digicert®

Upgrading WebPKI for 10X Scale

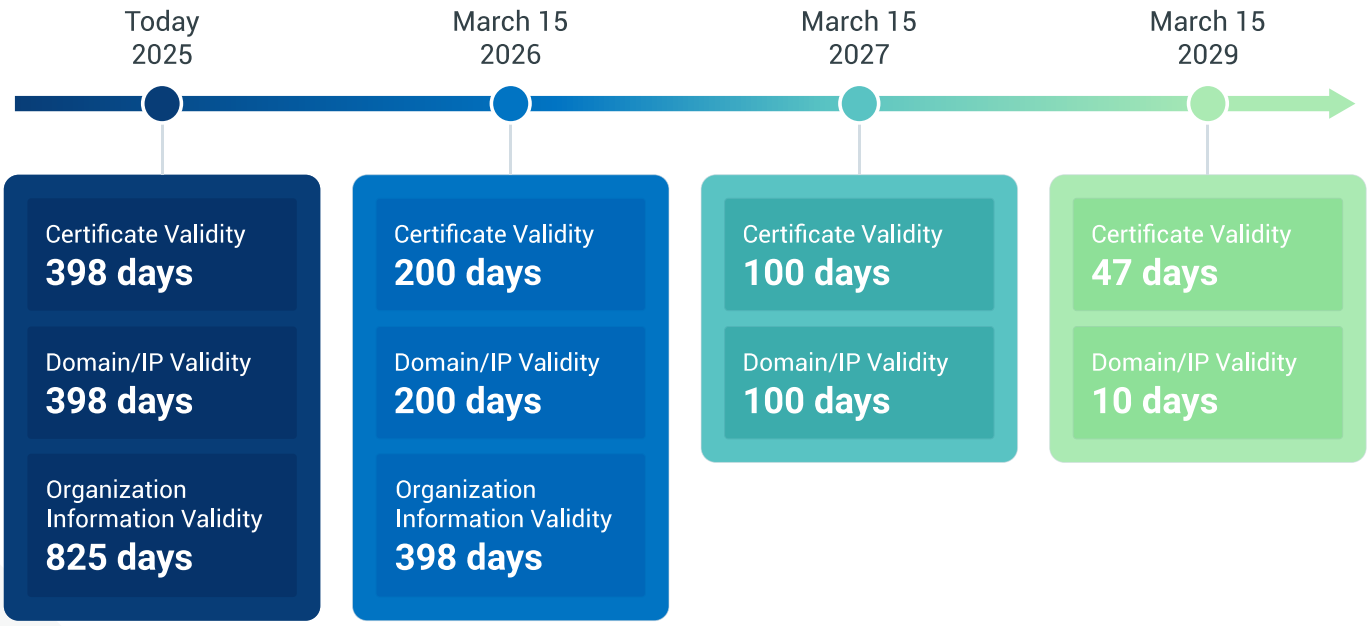
How DigiCert is investing in next-generation trust infrastructure and operations that enterprises need

WHITE PAPER

Executive Summary

The global Public Key Infrastructure (PKI) ecosystem is undergoing its most significant transformation in more than a decade. CA/Browser Forum policy changes will reduce TLS certificate validity from 398 days to 47 days by March 15, 2029. Domain and IP validation lifetimes will fall from 398 days to just 10 days. As a result:

- 8X more certificates will need to be issued
- 40X more domain validations will be required
- Organizations must automate or risk widespread outages and security failures
- PKI providers must massively scale infrastructure, security controls, and operations



8X more certificates, **40X** more validations will be needed

This white paper outlines DigiCert's comprehensive modernization program — across infrastructure, cryptography, compliance, automation, and operations — to support 10X more public certificates per day, ensure global trust, and deliver continuous digital security for enterprises, governments, and the public internet.

Scaling DigiCert Infrastructure 10X

DigiCert is scaling its enterprise WebPKI infrastructure by an order of magnitude, upgrading compute, cryptography, and global delivery so it can issue and manage dramatically more publicly trusted certificates without sacrificing performance, availability, or security.

