EXECUTIVE PRIMER

PKI Is Breaking in Slow Motion — and DNS Is Next

What CISOs and CTOs need to understand about the accelerating collision between certificate lifecycles, machine identity growth, and domain infrastructure

This primer distills the findings and discussion from a 2026 industry webinar on global PKI research — a conversation between an industry analyst and a certificate authority executive covering survey data from more than 420 senior IT and security decision-makers, plus a real-world modernization case study. It is written for a US CISO/CTO audience and does not endorse or recommend any specific vendor, product, or solution.

Bottom Line Up Front

Public Key Infrastructure has quietly stopped being background plumbing. Shrinking certificate lifespans, an explosion of machine and AI-agent identities, and a post-quantum migration timeline that keeps getting pulled forward are converging on the same operational reality: the manual, semi-automated, and loosely-owned PKI practices that worked for the last two decades no longer keep up. And because certificate issuance now depends on frequent, automated domain validation, **DNS infrastructure is being pulled into this pressure along with it** — a dependency most organizations still treat as a solved, static utility.

- **Visibility is the root problem.** Most organizations cannot fully account for their own certificate inventory, and the certificates nobody is tracking are consistently the ones that cause outages.
- **The pace is compressing, not stabilizing.** Certificate lifespans, domain validation cadence, and post-quantum timelines are all moving in the same direction — faster.
- **Ownership is diffuse by default.** PKI is used by nearly every team and owned, in practice, by none of them — which is precisely where risk accumulates.

Six Forces Reshaping PKI Right Now

The webinar's underlying research (a survey of more than 420 senior IT and security decision-makers, weighted toward North America) organizes the shift around six themes. None of them are new in isolation — what's new is that they are all under pressure simultaneously.

Force	What the Data Shows	Why It Matters to Leadership
Visibility	Most organizations report only a partial certificate inventory; a complete, real-time picture is the exception.	You cannot secure, automate, or rotate what you don't know exists — and untracked certificates are the ones that cause outages.

Force	What the Data Shows	Why It Matters to Leadership
Complexity	Segmentation, tool sprawl, and inconsistent tracking (spreadsheets, informal knowledge, multiple platforms) coexist inside the same organization.	Complexity — not the underlying cryptography — is now the primary obstacle to modernizing PKI.
Identity Explosion	Machine identities are growing fastest; human, code-signing, IoT, and now agentic-AI identities are all expanding at once.	Every new identity class is a new class of certificate to issue, track, and rotate — faster than manual processes can absorb.
Ownership	PKI touches nearly every team, but responsibility is diffuse; CISOs are the most common final decision-maker, rarely the only stakeholder.	Without clear, cross-functional ownership, certificates fall into the gaps between teams — and outages start in those gaps.
Readiness	Understanding of what needs to happen is well ahead of the ability to actually do it.	Awareness alone doesn't reduce risk. The gap between intent and execution is itself an exposure.
Timeline Pressure	Certificate lifespans are compressing, domain validation is recurring more often, and post-quantum migration dates are being pulled forward.	The operational cadence PKI now demands is faster than the processes most organizations still run it on.

You Can't Manage What You Can't See

The most consistent finding, echoed by both the survey data and the modernization case study discussed, is that organizations chronically underestimate their own certificate footprint. In the case study cited, a certificate authority undertaking its own internal modernization initially estimated somewhere between 3,000 and 7,000 certificates in its environment. The real number, once discovered, was over 18,000 — more than double the high end of the estimate.

- Network segmentation — especially micro-segmentation — makes discovery harder by design: each segment needs its own visibility mechanism, or certificates inside it go unseen.
- Certificate proliferation compounds the problem. It's now trivially easy for individual teams (marketing, support, engineering) to stand up a CA or obtain a publicly trusted certificate on their own, outside any central process.
- Broader research on enterprise data awareness (cited independently in the discussion, not specific to certificates) suggests only around 1 in 10 organizations can reliably account for 100% of their data footprint — a sobering benchmark for how confident any inventory claim should be taken.

Complexity Has Become the Default State

Consolidation onto a single platform is frequently framed as the fix for PKI sprawl — but the discussion flagged a specific trap: a “platform” that's really a loose bundle of disconnected tools doesn't solve the visibility problem, it just relabels it. In practice, most organizations are running two to three certificate-tracking methods simultaneously — some combination of manual spreadsheets, a certificate lifecycle management (CLM) tool, and what the panelists bluntly called “tribal knowledge”: certificates whose existence lives only in one person's memory.

