EXECUTIVE PRIMER

DNS Under Pressure: Why Domain Validation Is Becoming Your Next Operational Bottleneck

What CISOs and CTOs need to know as certificate lifetimes shrink from over a year to 47 days — and domain validation turns from a one-time task into a continuous cycle

This primer distills a 2026 industry webinar on DNS and certificate automation, presented by a certificate authority's solution engineering and DNS product teams as part of an ongoing automation-focused webinar series. It is written for a US CISO/CTO audience and does not endorse or recommend any specific vendor, product, or solution — examples from the session are cited only to illustrate the operational pattern.

Bottom Line Up Front

Domain control validation — proving you own or control a domain before a certificate authority will issue a certificate for it — used to be a once-a-year formality. As certificate lifespans compress and validation reuse windows shrink even faster, it's turning into a recurring operational requirement that most organizations are still handling with the same manual, ticket-based process they used when it only happened annually.

- **The clock is compressing fast.** Certificates have already dropped from roughly 13 months to 200 days, are headed to 100 days in 2027, and will hit 47 days — with domain validation reused for only 10 days — by 2029.
- **DNS and PKI teams are organizationally separate in most large enterprises** — and every domain validation event has historically required a ticket to cross that gap. That gap doesn't scale to a continuous, recurring process.
- **Automation is available, but it isn't automatic.** Whether through the ACME protocol or a purpose-built platform integration, closing this gap takes a deliberate architectural choice — not just goodwill between teams.

The Certificate Lifetime Countdown

The industry-wide schedule driving all of this is set by the CA/Browser Forum and applies to every publicly trusted certificate, regardless of which certificate authority issues it. As of this writing, the first two reductions have already taken effect.

Effective Date	Max. Certificate Validity	Domain Validation Reuse Window	What Changes
Recent history (pre-2026)	~398 days (~13 months)	~398 days	Validation and certificate life moved together — revalidate roughly once a year.
March 2026 (in effect now)	200 days	200 days	Issuance cadence has already doubled; validation still tracks the certificate's life.
March 2027	100 days	100 days	Cadence doubles again — certificates now need reissuing roughly every 3 months.
March 2029	47 days	10 days	For the first time, domain validation expires faster than the certificate. Issuing more than one certificate per domain inside a cycle now requires revalidating control mid-cycle.

That last row is the crux of the problem. Once domain validation windows drop below certificate validity, validation stops being tied to "when the certificate is issued" and becomes its own independent, recurring clock — one that keeps running regardless of how many certificates a domain needs.

What Domain Control Validation Actually Requires

Domain control validation (DCV) is the mechanism by which a certificate authority confirms that whoever is requesting a certificate for a domain actually controls that domain. In practice, that almost always means publishing a specific record — typically a DNS TXT record — that the certificate authority can look up and confirm before issuing.

- **Domain Validation (DV)** is the baseline check — confirming control of the domain, and nothing more.
- **Organization Validation (OV)** adds a layer of verified business identity on top — but still starts with the same domain control check underneath.
- **Extended Validation (EV)** adds further scrutiny on top of that — but again, domain validation is still the foundation every certificate type is built on.

That last point is easy to overlook: no matter how rigorous an organization's certificate policy is, every single certificate — DV, OV, or EV — depends on the same underlying DNS-based validation step. Whatever friction exists in that step applies to the entire certificate program, not just to the "cheap" certificates.

The Manual Process Most Organizations Still Run

In many large enterprises, the PKI team and the DNS team are separate groups that interact only when a domain needs to be validated. The typical flow looks like this: the PKI team orders a certificate, needs to prove control of the domain, and opens a support ticket with the DNS team to get a validation record created. That ticket enters a queue. Fulfilling it often requires a manager's change-control approval — which can itself be delayed if that manager is unavailable. Only once the record is written does the ticket route back, allowing the certificate authority to confirm the record and issue the certificate.

Even in smaller organizations where a PKI administrator has direct access to DNS, the work doesn't disappear — it just moves from inter-team coordination to a manually repeated task, one that becomes a real burden at the scale of hundreds or thousands of certificates.

Dimension	Manual, Ticket-Based Process	Automated, Integrated Process
Team coordination	PKI team opens a ticket with the DNS team; the request sits in a queue until picked up.	No handoff required — validation record creation and confirmation happen programmatically between systems.
Approval chain	Often requires a manager's change-control sign-off before the DNS record is written.	No human approval step sits inside the validation loop itself.
Typical time to complete	Hours to multiple days, depending on staffing, queues, and approvals.	Minutes — the system polls DNS until the record resolves, then marks validation complete.

Dimension	Manual, Ticket-Based Process	Automated, Integrated Process
Error risk	Manual record entry carries a real risk of typos or misconfigured values.	Records are system-generated and system-verified, removing manual entry as a failure point.
Record cleanup	Validation records are frequently left in place indefinitely once created.	Records can be automatically removed once each validation cycle completes.
Scaling to hundreds/ thousands of certs	Each certificate can mean another round of tickets and approvals.	The same workflow runs unattended, regardless of certificate volume.

