digicert®

Selling Private PKI: MSP Partner Program Seller's Guide

Quantum, AI, and PKI Sprawl permanently derailed manual certificate management

Field seller's guide to building a private PKI practice with the problems, solutions, discovery questions, objection handling, and financial proof points to win every conversation.

Seller's Guide | Confidential MSP Partner Use Only | May 2026 | Quantum Ready | Private PKI Practice

$250K+

lost by 18.5% of orgs per cert incident. Half endured 5–24 hrs downtime

DigiCert Trust Pulse Survey, July 2025

312%

ROI on DigiCert ONE over 3 years payback under 6 months

Forrester Total Economic Impact Study, 2025

47

days max TLS cert lifetime by March 2029. 8x more renewals per certificate per year

CA/B Forum Ballot SC-081, 2025

How to use this guide

01

Use **discovery questions** to open the conversation and surface pain your customer doesn't know they have

02

Match the **problem statement** to the pain point, then bridge directly to the DigiCert solution

03

Use **value metrics** and real incident examples to anchor the financial conversation

04

Close with the **MSP revenue model,** showing how this practice pays for itself and grows the customer's margin

Seller's Guide | 2026

01 The visibility gap: no one knows how many certificates they have

The executive team thinks there's a handful of certificates, when in reality, it's thousands (or more).

The problem

> *"We track our certs in a spreadsheet. We think we have around 200."*
>
> IT Manager, nearly every enterprise you'll call

For every 5 external TLS certificates a customer manages, there are roughly 1,000 private certificates running their internal infrastructure servers, VPNs, domain controllers, mobile devices, containers, and code signing pipelines. Most organizations have no centralized inventory, no single owner, and no accurate count. The problem can't be solved until it can be seen.

✗ **Shadow CAs** issuing certs with no governance or revocation infrastructure

✗ **Spreadsheets and homegrown tools** that only track certs the team knows about

✗ **No ownership model,** with developer-spun CAs and forgotten AWS Private CA instances

✗ **Over 56% of organizations** admit they can't reliably track certificate expiration dates

Discovery questions

- Q1 How many certificates does your organization currently manage, and who owns that number?
- Q2 How do you track certificates today? Spreadsheet, CA portal, CMDB, or something else?
- Q3 When did you last do a full audit of your internal PKI? What did it surface?
- Q4 Do you know how many certificate authorities are issuing certs inside your environment right now?

DigiCert solution:

✓ Full certificate discovery across all environments: public CAs, private CAs, AWS Private CA, Microsoft ADCS, Let's Encrypt, shadow CAs, and third-party tools like Qualys and Tenable

✓ Centralized inventory dashboard, showing every cert, its CA, expiry, owner, PQC readiness, and policy compliance status in real time

✓ AI Co-Pilot for accelerated discovery and gap identification, surfacing what manual audits miss

✓ No rip-and-replace required: Trust Lifecycle Manager overlays existing infrastructure and governs all CAs from one pane

MSP value & proof points

66%
of organizations experienced unexpected cert expiration outages
DigiCert State of PKI Automation Report

51%
of enterprises do not know how many public or private certs they have
DigiCert State of PKI Automation Report

MSP differentiator

Position the initial Trust Lifecycle Manager discovery deployment as a billable PKI Health Check engagement. The inventory report it produces is an executive-ready deliverable your customer can take to their board, insurer, and auditor. This is the door-opener that sells itself.

What to say

"Most of our enterprise customers are shocked by what the first discovery scan surfaces. We've seen organizations think they have 300 certificates and find 8,000. The good news is we can show you the complete picture in days, and you'll own that inventory report regardless of what you do next."

02 The 47-day mandate: manual renewal is mathematically broken

Certificate lifetimes are shrinking. Renewal frequency is multiplying. Manual human labor can't keep up.

The problem

> *"We manage our renewals manually. It's painful but we get it done."*
>
> IT Lead who hasn't done the math on 47 days yet

The CA/Browser Forum has mandated that TLS certificate lifetimes reduce from 398 days to 47 days by March 2029, with staged reductions beginning March 2026. What has been a once-a-year task will soon be a continuous operation.