- When ownership of tracking is split across teams using different methods, certificates fall into the gaps between them — unowned by either side, invisible to both, and the leading cause of unplanned outages.
- Automation coverage is uneven even inside a single, well-resourced program: in the case study, roughly half of devices initially supported ACME-based automation, requiring a mix of ACME, SCEP, and custom scripting to close the gap — and active coordination with device manufacturers (firewalls, HSMs, UPS systems were specifically flagged as lagging) to extend support over time.
- Cross-team coordination compounds further in regulated industries like healthcare and banking, where certificate changes often require coordinating with partner organizations and external teams entirely outside the company's own processes.

DNS: The Dependency Nobody Re-Budgeted For

This is where the PKI conversation stops being self-contained. Public certificate issuance and renewal depend on domain control validation (DCV) — proving ownership of the domain a certificate covers, typically by publishing a specific DNS record or responding at a specific URL. As the panel noted directly, getting public PKI validated *"oftentimes"* requires actively coordinating with the DNS team — and called it out as a distinct source of cross-team complexity in its own right.

That coordination used to be an occasional, low-stakes task: set the record once at issuance, revisit it rarely. Two industry shifts are changing that calculus at the same time — certificate validity periods are compressing toward 47 days (with shorter windows already under discussion), and the industry is moving toward domain validation windows as tight as roughly every 10 days. Every one of those cycles is a DNS transaction. A DNS team, or a DNS automation pipeline, that can't keep pace with that cadence becomes a certificate-outage risk — even if DNS resolution itself never goes down.

Dimension	Traditional Model	2026 Reality
Validation frequency	Set once at issuance; rarely revisited.	Recurring on a compressed cycle — trending toward roughly every 10 days as validation windows shrink industry-wide.
Relationship to PKI	Adjacent function; occasional, low-urgency coordination.	An embedded dependency inside the automated certificate issuance pipeline itself.
Failure mode	DNS outage means the site is unreachable — a familiar, well-monitored failure.	A slow or missed DNS change can silently block certificate renewal — producing a certificate outage even though DNS is technically "up."
Automation requirement	Manual record changes were an acceptable operating model.	API-driven, credentialed, auditable DNS changes are needed to support ACME-style automated validation at this pace.
Ownership model	Owned solely by the network/ infrastructure team, largely independent of security.	Needs shared governance between DNS/network teams and PKI/security stakeholders — the two can no longer operate on separate clocks.

The practical implication: DNS operational maturity — how automated, API-accessible, and well-governed an organization's DNS infrastructure is — is becoming a direct, measurable gating factor for whether that organization can keep up with shrinking certificate lifecycles at all. Treating DNS as static, low-priority infrastructure is no longer a neutral choice; it's a constraint on the entire PKI modernization effort.

The Identity Explosion: Human, Machine, and Now Agentic AI

Machine identities already dominate PKI coverage by a wide margin over human user identities, and the research shows that gap is widening. IoT devices, personal and BYOD phones, and — increasingly — autonomous AI agents operating on the corporate network are all adding to the pool of things that need an identity, a secure channel, and a lifecycle to manage.

- In the survey, 61% of organizations are prioritizing machine identity in their modernization efforts, versus 55% prioritizing user (human) identity — both substantial, neither dominant.
- Agentic AI identity coverage is currently the smallest category measured, which the panel attributed to how new the category is — not to how large it will stay. The expectation is that it grows significantly and quickly.
- One practical framing offered in the discussion: treat an AI agent like any other untrusted device joining the network — segmented, identified, communicating over a secured channel, and subject to health checks or signed attestations — rather than as a special case exempt from identity discipline.
- Software supply-chain identity is a related, growing concern: signing containers, builds, and third-party/open-source components as part of the build pipeline was cited as a direct response to rising software supply-chain risk.

Everyone Uses PKI. No One Owns It.

Asked who the final decision-maker for PKI is inside their organization, respondents overwhelmingly pointed to the CISO — by a wide margin over any other role. The panel flagged this as a potentially flawed default: PKI cuts across so many teams that concentrating final ownership in security alone, without broader organizational buy-in, is fragile.

