

Certificate lifecycle management is about to become a massive MSP headache

The CA/Browser Forum has issued a mandate to reduce TLS certificate lifetimes down to 47 days by March 2029, with staged enforcement starting now. MSPs responsible for preventing customer downtime face an exponential increase in cert renewals and reduced visibility, increasing the risk of outages.

2026	2027	2029
 199 days 2x renewals a year	 99 days 4x renewals a year	 47 days 8x renewals a year

Why you and your managed customers can't wait

Certificate visibility gap	47-Day renewal crisis	47-Day renewal crisis
✓ MSPs can't see where all their certificates are, or when they expire	✓ 100 certs = 800+ renewals/year at 47 days. Manual processes can't keep up	✓ "Harvest now, decrypt later" attacks are real today
✓ For every public TLS cert, there could be thousands of hidden internal PKI certs on servers, network devices, and user devices	✓ Let's Encrypt already forces 90-day renewals with no central certificate management	✓ <5% of orgs have implemented quantum-safe encryption. PQC migration requires a complete cert inventory
✓ Shadow CAs, forgotten ADCS instances, and non-standard private CAs are quietly multiplying risk	✓ 1-2 hours of engineer time per renewal 8x a year is untenable	✓ Government regulation on PQC starts in 2027

How DigiCert private PKI + MSP hub solves the problem for you

Asset discovery	Zero-touch automation	White-labeled CA for MSPs	PQC-ready today
Surface every certificate (public, private, shadow CAs) across your customer's infrastructure	Avoid SLA breaches and outages caused by expired certificates with fully automated renewals and no human intervention	Become the trusted certificate authority for your customers. Issue certificates, define the SLAs, and own the relationship.	PQC starts with inventory. Tag certificates by algorithm, and migration becomes a policy change. U.S. Executive Order 14409 raises the urgency.

What the numbers say

66% of organizations experienced certificate expiration outages last year DigiCert Trust Pulse Survey, 2025	\$250K+ per incident lost by 18.5% of organizations per certificate-related outage DigiCert Trust Pulse Survey, 2025	312% ROI on DigiCert ONE over 3 years, with payback in under 6 months Forrester TEI Study: DigiCert ONE, 2025
--	---	--

Ready to show your customers what's really running in their environments?

Talk to DigiCert about extending PKI management-as-a-service into your MSP offering.
 Contact DigiCert's MSP Partner Program: Scott Mellegaard scott.mellegaard@digicert.com
 Not Yet a DigiCert Partner? <https://www.digicert.com/partners>

About DigiCert

DigiCert is a global leader in intelligent trust, securing people, data, and devices with AI-powered solutions built to stop threats today and prepare for a quantum-safe future.

© 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.