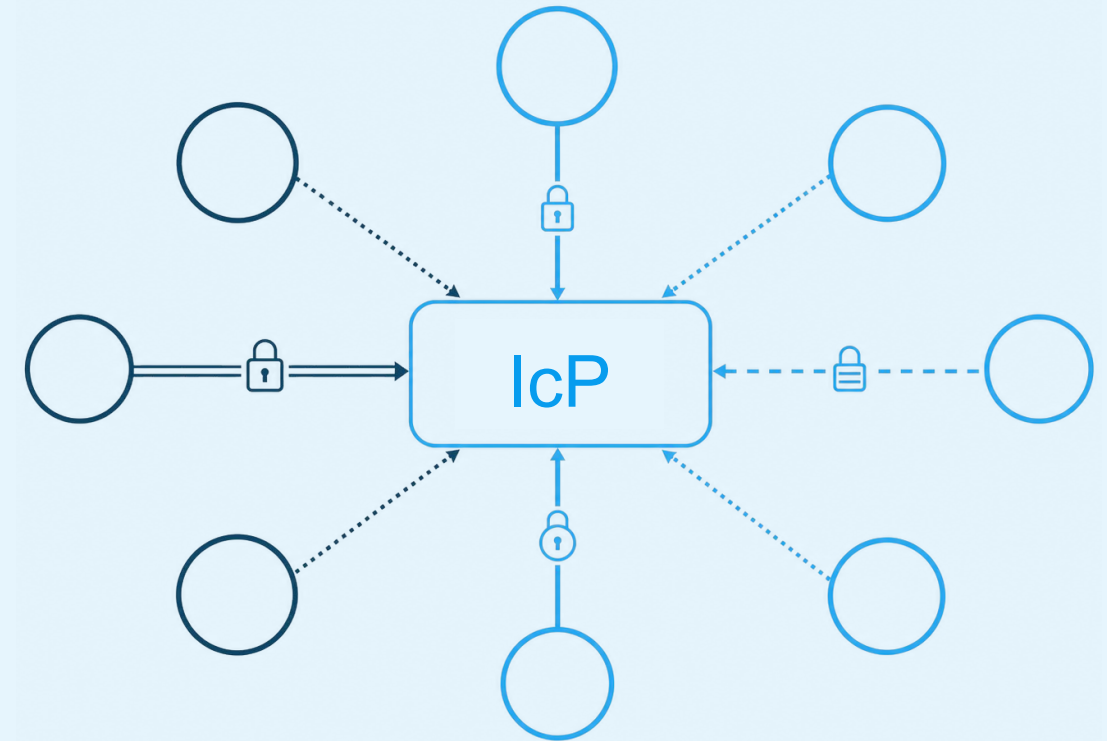
IcP is the default backstop

Reach: Connectivity in all the places needed to reach everyone.

Transport: TDM, TLS, IPsec, private Ethernet, whatever works.

Security: The provider negotiates and operates the protections.

Commercial model: Under an IcP proposal (like NTP), transit could be offered on common-carrier terms.



ALII makes the rulebook the contract

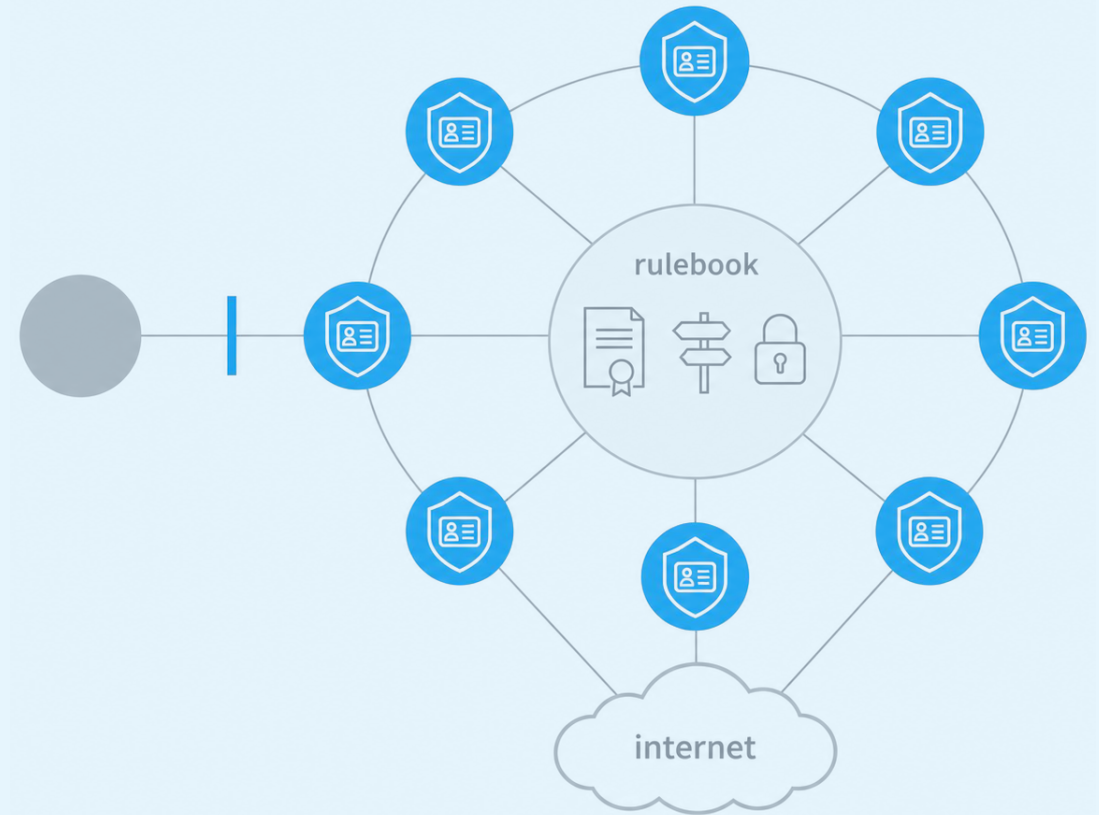
Covenant: One security standard, one discovery method, one routing rule set (still under discussion).