The alternative pattern described in the case study is a three-way alignment rather than a single owner:

- **CISO** — for policy support and organizational alignment.
- **CTO** — because engineering/SRE teams typically manage the largest volume of certificates day to day; without automation, a single certificate renewal can consume roughly an hour of engineering time.
- **CIO** — as the heaviest consumer of internal and user-facing certificates.

A related organizational pattern worth noting: rather than centralizing certificate operations, one approach is to appoint a neutral policy owner — sitting outside both the CIO's and CTO's direct reporting lines — who sets and enforces policy without taking over day-to-day certificate management, which stays with the individual business units that already do that work. The stated goal is to guide and correct without creating a bottleneck or notification fatigue for the teams doing the deployments.

The Readiness Gap: Intent vs. Execution

Perhaps the clearest signal in the research is the size of the gap between recognizing the problem and actually resourcing a fix for it.

Metric	Finding	What It Means
Clear understanding of what a modernization program requires	About 1 in 3 organizations	Most are operating on partial or beginner-level understanding, even where the business case is already accepted.
Actively implementing modernization today	About 1 in 4 organizations	The remaining majority are still in a planning stage, not an execution stage.
Planning to modernize within the next 12–24 months	Roughly three-quarters of organizations	Intent is close to universal. Execution capability is not.
Confidence in near-term post-quantum readiness	Low, by the panelists' own assessment	Most organizations still need to resolve foundational visibility and automation gaps before PQC planning becomes practical.

Why “Later” Isn't a Neutral Choice

Three separate pressures are compounding on the same timeline, not spread out over the next several years:

- **Certificate lifespans are compressing** toward a 47-day maximum, with shorter public roots and intermediate CAs expected to require future rotation as well.
- **Post-quantum cryptography adoption dates have been moved up** — for the first time in years, according to the panel — while the industry is still actively debating hybrid versus pure post-quantum approaches.
- **AI is accelerating the discovery of weaknesses** — outdated protocols, unpatched vulnerabilities, and poor communication practices — faster than defenders can typically respond, which raises the cost of any remaining blind spot in the certificate estate.

Combined, these mean an organization that is not crypto-agile when “harvest now, decrypt later” threats mature into an active exploitation problem may not have the operational ability to rotate its way out of it in time. The panel was explicit that immediate, urgent action on post-quantum cryptography specifically isn't yet warranted for most organizations — but building the underlying visibility, automation, and inventory discipline that any future PQC migration will depend on can't be deferred until the deadline approaches.

There is also a supply-chain dimension: an organization's own PKI hygiene is only part of its exposure. The panel specifically recommended checking with vendors and device manufacturers — IoT vendors in particular were named — about their own PKI modernization posture, since a vendor's lagging automation support can become the customer's outage.

What This Means for Leadership

None of these points to a single fix, and the research doesn't endorse one. What it does make clear is that the status quo — partial inventories, diffuse ownership, DNS treated as a separate concern from certificate lifecycle, and modernization treated as a someday project — is no longer a sustainable operating position given the pace described above. Questions worth putting to your own teams:

1. Do we have a complete, current inventory of every certificate we operate—including those issued outside central IT?
2. Is DNS change management fast and automated enough to support the validation cadence our certificates now require — and does that team know it's now on the critical path for uptime?
3. Who actually owns PKI policy versus PKI operations in our organization, and is that split clear enough to survive a key person leaving?

4. Have we asked our critical vendors and device manufacturers what their own certificate automation and PQC posture looks like?
5. If a quantum-capable adversary were able to break current asymmetric cryptography tomorrow, could we actually rotate our estate in time — and if not, what's the realistic timeline to get there?

Bottom Line

PKI's operating assumptions were built for a slower world: certificates that lasted a year or more, DNS changes made rarely, and a small, well-understood population of human and server identities. Every one of those assumptions is now false, and the pace of change — shrinking certificate lifespans, recurring domain validation, AI-driven identity growth, and a compressing post-quantum timeline — is accelerating, not stabilizing. Standing still is itself a decision, and based on the data discussed here, it's an increasingly expensive one. The right next step will look different for every organization; what the research makes hard to justify is treating the current approach as good enough for what's coming.