DNS Hygiene: The Overlooked Risk

One point raised in the session deserves more attention than it usually gets: leftover validation records aren't just clutter, they're an operational risk in their own right. Every accumulated TXT record under a given label adds to the size of the DNS response for that label. Enough accumulated records can push a response past the size a standard DNS query can carry, forcing clients to fall back from UDP to TCP just to complete the lookup — adding latency and, in some resolver configurations, outright failures.

- Some newer validation methods use a persistent token that's designed to stay in DNS indefinitely and be reused across validation cycles — convenient, but it works against the basic hygiene principle of removing a record once it's served its purpose.
- An approach that automatically retires each validation record once a cycle completes avoids that accumulation entirely — but only if cleanup is actually built into the process, rather than left as a manual follow-up step nobody circles back to.
- At a validation cadence measured in days rather than months, across potentially hundreds of domains, un-cleaned records compound quickly. What was a minor housekeeping item at an annual cadence becomes a real technical debt problem at a weekly or 10-day cadence.

Access Scope Matters as Much as Automation

Automating domain validation solves the speed problem, but it introduces a new question: how much access does the automation actually have inside your DNS zone? This is a legitimate point of friction between DNS and security teams. A generic automation client is often granted fairly broad DNS-editing credentials — enough to manage the validation record it needs, but frequently enough to touch far more of the zone than that. DNS teams are, understandably, wary of handing out that level of access.

- A narrower alternative is to scope automation access down to only the specific, system-generated records needed for validation — and only on domains explicitly designated as eligible for that automation, rather than the entire DNS account by default.
- Whatever automation approach an organization chooses — a scripted protocol client, a managed platform integration, or something built in-house — the access-scope question is worth asking explicitly rather than assuming the default configuration is the safe one.
- This is a genuine trade-off, not a solved problem: broader access tends to mean simpler setup and fewer moving parts; narrower, scoped access tends to mean more configuration up front in exchange for a smaller blast radius if credentials are ever compromised.

A Terminology Trap Worth Clearing Up

Not every “DNS provider” can actually host a domain validation record, and conflating the two types causes real confusion. The distinction came up directly in the session's Q&A, in response to a common misconception about which DNS products can support validation at all.

DNS Type	What It Does	Can It Host a Validation Record?
Authoritative DNS	Hosts the actual DNS zone for your domain — the source of truth that resolvers query to reach your services.	Yes — this is where a validation record must be published for a certificate authority to find it.
Recursive DNS	Resolves lookups on behalf of clients or users (for example, an organization's outbound internet DNS resolver).	No — it doesn't host your zone, so it cannot be used to prove domain control.

The practical takeaway: confirm which category each DNS product in your environment actually falls into before assuming it can participate in certificate validation. This also matters in multi-vendor DNS setups — organizations running primary and secondary authoritative DNS across more than one provider should specifically verify that validation records written to the primary are propagating correctly to every secondary before relying on automation in production.

Where This Is Heading: Delegated Validation

One emerging pattern worth watching, discussed as a near-term roadmap item in the session, is decoupling domain validation from full DNS ownership entirely. The mechanism is a targeted DNS delegation: an organization creates a CNAME record at a specific, dedicated label in its own zone that points to a separate validation service, without migrating or handing over control of its actual DNS hosting. The validation service can then manage just that narrow slice of DNS activity — automatically and on a recurring cycle — regardless of which company hosts the organization's primary authoritative DNS. The significance for planning purposes: this pattern suggests the industry is moving toward treating domain validation as its own decoupled service layer, rather than something that has to be bolted onto whichever DNS platform an organization already uses. That's worth factoring into any longer-term DNS or PKI architecture decision, independent of which specific vendor ultimately offers it.

What This Means for Leadership

None of these points to one specific product or platform, and the session itself repeatedly acknowledged multiple valid paths — a scripted ACME implementation, a managed platform integration, or some hybrid depending on the DNS providers already in use. What's no longer optional is treating domain validation as a designed, owned, and automated process rather than an ad hoc ticket exchange. Questions worth putting to your own teams:

- How long does a domain validation cycle actually take today, end to end, including approvals, and does that timeline still work at a 100-day or 47-day certificate cadence?
- Do our PKI and DNS teams have a standing working relationship, or does coordination only happen when a ticket forces it?

- What access does our current certificate automation (if any) actually have inside our DNS zones — and is that access scoped, or broader than it needs to be?
- Do we have a process for cleaning up validation records after use, or are they accumulating unnoticed?
- If we run DNS across more than one provider or in a primary/secondary configuration, has automated validation actually been tested against that full topology — not just the simplest case?
- Is our authoritative DNS infrastructure itself API-driven and automatable, or would supporting this kind of validation cadence require a platform change first?

Bottom Line

Domain validation was designed for a world where certificates lasted a year and DNS changes were rare, deliberate events. That world is ending on a fixed, published schedule — not a hypothetical one. By 2029, validation will need to happen faster than certificates themselves expire, on domains that may number in the hundreds or thousands per organization. A manual, ticket-based handoff between separate PKI and DNS teams was already a source of delay and error at an annual cadence; it does not scale to a continuous one. The specific mix of protocol automation, platform integration, and process redesign will differ by organization — but the underlying requirement, that domain validation become a designed and automated capability rather than a manual afterthought, is no longer optional on any timeline leadership controls.