Discovery: Number to authoritative provider, FQDN to DNS, then the public internet.

Admission: An Authorized Voice Service Provider (AVSP) certificate is checked at TLS setup.

Exposure: The value and the risk share one source. It crosses the public internet.

Your public internet is not my public internet.

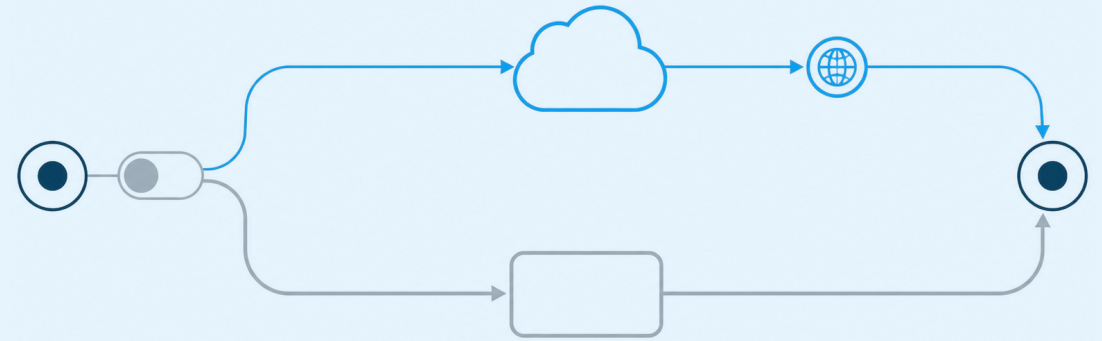


IcP and ALII compose; they do not compete

Direct Path: ALII carries rulebook-as-contract across the public internet.

Accountable Path: IcP supplies the alternate path when the direct route is unusable.

Combined value: Together they close governance and reliability gaps neither closes alone.



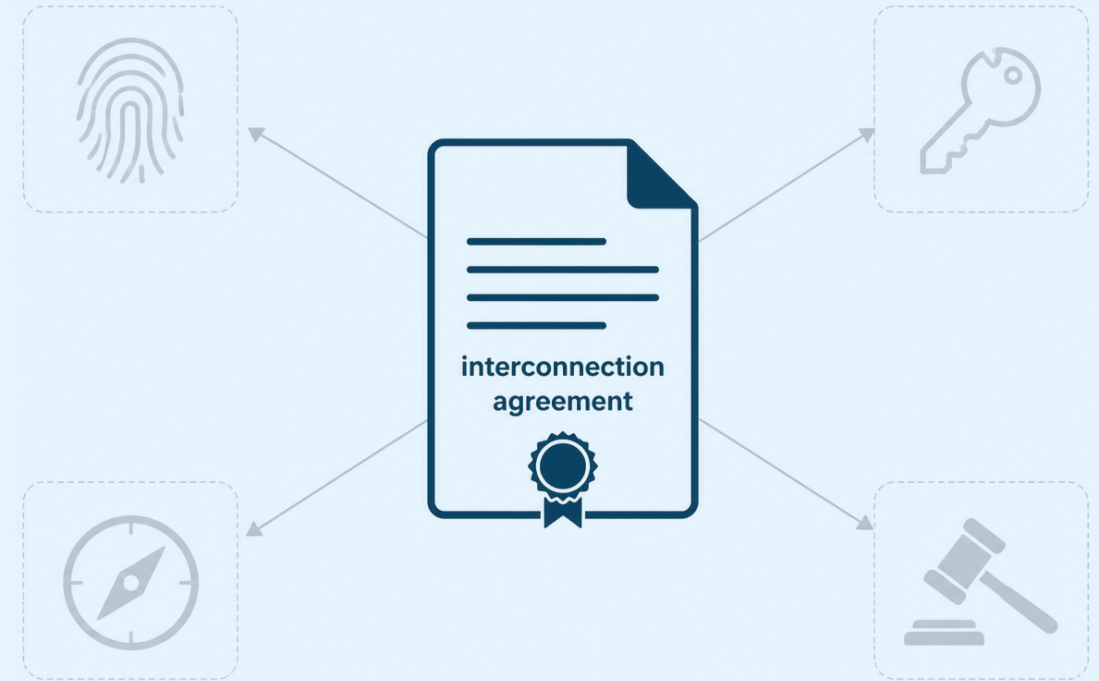
A bilateral agreement quietly bundles four products

Identity: I know who you are.

Permission: You may send me this call.

Reachability: I know where to send traffic.

Remedy: Misbehavior has consequences.