Organizations managing 100 external certs manually today will need to execute 800+ renewals per year by 2029, with each requiring DNS validation, ticket creation, CSR generation, installation, and endpoint binding.

- ✗ **1–2 hours of labour per renewal** on DNS validation, ticket workflow, approvals, installation
- ✗ **8x more renewals per certificate per year** by March 2029 with zero new headcount budgeted
- ✗ **Let's Encrypt certs** already require 90-day renewals with no central management tool
- ✗ **MSPs billing ~$250–$750 per certificate rotation,** which is unsustainable at scale without automation

Discovery questions

- Q1 How long does a single cert renewal take end-to-end today, including ticketing and validation?
- Q2 Have you modelled what your renewal workload looks like under 47-day lifetimes?
- Q3 How many Let's Encrypt or other free certs are in your environment, and how are those expirations being tracked?
- Q4 What happens to your team's capacity if renewal frequency doubles in 2027 and doubles again by 2029?

DigiCert solution:

- ✓ **Automated renewal via ACME, EST, SCEP, and CMPv2** for zero-touch cert replacement with no human in the loop
- ✓ **Manages Let's Encrypt issued certs through Trust Lifecycle Manager**, enabling certs to become a managed, automated service your MSP bills for
- ✓ **Bulk reissue and renew workflows** for batched remediation of expiring cert cohorts
- ✓ **DevOps and CI/CD pipeline integrations** provisions certs automatically at deployment, not after the fact
- ✓ **AI Co-Pilot** for non-standard systems where protocol-based automation isn't available

MSP revenue math

$7.9M

labour savings over 3 years per enterprise with DigiCert ONE

Forrester TEI Study, 2025

$18–25

DigiCert Trust Lifecycle Manager software cost per seat per year vs. $750–$1K billed per manual rotation

DigiCert MSP Pricing, Oct 2025

MSP differentiator

Trust Lifecycle Manager is the only CLM platform that manages all public third-party CA certs, including Let's Encrypt and Windows Certificates, all in one place. Increase services revenue by managing your customers 'free' certificates inside a single, automated management platform.

What to say

"At 47 days, every external cert needs to be renewed 8 times a year. If that's still manual, your team is spending 1–2 hours per renewal do the math on 100 certs. That's 800–1,600 hours a year just keeping the lights on. DigiCert Trust Lifecycle Manager makes every one of those renewals zero-touch."

03 The internal PKI problem: private certs are the real exposure

The external TLS conversation is table stakes. Private PKI is where the real risk and revenue lives.

The problem

> *"We handle our internal PKI with ADCS. It's fine."*
>
> IT Director whose ADCS hasn't been audited since 2019

For every 5 external certificates an enterprise manages, there are approximately 1,000 private PKI certificates running their internal infrastructure. These certs are issued by a patchwork of Microsoft ADCS instances, AWS Private CAs, no-ownership model developer-spun certificate authorities, and legacy homegrown systems with no centralized governance, no policy enforcement, and no revocation infrastructure. When one fails, it's not a website going down. It's a production line stopping or a payment system halting.

- ✗ **No single source of truth** across multiple internal CAs ADCS, AWS Private CA, HashiCorp Vault
- ✗ **Expired internal certs** cause silent failures in machine-to-machine authentication and VPN access
- ✗ **Lateral movement risk:** compromised certificate infrastructure is a primary attack vector, post-breach
- ✗ **M&A risk:** inherited certificate estates from acquisitions are routinely unaudited

Discovery questions

- Q1 Who owns your internal PKI today? Is there a dedicated team or does it sit with general IT?
- Q2 How many internal certificate authorities are issuing certs in your environment?
- Q3 When a VPN cert or server auth cert expires, how do you find out proactively? Is it typically a user complaint?
- Q4 Have you gone through any acquisitions in the past 5 years? Were the inherited cert estates audited?

