



SECURETRON INC.

**NextGen Certificate Management
for Managed Service Providers**

How MSPs Can Transform PKI into a Scalable, Automated Revenue Stream
with Securetron PKI Trust Manager

A Securetron Inc. Whitepaper | April 2026

CONFIDENTIAL

Table of Contents

Contents

- Table of Contents 2
- 1. Executive Summary 4
- 2. The Certificate Crisis: Why the Status Quo Is Broken 6
 - 2.1 The Lifespan Reduction Timeline 6
 - 2.2 The Current State of Certificate Management Is Already Failing 7
 - 2.3 Why Manual Management Cannot Scale 7
- 3. The MSP Opportunity: PKI as a Managed Service 9
 - 3.1 A Rapidly Growing Market 9
 - 3.2 Why MSPs Are the Natural Delivery Vehicle 9
 - 3.3 Certificate Management as Recurring Revenue 10
 - 3.4 Differentiation Through Proactive Governance 11
- 4. Introducing Securetron PKI Trust Manager 12
 - 4.1 Three Simple Steps to Get Started 12
 - 4.2 Single Pane of Glass 13
 - 4.3 Broad Integration Ecosystem 13
 - Certificate Authority Integrations 13
 - Protocol Support 14
 - 4.4 Use Cases Across the Enterprise 14
 - 4.5 Free Community Edition 15
- 5. Architecture & Multi-Tenancy for MSPs 16
 - 5.1 Architecture Overview 16
 - 5.2 Multi-Tenancy: Built for MSPs 17
 - 5.3 Role-Based Access Control (RBAC) 17
 - 5.4 Audit Trail & Compliance 18
 - 5.5 HSM Integration 18
 - 5.6 Deployment Flexibility 18
- 6. Key Capabilities Deep Dive 19

6.1 Smart Certificate Discovery	19
6.2 Automated Certificate Lifecycle Management	20
6.3 Proactive Expiry Notification & Alerting	20
6.4 Bulk Operations & Templates	21
6.5 Comprehensive Reporting & Compliance	22
7. MSP-Specific Benefits	23
7.1 Operational Efficiency	23
7.2 Revenue Generation	24
7.3 Client Retention	24
7.4 Scalability	25
7.5 Training and Cross-Team Enablement	25
8. Deployment Models for MSPs	27
9. Future-Proofing: Post-Quantum Cryptography Readiness	29
9.1 The Quantum Computing Threat	29
9.2 NIST Post-Quantum Standards	30
9.3 Crypto-Agility: The Essential Capability	30
9.4 The MSP Advisory Opportunity	31
10. Getting Started with Securetron	32
11. About Securetron Inc.	33

1. Executive Summary

The digital certificate landscape is undergoing a seismic transformation. With the CA/Browser Forum's approval of **Ballot SC-081v3** in April 2025, the maximum lifespan of TLS certificates will plummet from 398 days to just **47 days by March 2029**. This single policy change will fundamentally reshape how organizations manage their cryptographic infrastructure and create an unprecedented opportunity for Managed Service Providers (MSPs) prepared to meet the challenge.

The scale of the problem is staggering. The average enterprise today manages over **3,700 TLS certificates**, a number expected to exceed 5,000 in the near term. Under the new 47-day maximum lifespan, organizations will face **12 times more renewal cycles** annually than they do today. Manual certificate management already a leading cause of outages and security incidents will become operationally impossible at scale.

Market Opportunity

The global PKI market is projected to reach **\$22.99 billion by 2031**, growing at a 20.76% CAGR. The managed PKI services segment alone was valued at \$4.8 billion in 2025 and is expected to reach \$14.2 billion by 2034. MSPs that invest in certificate management capabilities today are positioning themselves at the center of a rapidly expanding market.

MSPs are uniquely positioned to capture this growing market. Operating at the intersection of automation expertise and multi-client operations, MSPs can transform certificate lifecycle management from a reactive, break-fix expense into a **proactive, recurring revenue stream**. However, seizing this opportunity requires the right platform one purpose-built for the demands of multi-tenant certificate management at scale.

Securetron PKI Trust Manager is that platform. Designed from the ground up to enable MSPs to deliver **Certificate Lifecycle Management (CLM) as a managed service**, it provides the multi-tenancy,

automation, and single-pane-of-glass visibility that MSPs need to onboard clients rapidly, manage certificates across diverse environments, and demonstrate continuous compliance all while building a differentiated, high-margin service offering.