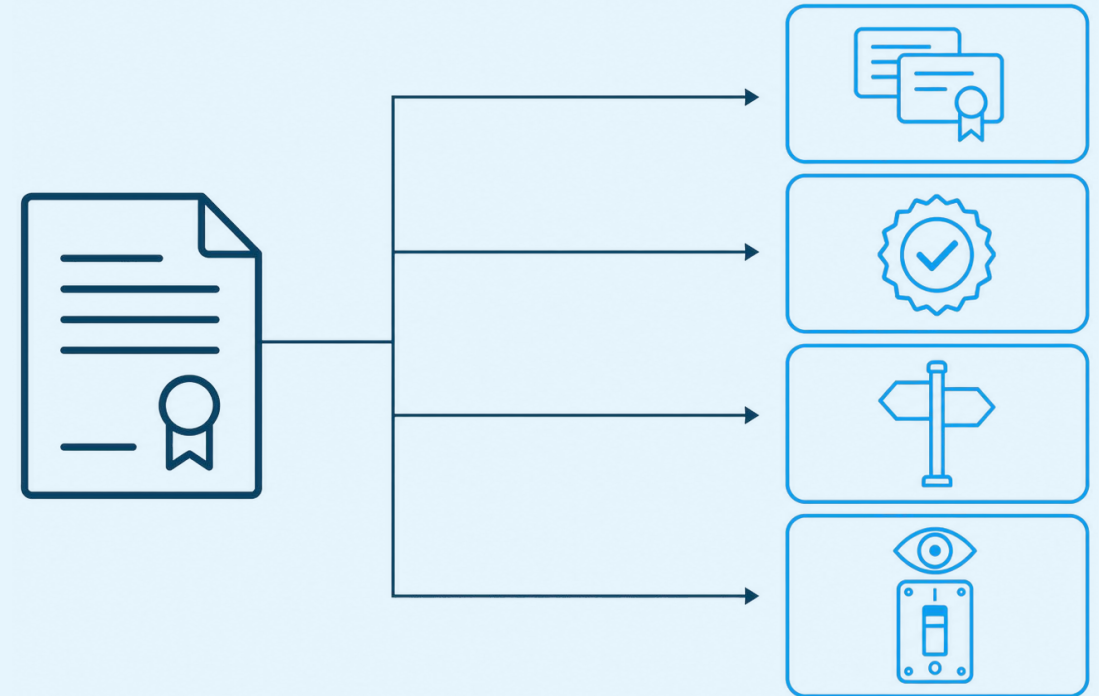
ALIII turns those functions into buyable products built from proven components

Identity: Mutual TLS on public-key infrastructure.

Permission: AVSP certification, IP subnets

Reachability: Discovery & Routing (Mapping TN to FQDN, FQDN to IP Addresses)

Remedy: Monitoring and revocation (Automated removal of an AVSP)



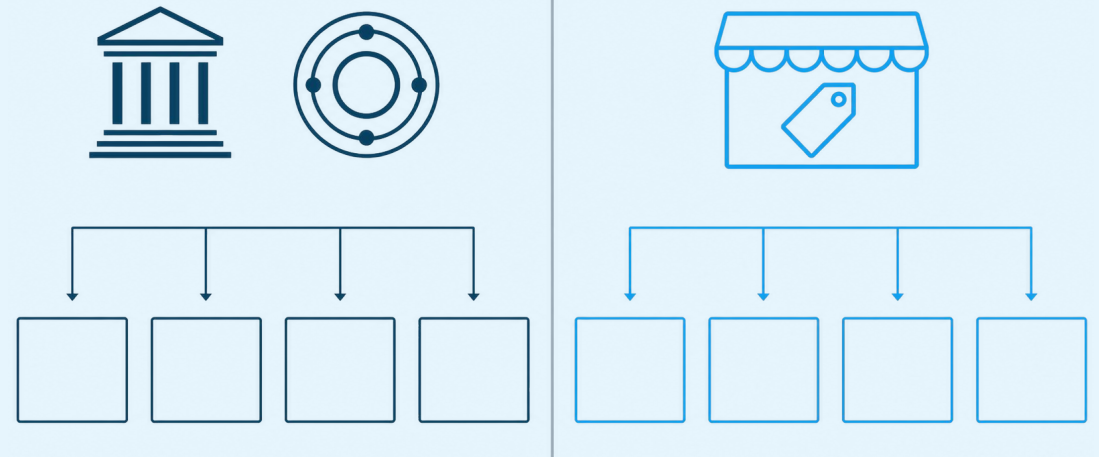
The buyer changes; the function does not

Before: A lawyer and a regulator supplied identity, permission, reachability, and remedy.

Next: A vendor supplies them, or you sell all four as one managed product.

Winning bundle: Four essential functions that belong together.

Same functions. New Supplier.

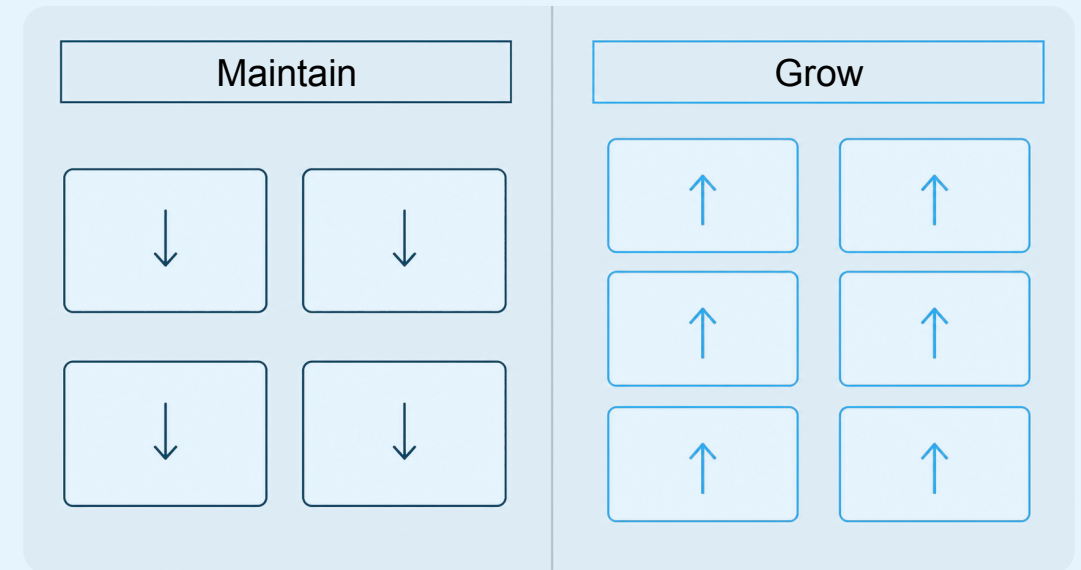


The product board is simple: Maintain or Grow

Maintain: TDM tandems, 911 Gateways for the 70% on TDM, PRI gateways, CNAM as source of truth, access-charge rating.