DigiCert solution:

- ✓ **DigiCert Private CA** delivers a cloud-hosted, fully managed private CA, replacing on-premises ADCS across 7 global PKI facilities
- ✓ **MSP Branded Private CA** issues its own intermediate and root certs, assigns SLAs per customer, and becomes the CA
- ✓ **Multi-forest Active Directory support** with agent and agentless deployment options
- ✓ **UEM integrations** with Intune, JAMF, and MDM solutions for zero-touch device cert provisioning
- ✓ **Vault and IaC integrations** for HashiCorp Vault, Kubernetes, and Terraform support for DevOps pipelines

Scale proof points

1M+

certs managed by single enterprise customers on DigiCert ONE platform, zero chaos

DigiCert Customer Data

5,700+

public and private customers across 7 global PKI facilities with 25+ years of CA operations

DigiCert, 2025

MSP differentiator

The MSP Branded Private CA is the highest margin product in this portfolio. The MSP issues intermediate and private root certs under their own brand name, assigns custom SLAs per customer contract, and controls policy delivering a 'Big 4' systems integrations-level capability at software pricing.

What to say

"The TLS conversation is what got us in the room. But the private PKI conversation is where the real value is and where most of your competitors aren't going yet. With DigiCert, your MSP can become the certificate authority for your customers. You issue the certs. You set the SLAs. That's a fundamentally different relationship than reselling."

04 MSP liability: your SLA doesn't care why the certificate expired

As renewal frequency increases 8x, MSPs without automation are accumulating outage liability faster than they know.

The problem

> *"Certificate management isn't really in our managed services scope."*
>
> MSP Account Manager who will get that call at 2am anyway

If an MSP manages a customer's IT environment under a managed services contract and a certificate expires causing a production outage, the SLA breach falls on the MSP regardless of whether certificate management was explicitly in scope. The customer doesn't read the contract at 2am. They call their MSP. As cert renewal frequency increases 4–8x under the 47-day mandate, the probability of an expiry-related incident within a managed environment escalates proportionally.

✗ **SLA breach costs,** resulting in financial penalties, service credits, and contract renegotiation risk

✗ **Reputational damage:** 48% of orgs report customer confidence affected after a certificate outage

✗ **Emergency labour costs** an average of 5+ hours and 8 staff members, per incident, at engineer rates

✗ **Competitive vulnerability:** a single outage on your watch opens the door for a competitor MSP conversation

Discovery questions

- Q1 Have you ever had an outage trace back to an expired cert in a customer environment you manage?
- Q2 Is certificate lifecycle management explicitly in or out of scope in your current MSA template?
- Q3 How do you currently get visibility into cert expiry across all your customer environments?
- Q4 What does an unplanned outage cost you in labour and SLA exposure on your largest customer?

DigiCert solution:

✓ **Multi-tenant MSP Hub:** single control plane across all customer environments with per-customer dashboards and alerting

✓ **Expiry alerting and reporting** delivers proactive alerts via Slack, webhooks, ServiceNow, and JIRA before any cert goes critical

✓ **Automated renewal workflows** eliminate the human dependency that causes missed renewals

✓ **Role-based access control (RBAC)** delegates cert management while maintaining MSP-level governance and visibility

✓ **Audit trails and compliance reporting** provides documentation that demonstrates proactive management to customers and auditors

Financial impact of inaction

45%

of enterprises experienced cert-related service downtime in the past year

DigiCert Trust Pulse, July 2025

$2.8M

saved in security incident costs over 3 years, per DigiCert ONE customer

Forrester TEI Study, 2025

MSP differentiator

Position DigiCert Trust Lifecycle Manager as the customer's liability shield. It's the solution that eliminates outage risk from their managed service contracts before customers know to ask for it. Proactively expanding scope to include CLM is a defensive move that protects margin and locks in renewal.

What to say

"You may not think cert management is your problem until your customer calls you at 2am. We've seen MSPs lose contracts over a single cert expiry. DigiCert Trust Lifecycle Manager means that call never happens, and you can prove proactive management in your next QBR."

05 Compliance and audit exposure: certs are now a board-level risk

SOC 2, ISO 27001, HIPAA, PCI-DSS, and EU DORA all require demonstrable certificate controls. Most organizations can't produce them.

