

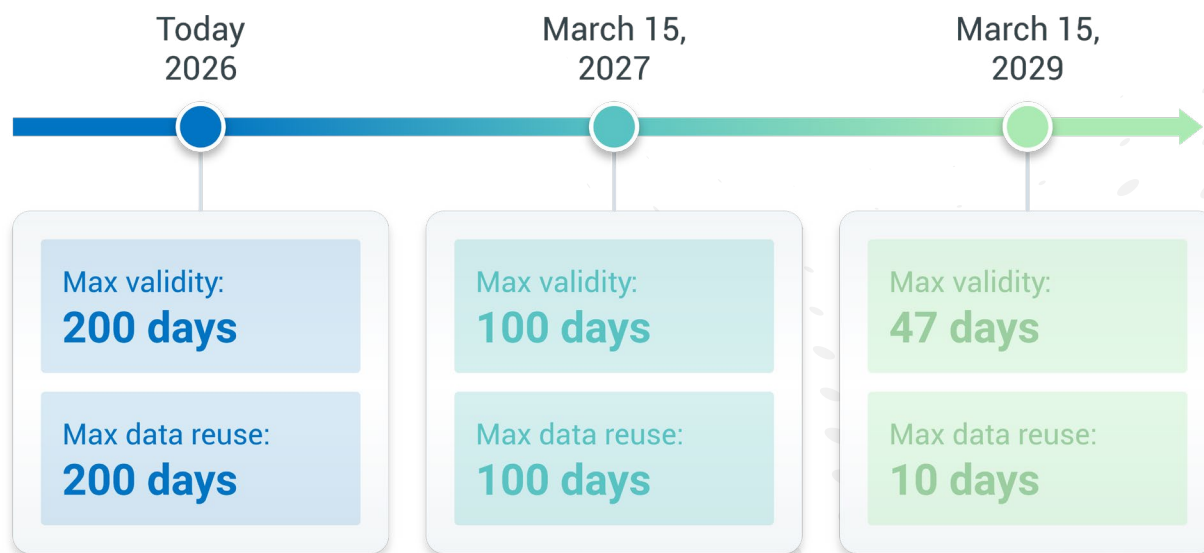
Unified trust: Automating PKI and DNS workflows

Overview

In an era of increasing digital complexity, the reliability of your online presence depends on the seamless coordination of Public Key Infrastructure (PKI) and the Domain Name System (DNS). Historically, these two critical functions have operated in silos, leading to operational friction and security gaps.

As the [CA/B Forum roadmap](#) pushes toward a **47-day certificate lifespan by 2029**, the window for manual domain validation is closing. Organizations must move from manual, ticket-based processes to a unified digital trust fabric that automates domain control and certificate issuance at scale.

Shrinking certificate lifespans



The challenge: Siloed operations and rising risks

Enterprise security teams are facing a “perfect storm” of shrinking lifecycles and fragmented workflows.

Operational friction

Large-scale enterprises illustrate the challenges of disconnected PKI and DNS teams:

- **Access constraints:** DNS teams prioritize stability and are often hesitant to grant certificate teams the access required for Domain Control Validation (DCV)
- **Communication delays:** Relying on manual ticketing for DNS record creation causes delays in certificate issuance, often taking hours or days when seconds matter
- **Scalability barriers:** Manual DNS-01 validation—which requires the precise creation and removal of TXT records—is prone to human error and cannot scale to meet the high-frequency renewal demands of 47-day lifecycles

The cost of disruption

- **Legacy vulnerabilities:** 2025 industry outages, such as those affecting major providers like Cloudflare, highlight the risk of DNS as a single point of failure
- **Compliance and downtime:** Failure to synchronize DNS and PKI leads to expired certificates, browser warnings, and lost revenue. For many enterprises, even minutes of downtime results in significant financial and reputational damage.

DigiCert's 2025 Trust Pulse Survey highlights the business impact of mismanaged digital certificates

45%

45% of respondents reported experiencing service **downtime due to certificate-related incidents** in the last year

31%

31% of organizations reported **losses of \$50,000 - \$250,000**, while **18.5% lost more than \$250,000** due to certificate-related issues

50%

Over **50%** of respondents endured **5 - 24 hours of downtime** and **15.4%** experienced **25 hours or more of downtime**

In addition:

- **37.5%** attributed **outages specifically to expired certificates**—one of the most preventable causes of disruption in enterprise environments
- **56.6%** expressed concern about their ability to **track certificate expiration dates**

The Solution: DigiCert ONE

DigiCert® ONE converges PKI and DNS into a [single, intelligent platform](#), enabling end-to-end automation of digital trust. With DigiCert ONE, organizations can eliminate manual intervention and ensure SLAs of 100% availability.

Automated Domain Control Validation (DCV)




Our integrated solution automates the DNS-01 challenge, the most secure method for domain validation.

- **Zero-touch provisioning:** DigiCert CertCentral automatically pushes the required TXT records to UltraDNS and removes them once validation is complete
- **Enhanced security:** Remove the need for DNS team intervention or shared credentials, maintaining a strict security posture while accelerating workflows
- **Continuous validation:** Validate domains every seven days to ensure renewals are always “ready to fire,” eliminating issuance delays

The DigiCert advantage

- **100% uptime SLA:** UltraDNS is built on a global Anycast network with 50+ nodes and 3,000+ peers, ensuring your DNS—and your certificates—are always reachable
- **Unified visibility:** Manage DNS records and certificate lifecycles from a “single pane of glass,” providing total oversight for both IT and Security teams
- **Future-ready:** Built for the “Quantum Age,” our platform provides the crypto-agility needed to adapt to changing industry standards and shorter lifespans

Efficient, automated, resilient DNS means...

 Availability 100% uptime SLA	 Security Reputable, secure brand	 Scalable operations Always-on reliability Future-proofed	 Revenue growth Consistent CX Reduce abandonment Market expansion
--	--	---	--

About DigiCert

DigiCert is a global leader in intelligent trust. We protect the digital world by ensuring the security, privacy, and authenticity of every interaction. Our AI-powered DigiCert ONE platform unifies PKI, DNS, and certificate lifecycle management, to secure infrastructure, software, devices, messages, AI content and agents. Learn why more than 100,000 organizations, including 90% of the Fortune 500, choose DigiCert to stop today's threats and prepare for a quantum-safe future at www.digicert.com.

© 2026 DigiCert, Inc. All rights reserved. DigiCert is a registered trademark of DigiCert, Inc. in the USA and elsewhere. All other trademarks and registered trademarks are the property of their respective owners.