Grow: Trusted trunks, branded and RCD display, voice PKI, FQDN handling, quality monitoring, NG911 IP.

Should any of us be investing in the
“Maintain” category?

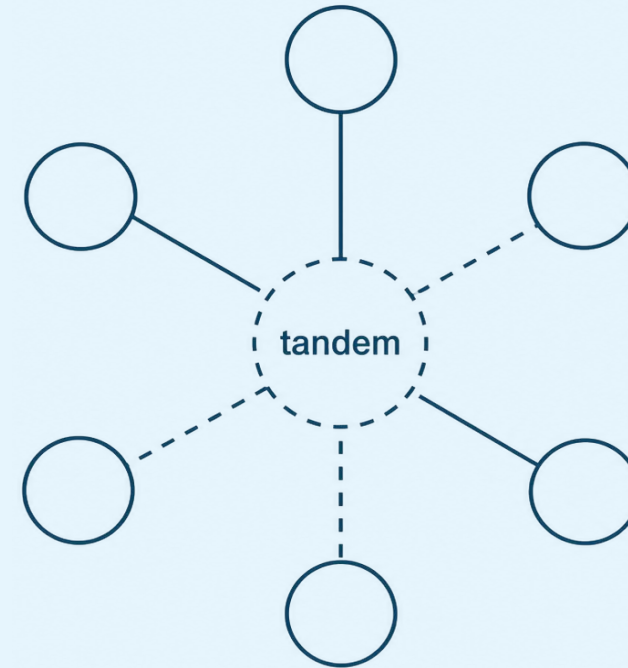


TDM tandems and access-charge rating die by rule

TDM tandems: When TDM interconnection is retired obligations sunset, their reason to exist disappears.

Rating engines: Bill-and-keep would remove the per-minute transactions they rate, bill, and dispute.

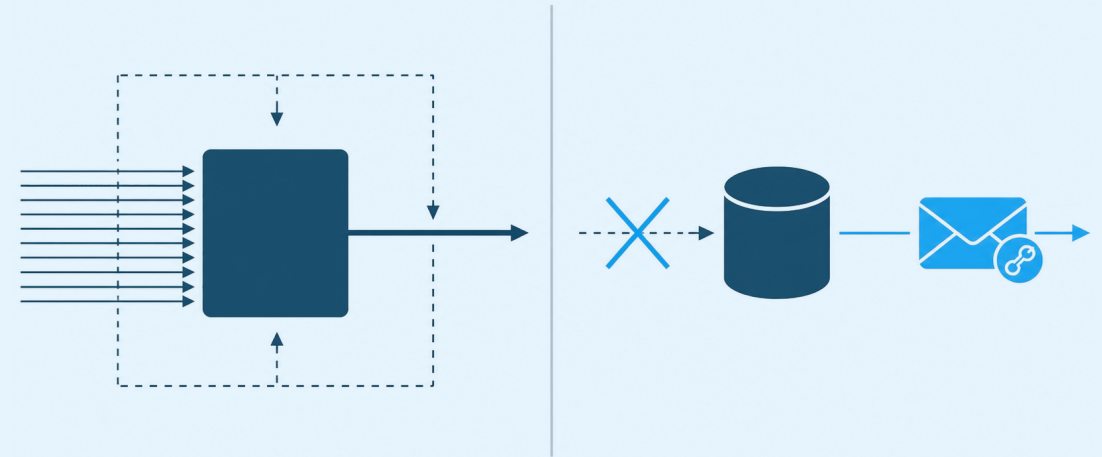
These products do not lose to a competitor, if the rule that created them is withdrawn.



PRI gateways and CNAM die by substitution

PRI gateways: Keep selling and supporting them. Stop adding features to a shrinking population.

CNAM: Signed identity and Rich Call Data (RCD) are moving caller information from a queried database to a credential carried with the call.