The problem

> *"Our auditor asked us to produce a complete certificate inventory last quarter. We couldn't."*
>
> CISO

Regulatory frameworks, including SOC 2 Type II, ISO 27001, HIPAA, PCI-DSS, and EU DORA, all require that organizations demonstrate comprehensive certificate inventory and lifecycle controls. Cyber insurers are increasingly asking for certificate management evidence during underwriting.

Organizations that cannot produce a complete, current certificate inventory fail audits, receive compliance findings, face higher insurance premiums, or lose coverage entirely.

✗ **Failed audits:** average of 5 failed audits per 2 years among orgs without dedicated CLM tools

✗ **Cyber insurance** underwriters now require certificate management evidence, and gaps increase premiums

✗ **EU DORA** explicitly requires PKI controls for financial services organizations

✗ **Weak key and deprecated algorithm risk:** certs using outdated SHA-1 or 1024-bit RSA are audit findings waiting to happen

Discovery questions

- Q1 Has your organization had a compliance finding related to certificates or PKI in the past 2 years?
- Q2 Can you produce a complete certificate inventory on demand for an auditor today?
- Q3 Is your cyber insurer asking questions about certificate management as part of renewal underwriting?
- Q4 Are you subject to EU DORA, PCI-DSS, or HIPAA? Do you have documented PKI controls?

DigiCert solution:

✓ **Policy enforcement engine** eliminates weak keys, deprecated algorithms, and unauthorized CAs automatically

✓ **Audit-ready reporting** delivers on-demand inventory reports showing all certificates, compliance status, and renewal history

✓ **Compliance controls mapping** offers governance capabilities that map directly to SOC 2, ISO 27001, PCI-DSS, and EU DORA

✓ **Cryptographic inventory** provides complete details on all TLS algorithms running across the entire estate for PQC readiness

✓ **Ownership and delegation workflows:** assign certificate ownership by business unit with full accountability trails

Compliance value

62%
of CISOs rank regulatory compliance as a top cert management concern
DigiCert Trust Pulse, July 2025

$1.1M
average annual financial impact of non-compliance and audit failures
DigiCert State of Digital Trust Report

MSP differentiator

Package DigiCert Trust Lifecycle Manager as a Compliance Readiness Service. The inventory report, policy enforcement, and audit trail documentation are exactly what auditors ask for. This is something your MSP can deliver at a recurring managed service price point, not a one-time consulting fee.

What to say

Your auditor is going to ask for a certificate inventory, and your cyber insurer already is. We can make your next audit faster and your renewal cheaper. That's not a security sale, that's a CFO conversation."

06 Post-Quantum Cryptography: the migration clock is running now

Harvest now, decrypt later" attacks are live. Organizations that don't know their cryptographic posture can't fix it.

The problem

> *"Quantum computing is years away. We'll deal with PQC when it matters."*
>
> CISO who hasn't heard of harvest-now-decrypt-later

NIST finalized its first post-quantum cryptography standards in August 2024. The US government has mandated that federal agencies begin PQC migration planning. Threat actors are already conducting "harvest now, decrypt later" attacks.

Organizations that don't know which cryptographic algorithms they're running across their certificate estate cannot assess their exposure, let alone remediate it. Crypto-agility requires a complete, governed certificate inventory as a non-negotiable prerequisite.

✗ **80% of organizations** are concerned about their ability to adapt to cryptographic changes—up from 48% in 2023

✗ **Only 23% of organizations** have started PQC readiness work, despite the finalizing of NIST standards

✗ **Organizations running RSA and ECC-based certs at** scale face complete re-issuance as algorithms are deprecated

✗ **Legacy PKI configurations** will be broken by quantum-safe algorithm migration if not inventoried and governed now

Discovery questions

- Q1 Do you know which cryptographic algorithms are running across all your certificates right now?
- Q2 Has your organization started a PQC readiness assessment? If so, what did the cryptographic inventory look like?
- Q3 Are you aware that migrating to PQC requires knowing every cert and its algorithm before you can swap anything?
- Q4 Is quantum readiness on your security roadmap, and if so, when does it become a board-level conversation?