Compute, Storage, and HSM Investments

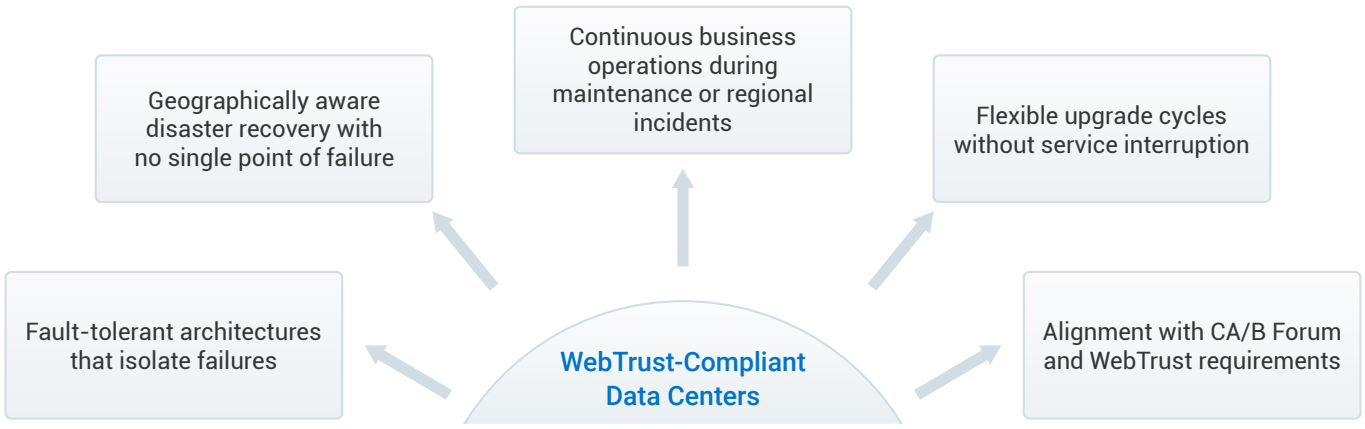
To meet a tenfold increase in certificate issuance, DigiCert is upgrading the core cryptographic and compute foundation that powers signing operations. These investments ensure the performance, durability, and elasticity required for a global trust service.

- High-performance signing clusters optimized for parallel certificate issuance
- Redundant global Hardware Security Module (HSM) networks for secure and compliant key protection
- Next-generation compute, storage, and analytics frameworks for high-volume PKI workloads
- Elastic scaling architecture to absorb global spikes without performance degradation

These upgrades provide the cryptographic throughput and low-latency performance necessary to sustain exponential growth in certificate demand.

Availability Zones in WebTrust-Compliant Data Centers

To strengthen continuity and fault isolation, DigiCert is implementing multiple availability zones within physically audited, WebTrust-compliant data centers. These zones enable independent operation and failover within the same region.



This design delivers significantly higher availability under increasing load, backed by DigiCert's 99.99% contractual SLA commitment.

Multi-Perspective Issuance Corroboration (MPIC)

As DNS threats expand globally, DigiCert now performs Domain Control Validation (DCV) and Certificate Authority Authorization (CAA) checks across multiple independent geographic vantage points.

- Detects poisoned DNS cache responses
- Identifies ISP or last-mile path manipulation
- Blocks regional man-in-the-middle (MITM) attacks
- Prevents asymmetric or inconsistent authoritative DNS responses

This MPIC approach significantly enhances issuance integrity and protects customers from region-specific DNS attacks.

Post-Quantum Cryptography (PQC) Investments

To prepare customers for the transition to quantum-resistant security, DigiCert has deployed next-generation PQC capabilities throughout its infrastructure. These capabilities enable organizations to begin adopting hybrid and pure quantum-safe certificates today.

- PQC-ready HSMs capable of handling larger key sizes
- Dedicated PQC private roots anchoring next-generation certificate hierarchies
- Support for all NIST- approved PQC algorithms with high-performance optimizations
- Production-ready issuance of hybrid and pure post-quantum certificates

DigiCert is establishing a quantum-safe trust foundation designed to protect customers and their ecosystems for decades.

Scaling CT, OCSP, and CRL Infrastructure

As issuance volumes grow, Certificate Transparency (CT), Online Certificate Status Protocol (OCSP), and Certificate Revocation List (CRL) systems must scale accordingly. These services ensure that browsers and servers can verify certificate authenticity and revocation status in real time.

- Sharded and replicated CT log infrastructure with high-volume ingestion
- Global edge distribution for both OCSP responses and CRLs
- Advanced monitoring and alerting pipelines for rapid anomaly detection
- Redundant, geo-distributed infrastructure ensuring uninterrupted service

These enhancements guarantee predictable, fast, and reliable certificate status checking worldwide.

Multi-CDN Architecture for Global Performance and Resilience

To guarantee sub-100ms availability of trust artifacts worldwide, DigiCert has expanded its edge footprint using a Multi-CDN strategy. This provides maximum speed, redundancy, and stability across all global regions.

- Multiple Tier-1 Content Delivery Networks (CDN) for worldwide coverage
- Automated geo-routing to deliver responses from the closest edge
- Native DDoS protection integrated into the delivery path
- Unified OCSP response distribution across edge locations
- High-availability delivery for CT logs and CRLs

This multi-layered architecture ensures world-class performance and resilience for all trust services.