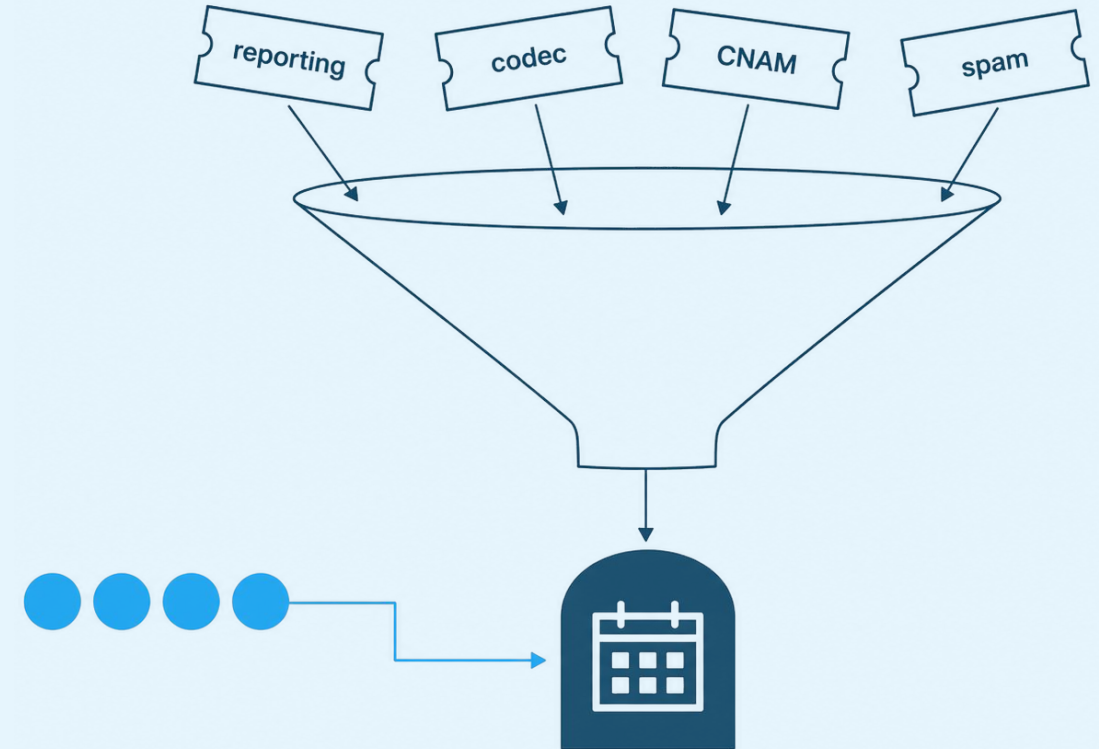


The backlog can trap scarce legacy expertise

Loud requests: Tandem reporting, PRI codec support, CNAM enhancements, legacy spam flags.

The test: Am I adding features to something with a drop-dead date?

The cost: Even a signed purchase order can consume the few engineers who understand the legacy stack.



Six categories of technology products exist in the future

Trusted trunks

Wholesale trunks with STIR/SHAKEN attestation.

Branded calling

Branded calling and Rich Call Data display.

Voice PKI

PKI operations sold as a voice product. A new category.

Discovery

FQDN handling and number discovery.

Accountability

Traffic monitoring and quality accountability.

NG911

Next-generation 911 IP delivery.

If trust becomes baseline, the premium compresses

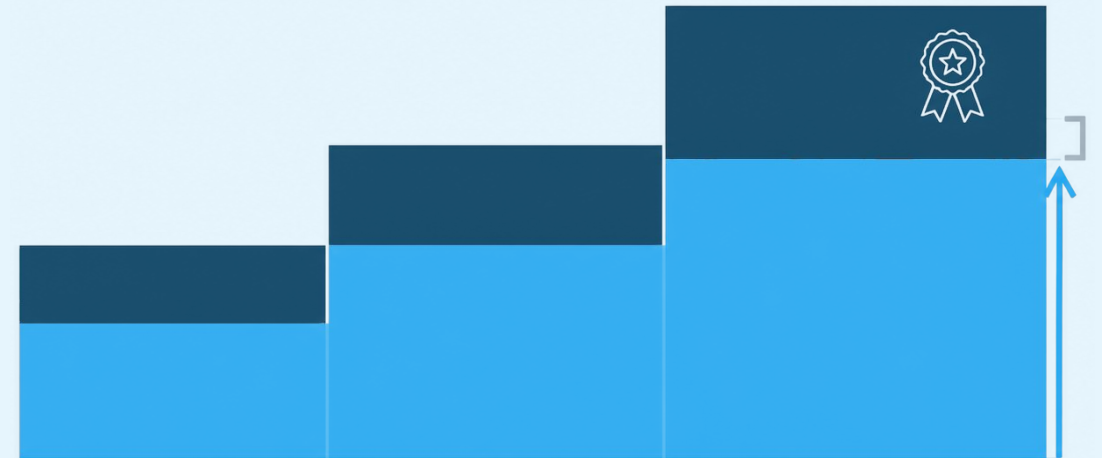
Market shift: RCD plus serious know-your-customer checks could make trusted caller identity the expected baseline.

Commercial effect: The fee for merely looking legitimate shrinks.

Durable value: Sell analytics and know-your-customer operations, not trust itself.

Is verified identity a premium feature – or basic infrastructure?

Source: FCC-25-76, Improving Verification and Presentation of Caller ID, Oct. 29, 2025



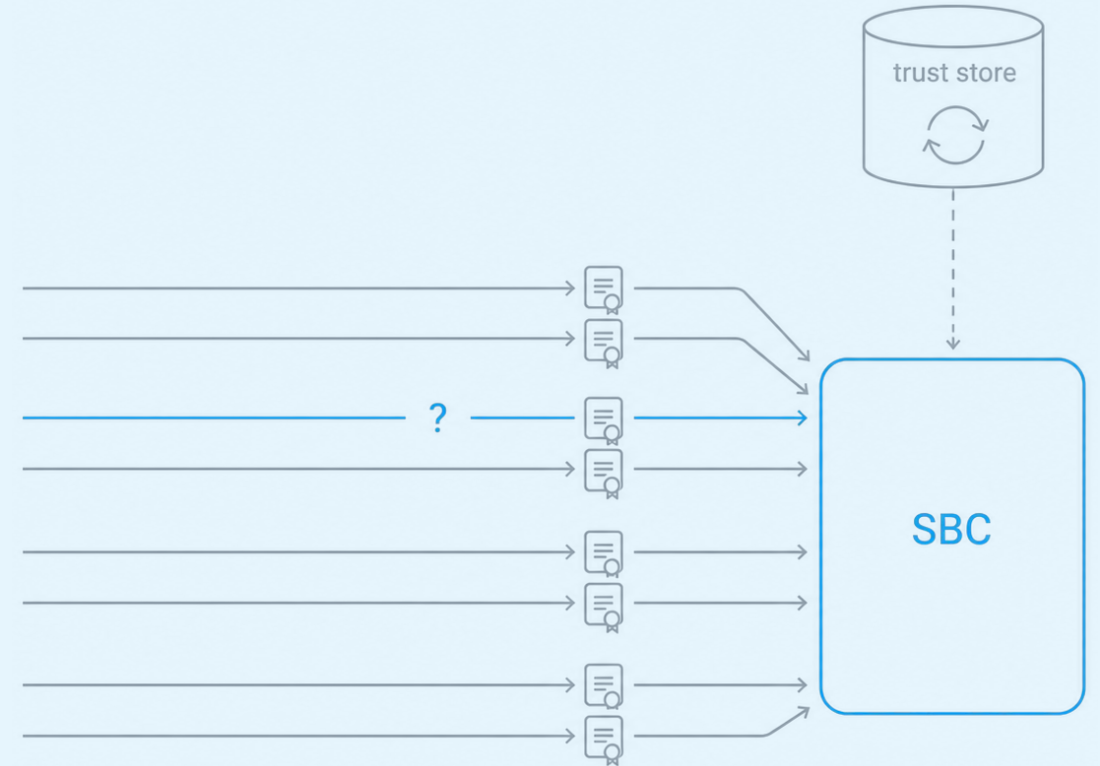
SBCs must operationalize mutual TLS at scale

Every connection: Client certificates become routine, not exceptional.