DigiCert solution:

✓ **Cryptographic inventory:** Trust Lifecycle Manager tracks the algorithm, key length, and cipher suite of every certificate for PQC migration planning

✓ **PQC migration support in Trust Lifecycle Manager Premium** enables migration from RSA/ECC to NIST-standardized quantum-resistant algorithms

✓ **Production-ready PQC certificate management:** DigiCert was the first to market at enterprise scale, launching February 2026

✓ **Crypto-agile architecture** with DigiCert's integrated policy engine allows algorithm-level changes to propagate across the entire estate without manual intervention

✓ **Quantum-safe Private CA** offers PQC certificate issuance from DigiCert's Private CA infrastructure, backed by 7 global PKI facilities

Market urgency

69%

of enterprise recognize quantum computers will break current encryption within 5 years

DigiCert Quantum Pulse Survey

5%

of orgs have implemented quantum-safe encryption

DigiCert Quantum Pulse Survey

MSP differentiator

PQC Readiness is a named, priced engagement your MSP can sell today. The deliverable is a cryptographic posture report, showing which algorithms are running and which certs are at risk, along with a phased migration plan. This positions your MSP as a strategic security advisor, not a ticket-taker.

What to say

PQC migration starts with knowing what you have. If you can't produce a complete cryptographic inventory today, you can't start. We can give you that inventory and a roadmap to get quantum-ready before your competitors and your customers' auditors demand it."

Financial proof points

62%

Unplanned outages

Occurred causing severe application downtime due to unmanaged certificates

DigiCert & Ponemon Financial Services Report

5 - 24 hrs

Manual recovery time

Average hours required for IT staff to manually isolate, replace, and fix a certificate failure without automated CLM tools

DigiCert State of PKI Automation

$250K+

Financial loss per incident

18.5% of orgs lost over $250K. 31% lost $50K–$250K. Over half endured 5–24 hrs of downtime per incident.

DigiCert Trust Pulse Survey July 2025

312%

ROI on DigiCert ONE

over 3 years with payback under 6 months, based on interviews with 5 enterprise DigiCert ONE customers

Forrester Total Economic Impact™ Study, DigiCert 2025

$7.9M

Labour cost savings

over 3 years per enterprise from eliminating manual certificate management workflows

Forrester Total Economic Impact™ Study, DigiCert 2025

$1.3M

New revenue generated

by DigiCert ONE customers from meeting customer and partner security requirements they couldn't satisfy before

Forrester Total Economic Impact™ Study, DigiCert 2025

Scenario	Annual cost	Risk exposure	MSP outcome
Manual renewal today Spreadsheet tracking, human-managed, calendar reminders	~$250–$750/cert rotation x 4–8x/yr at 47 days	High: any missed renewal = outage + SLA breach	Labour-heavy, not scalable, liability accumulates
DigiCert TLM Advanced Automated CLM, full inventory, ACME/EST/SCEP automation	From $16.87/seat/yr at partner pricing	Low: automated alerts, zero-touch renewal	Margin expansion delivers more for less labor
DigiCert TLM Premium + Branded Private CA Full CLM + MSP as the CA + white-label portal + PQC	From $25.30/seat/yr (Private CA optional add-on)	Minimal: proactive governance + PQC-ready	New revenue stream PKI-as-a-Service practice

Objection Handling

"We already use Let's Encrypt. It's free, so why pay for cert management?"

The certificate is free. The management is never free. Each Let's Encrypt cert requires renewal every 90 days, and at 47-day mandates on public TLS, that frequency only increases. At 1–2 hours of labour per renewal, the hidden cost is substantial. **DigiCert Trust Lifecycle Manager manages Let's Encrypt-issued certs** automatically, so your team captures the savings without giving up the free issuance.

Show the 47-day renewal math:
100 certs x 8 renewals x 1.5 hrs = 1,200 hrs/yr of labour

"We have Microsoft ADCS. That handles our internal PKI."

ADCS handles issuance inside your Windows environment. It doesn't give you visibility across non-Windows systems, cloud workloads, containers, or third-party CAs. It has no centralized dashboard, no automated renewal for non-Windows endpoints, and no audit trail your compliance team can use. **DigiCert Trust Lifecycle Manager overlays ADCS** you keep the existing infrastructure and gain the governance layer on top.