Upgrades Across 30+ Global Data Centers

DigiCert is modernizing infrastructure across more than 30 global data centers to support regional compliance, sovereign data requirements, and low-latency trust delivery. These upgrades include improvements to compute, transit, networking, and power redundancy, and span facilities in the United States, the European Union, Japan, Australia, and India. Together, these global investments ensure faster, more reliable, and regionally compliant trust services for customers wherever they operate.

Scaling DigiCert Support and Operations

World-class infrastructure requires world-class operational excellence. DigiCert is modernizing support, compliance, and cloud operations to handle 10X operational demand.

AI Automation for Organization & Extended Validation

As certificate lifetimes shorten, the speed and accuracy of Organization Validation (OV) and Extended Validation (EV) become critical. DigiCert is applying AI to streamline validation, reduce friction, and ensure faster time-to-issuance at global scale.

- Business registration verification accelerated with AI
- Identity and entity confirmation using automated cross-referencing
- Document extraction, parsing, and classification through ML models
- Automated entity resolution and validation heuristics
- AI-driven fraud and anomaly detection for issuance security

These enhancements significantly reduce validation time, increase accuracy, and exceed industry baseline requirements.

Open-Source Domain Control Validation

Domain Control Validation (DCV) is the backbone of trust in TLS issuance. DigiCert's open-source DCV library provides a hardened, consistent, and automation-ready foundation that strengthens both customer and industry-wide security.

- Standardized validation logic for all DCV methods
- Hardened DNS and HTTP validation mechanisms
- Transparent, auditable implementation for the ecosystem
- Automation-friendly tooling for enterprise-scale deployments

This approach delivers consistent, secure domain validation and accelerates automation for customers operating at massive scale.

Scaling Global Support & Services

Shorter certificate lifecycles increase customer touchpoints and operational load. DigiCert is expanding its global support footprint to ensure high-quality service as issuance volume and automation demand grow rapidly.

- Expanded technical support personnel and systems
- Strengthened customer success and deployment teams
- Enhanced professional services for enterprise onboarding
- Specialized PKI operations and compliance engineering

These investments ensure world-class support quality even as certificate renewal cycles accelerate.

AI-Powered Knowledge & Self-Service Systems

As global PKI complexity increases, customers need instant access to accurate guidance. DigiCert is deploying AI throughout the platform to deliver intelligent, contextual help without requiring human escalation.

- AI guidance embedded across DigiCert ONE
- AI-driven support assistants for real-time troubleshooting
- AI-curated knowledge bases using internal and community content
- Context-aware diagnostic and resolution workflows
- Guided automation for common PKI, DNS, and lifecycle tasks

These systems elevate customer experience and power DigiCert's goal of maintaining an industry-leading NPS above 80.

Scaling Audits with Compliance Automation

As infrastructure and issuance scale, the audit footprint grows as well. DigiCert undergoes more than 30 audits annually and is automating audit preparation to maintain trust and compliance without operational bottlenecks.

- Automated evidence gathering across systems
- Structured control and policy mapping
- AI-based sampling for auditor review
- Continuous monitoring of compliance controls

DigiCert is expanding certifications to include ISO 27001 and FedRAMP, reinforcing its position as the most trusted global certificate authority.

Cloud Operations Automation

Scaling 10X requires a cloud operations model built on automation, observability, and safe deployment practices. DigiCert's Site Reliability Engineering (SRE) teams are modernizing cloud systems to deliver consistent, zero-downtime service worldwide.