Dynamic trust: Certificate authority list changes must propagate safely into the trust store.

Open problem: What tears down a live session after revocation, and how fast?

This is being specified now. A demo is a product opening.

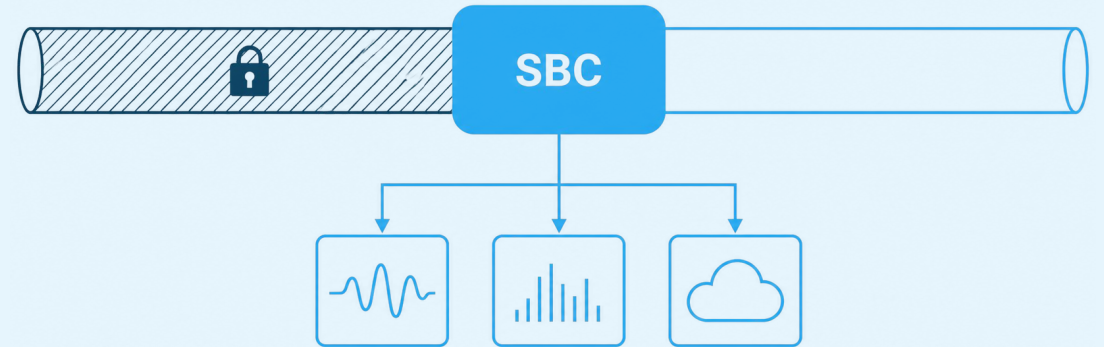


The SBC is where media becomes usable

Boundary: Encrypted traffic arrives and the SBC decrypts it.

Attach point: Recording, biometrics, analytics, transcription, and cloud cross-connect all branch here.

Packaging: Expect SRTP handling to become a licensing dimension.



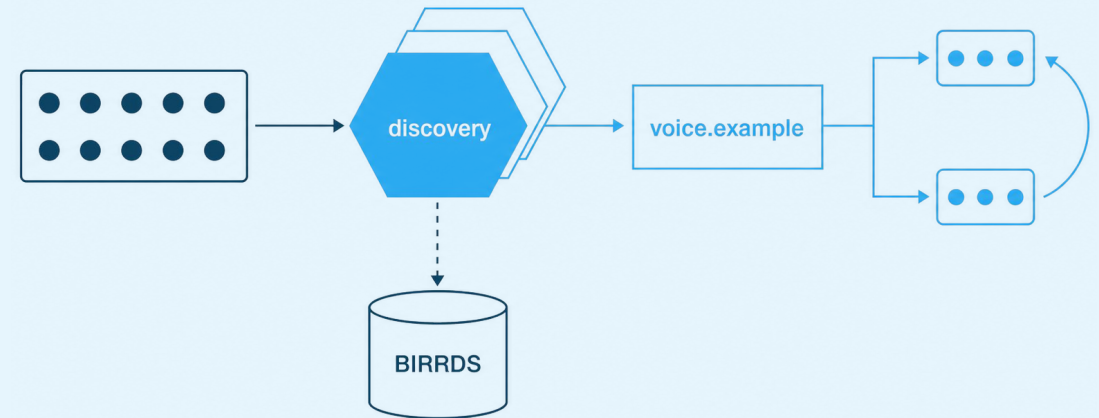
Reachability becomes a registry contest

The query: Given a phone number, return an authoritative provider, FQDN, SRV records, and failover.

Existing data: BIRRDS already carries the relevant fields.

The contest: Who exposes them as a queryable, IP-facing discovery service?

Every least-cost routing engine will ask: is this ALIII-eligible traffic?



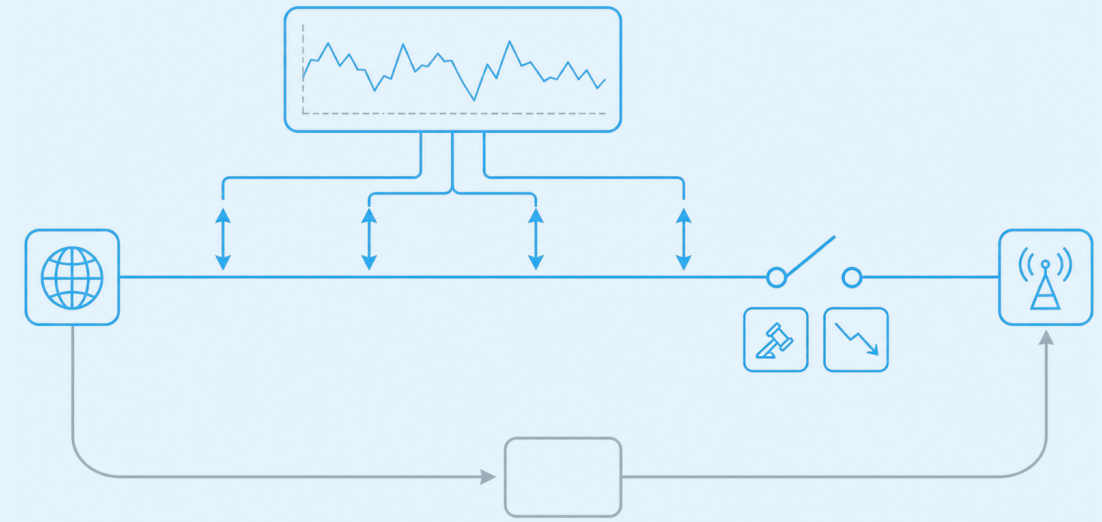
Monitoring turns remedy into routing

Telemetry: sRTCP and sRTP session data expose quality in both directions.