Ask: Can you produce a complete cert inventory from ADCS for an auditor today?

"We've never had a certificate outage. This doesn't seem urgent."

86% of organizations experienced at least one cert-related outage in the past year. As cert renewal frequency increases 4–8x under the 47-day mandate, the probability of a missed renewal in any 12-month period climbs sharply. **The urgency isn't what's happened. It's what the math says is coming.**

"One in three organizations has this happen quarterly. What's your plan when it's your turn?"

"We don't have budget for another security tool."

The budget already exists, it's simply an expenditure buried in your team's labour costs. At an average of 5+ hours and 8 staff members per cert incident, plus $50K–$250K in financial exposure per outage, the question isn't whether you can afford DigiCert Trust Lifecycle Manager. It's whether you can afford not to have it. Forrester **found 312% ROI with a payback period under 6 months.**

Pull the Forrester TEI study. Ask: "What does one outage cost you in labour and SLA exposure?"

"PQC is years away. We'll deal with it when it matters."

NIST finalized PQC standards in August 2024. The US government has mandated federal agency migration planning. But the most immediate issue is practical: **you can't start PQC migration without a complete cryptographic inventory**. Every month you wait is a month further from being ready when regulators and customers demand proof.

Ask: "The migration itself takes 18–36 months for a large estate. When do you want to start the clock?"

"Can't we just set calendar reminders and automate with scripts?"

Scripts and calendar reminders are how you get the 2am call. They only track certs you know about, they break when someone leaves the team, and they don't scale to 47-day lifetimes.

The DigiCert State of PKI Automation report found that 47% of enterprise IT practitioners frequently discover rogue certs deployed entirely without their knowledge. **Manual processes and siloed tools have blind spots that the 47-day mandate will painfully expose.**

Ask: "How does your script handle a cert that was issued by a shadow CA you don't know about?"

Quick reference MSP plays

Door-opener: The PKI Health Check

Target
Any enterprise with 500+ employees and mixed IT infrastructure

Pitch
We'll show you every certificate in your environment in 5 days. You own the report."

Tool
DigiCert Trust Lifecycle Manager discovery deployment time-boxed, billable assessment

Outcome
Inventory report + risk scoring + natural path to managed CLM contract

Expansion play: From TLS to Private PKI

Target
Existing customers who manage external certs but have no internal PKI visibility

Pitch
"You know us for TLS. Here's what we've found below the proverbial certificate iceberg."

Tool
Trust Lifecycle Manager discovery scan of internal infrastructure shows the iceberg to the CIO

Outcome
Trust Lifecycle Manager Advanced or Premium contract + internal PKI governance retainer

Premium play: MSP Branded Private CA

Target
Enterprise customers with complex internal PKI who want branded certificate governance

Pitch
"Your certificates, your brand, your SLAs backed by DigiCert's global PKI infrastructure."

Tool
DigiCert MSP Hub + Branded Private CA + Trust Lifecycle Manager Premium

Outcome
Highest-margin managed service MSP becomes the CA, not the middleman

Strategic play: PQC readiness practice

Target
CISOs and security-focused buyers at regulated enterprises

Pitch
"PQC migration starts with knowing your cryptographic posture. We can give you that today."

Tool
Trust Lifecycle Manager Premium cryptographic inventory + DigiCert PQC cert management (GA Feb 2026)

Outcome
Executive-level advisory relationship + multi-year migration engagement

Quantum, AI, and PKI Sprawl permanently derailed manual certificate management

Every day without a managed CLM practice is a day your customers' certificates grow more complex, more fragile, and more expensive to fix. The MSPs who build this practice now will own it. The ones who wait will lose the conversation to a system integrator.

1. **Book a PKI Assessment for your top 3 enterprise customers this quarter**
2. **Stand up your MSP Hub and Internal PKI environment demo-ready in days**
3. **Establish your Branded Private CA intermediate + root cert under your name**
4. **Launch your PQC Readiness Practice (51% of CISOs already have budget for it)**

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.