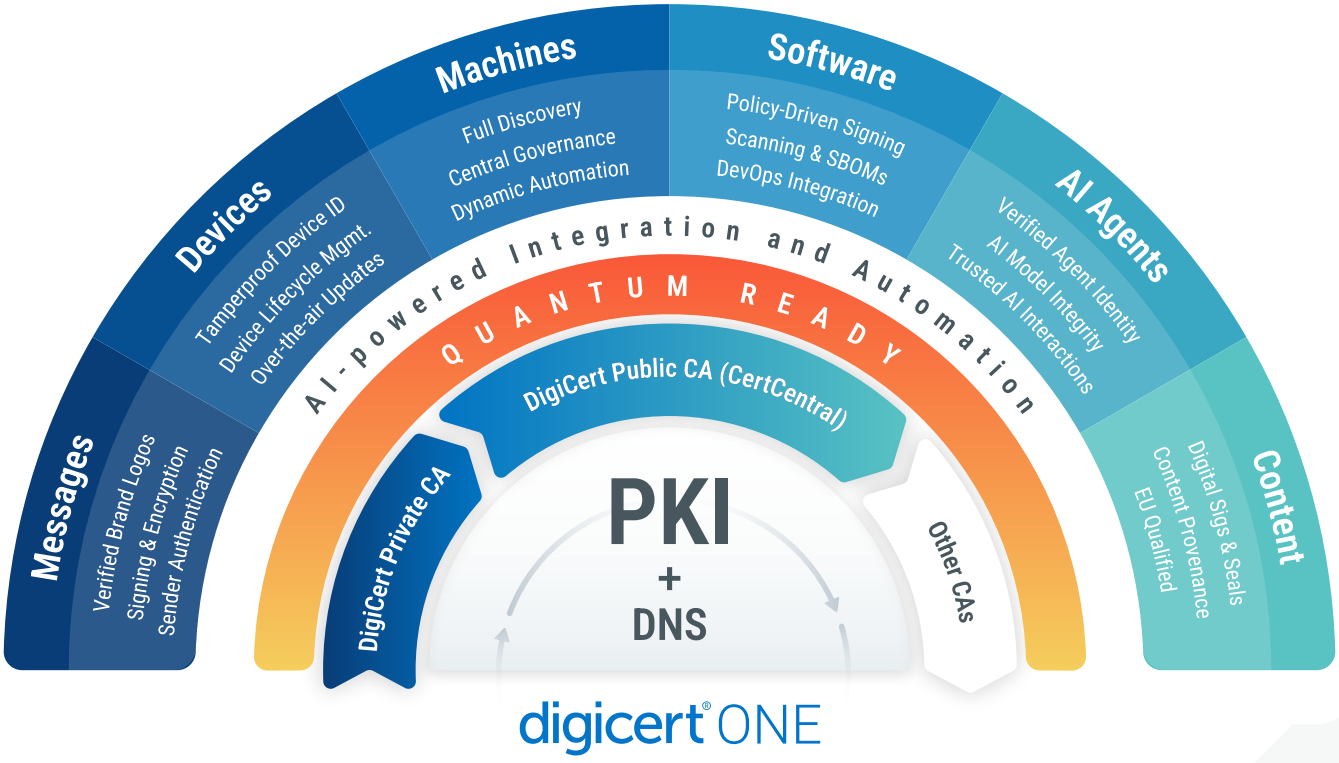
- Upgraded CI/CD pipelines for rapid, safe releases
- Blue/Green and canary deployment architectures
- Infrastructure-as-code governance for reliable provisioning
- SRE-authored automation playbooks for incident prevention
- Deep observability through real-time logs, metrics, and tracing

These investments enable continuous improvements while maintaining global uptime and consistent platform reliability.

Delivering Resilience for Customers

As certificate lifetimes shrink and renewal frequency explodes, automation becomes the only reliable way to keep environments secure and available. DigiCert is embedding automation into every layer of its platform so customers can eliminate manual renewal risk, reduce operational overhead, and prevent outages before they happen.

All DigiCert public TLS certificates include default support for ACME (Automated Certificate Management Environment), the industry-standard protocol for automating certificate issuance and renewal. With DigiCert's ACME service, customers can use DigiCert's built-in ACME client or any ACMEv2-compliant client (e.g. Certbot or win-acme) to request and install certificates directly from CertCentral. Once ACME credentials are configured, the client continuously manages certificate lifecycle events in the background, renewing certificates before they expire and deploying them to supported endpoints, which dramatically reduces TLS administration overhead and human error.



DigiCert ONE extends this automation model beyond public TLS into a unified platform for all enterprise PKI and DNS use cases as a SaaS offering. Built on a modern, container-based architecture, DigiCert ONE delivers scalable, extensible, and automated certificate lifecycle management and authoritative DNS across machines, software, IoT devices, services, and content in any environment, including cloud, on-premises, hybrid, and air-gapped deployments. Through DigiCert Trust Lifecycle Manager and its APIs, enterprises can automate discovery, issuance, renewal, and revocation for public and private certificates that secure internal and external servers, workloads, VPNs, WiFi, network access, and application infrastructure, while UltraDNS integration brings DNS and PKI into a single operational flow. This unified, policy-driven automation fabric reduces security risk, prevents outages, ensures compliance, and provides the fail-safe foundation customers need to operate at WebPKI scale.

Conclusion

The transformation of WebPKI, driven by radically shorter certificate lifetimes, continuous validation requirements, and the rise of quantum-era cryptography, marks the most disruptive shift in digital trust in decades. Meeting these changes requires more than incremental improvements; it demands a reinvention of scale, automation, resilience, and intelligence across the entire certificate lifecycle. DigiCert is investing ahead of the curve, delivering 10X issuance performance, global multi-zone redundancy, multi-perspective validation, quantum-safe cryptography, and an automation-first operational model powered by AI. With this next-generation platform, DigiCert enables organizations to operate securely and continuously, without outages, compliance risk, or unnecessary operational burden, even as trust requirements accelerate each year. DigiCert is not just adapting to the future of WebPKI; it is defining that future and delivering intelligent, automated, globally resilient trust infrastructure for the next era of the internet.

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.