Regulatory cutoff: A provider is barred for carrying scam traffic. ALIII allows service providers and certificates to be revoked by authorities automatically.

Commercial cutoff: A poor ALIII path is bypassed through an IcP-style provider.

Quality decides whether a link stays usable at all.



Do buyers want one subscription?

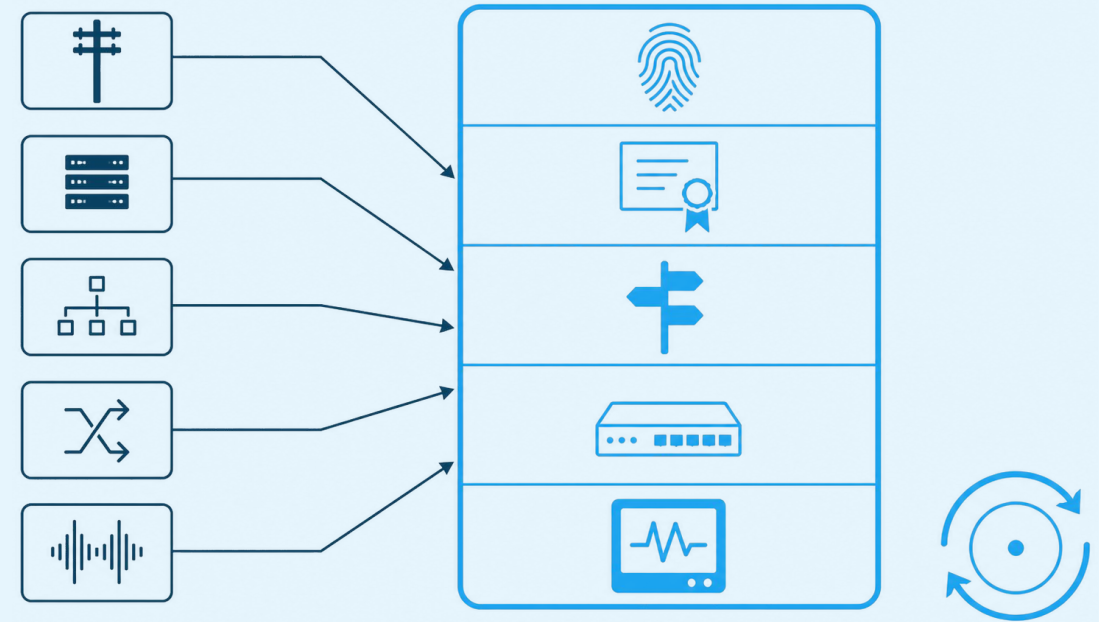
Identity: Attest who is connecting.

Authorization: Operate certificates and admission.

Reachability: Manage FQDNs and discovery.

Remedy: Monitor, route around, and revoke.

Carriers will need one accountable operating model, even if several vendors supply it.



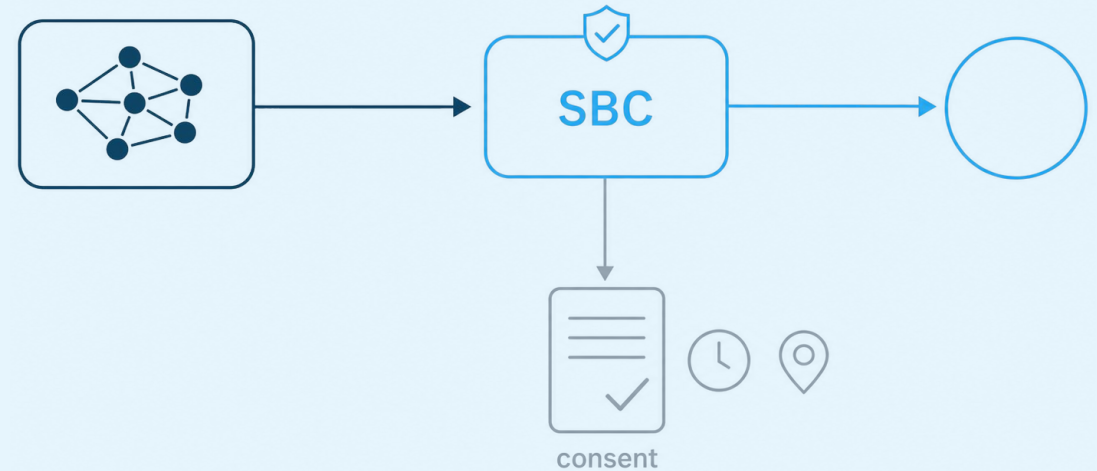
Voice agents ride on attested paths

Distribution moat: Trusted origination matters more than the model alone.

Attach point: The SBC exposes clear media to the agent workflow.

Consent: Pair every voice-agent SKU with a ledger of when and where consent was obtained.

vCon can make consent portable and auditable.



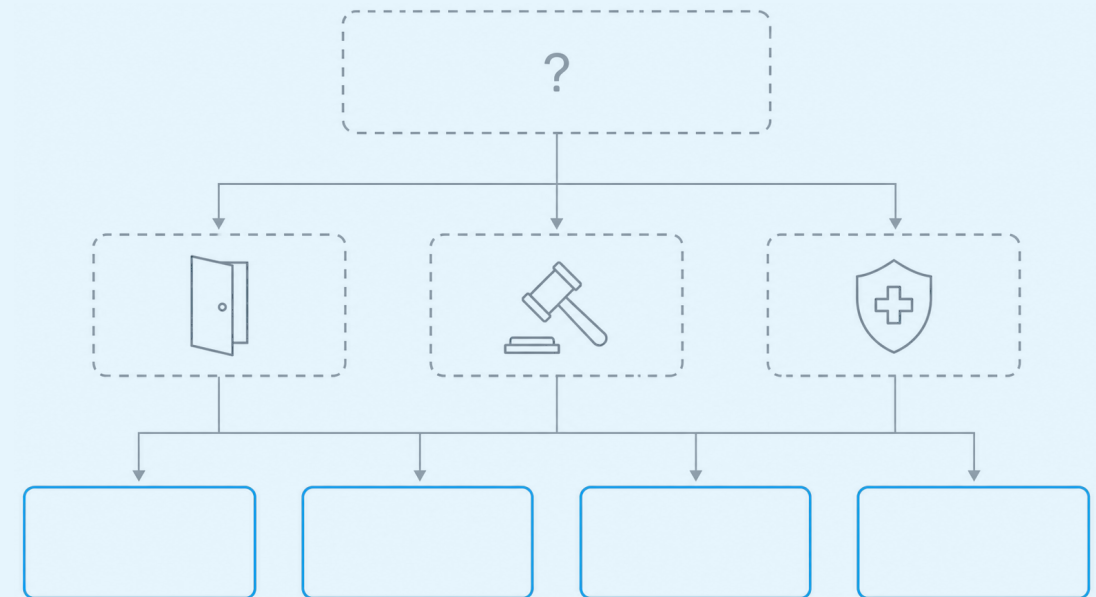
The institutions do not exist yet

Authority: Who governs ALIII, or each IcP?

Admission: Who gets to participate, and on what terms?

Due process: What precedes revocation?

911: Who answers when TDM delivery becomes prohibitively expensive?



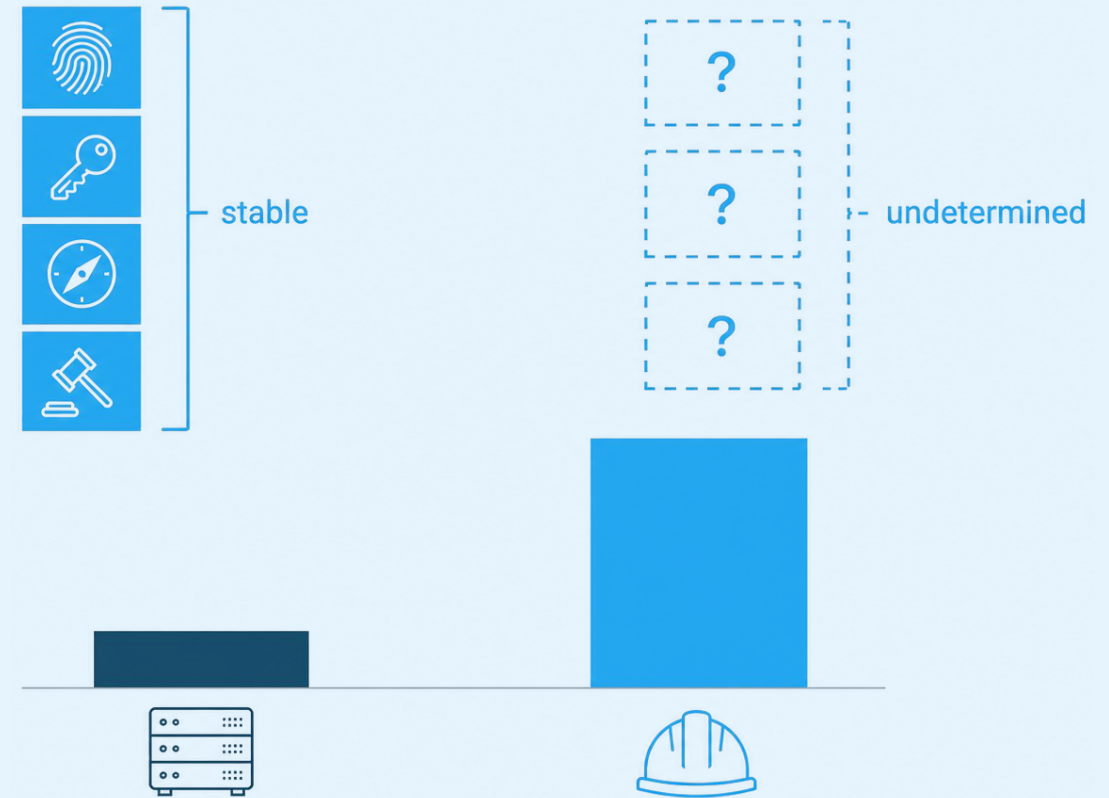
Build for functions; bet on institutions later

Stable: Identity, permission, reachability, and remedy survive every scenario.

Flexible: The institutions delivering them are still undetermined.

Falsifiable claim: The rural bottleneck for IP transition is staffing fluent with both SS7 & SIP/TLS. Prove me wrong with the data.

Decision cost: Indecision is invoiced monthly at TDM rates.



What to demand from any provider

If a provider or an architecture cannot answer these questions, or demonstrate the answers, do not buy. That includes us.



Identity

How do we know who is calling? Is the trust problem fully solved?



Permission

Who decides whether this call is allowed?
Is there an appeal process?



Reachability

Which routing database is authoritative?
Does it work with other ICPs and ALII?



Remedy

What happens on failure? Who responds
when something goes wrong?

Finishing the transition is an act of stewardship

A network that makes deception cheap and honesty expensive is a moral failure as much as an engineering one.