This whitepaper explores the forces driving the certificate management crisis, quantifies the opportunity for MSPs, and demonstrates how Securetron PKI Trust Manager provides the foundation for building a scalable, profitable PKI practice.

2. The Certificate Crisis: Why the Status Quo Is Broken

For years, the industry has been on a trajectory toward shorter certificate lifespans. What began as a gradual compression from five-year certificates to three, then two, then one has now accelerated into a mandate that will reshape enterprise operations. The CA/Browser Forum's Ballot SC-081v3, approved with broad industry support in April 2025, establishes a clear and aggressive timeline for reducing the maximum lifespan of TLS certificates.

2.1 The Lifespan Reduction Timeline

The phase-down is structured in three stages, each one dramatically increasing the operational burden on organizations that depend on TLS certificates to secure their infrastructure:

⚠ Critical Timeline: TLS Certificate Lifespan Reduction			
Enforcement Date	Maximum Lifespan	DCV Reuse Period	Impact
March 15, 2026	200 days	200 days	~2x more renewals than today
March 15, 2027	100 days	100 days	~4x more renewals
March 15, 2029	47 days	10 days	~12x more renewals

The implications extend beyond certificate renewal itself. **Domain Control Validation (DCV) reuse** — the process by which Certificate Authorities verify domain ownership will shrink to just **10 days by March 2029**. This means organizations will need to re-validate domain ownership almost continuously, adding another layer of operational complexity that manual processes simply cannot absorb.

2.2 The Current State of Certificate Management Is Already Failing

Even under today's comparatively lenient 398-day maximum, organizations are struggling. The data paints a stark picture of an industry already in crisis:

- **72% of organizations** experienced at least one certificate-related outage in the past year
- **67% of organizations** experience certificate-related outages on a monthly basis
- **45% of organizations** report weekly disruptions tied to expired or misconfigured certificates
- The average enterprise manages **3,730+ TLS certificates**, with that number expected to grow to over 5,000 as organizations expand cloud, IoT, and microservices deployments

Each of these outages carries real consequences: service disruptions, lost revenue, damaged customer trust, and in regulated industries, potential compliance violations. When a certificate expires unexpectedly on a production load balancer or API gateway, the result is often a cascading failure that takes hours or days to fully resolve.

2.3 Why Manual Management Cannot Scale

The root cause of these failures is clear: the vast majority of organizations still rely on spreadsheets, calendar reminders, and ad-hoc manual processes to track and renew their certificates. This approach was barely adequate when certificates lasted for years. Under the new regime of 47-day lifespans, it becomes mathematically impossible.

Consider an enterprise managing 4,000 certificates with a 47-day lifespan. That organization will need to process approximately **31,000 renewal operations per year** roughly 85 renewals per day, every day, with zero margin for error. A single missed renewal can take down a customer-facing application, a VPN gateway, or an API integration.

The Skills Gap Compounds the Problem

PKI and cryptographic operations require specialized expertise that is in short supply. A 2025 (ISC)² Cybersecurity Workforce Study found that the global cybersecurity workforce gap exceeded 4 million professionals. Organizations without dedicated PKI engineers which includes the vast majority of mid-market and SMB enterprises face an impossible choice: invest in scarce, expensive in-house talent, or accept the risk of unmanaged certificates. This is precisely where MSPs can step in with the right tooling and expertise.

The convergence of shorter lifespans, increasing certificate volumes, expanding attack surfaces, and a persistent skills gap creates a clear inflection point. The status quo is not just suboptimal it is broken. Organizations need a new model for certificate management, and MSPs are the natural delivery vehicle for that model.

3. The MSP Opportunity: PKI as a Managed Service

The certificate management crisis described in the previous section is not merely a problem to be solved — it is a market opportunity of significant scale and durability. For MSPs already trusted to manage their clients' IT infrastructure, security posture, and compliance obligations, **certificate lifecycle management represents a natural and highly strategic service expansion.**

3.1 A Rapidly Growing Market

The numbers tell a compelling story. The **managed PKI services market** was valued at approximately **\$4.8 billion in 2025** and is projected to reach **\$14.2 billion by 2034**, representing a compound annual growth rate (CAGR) of 12.8%. This growth is being driven by the same forces creating the certificate crisis: shorter lifespans, expanding digital footprints, and increasingly stringent regulatory requirements.

Revenue Potential at a Glance

Managed PKI Services Market (2025): \$4.8 billion

Projected Market Size (2034): \$14.2 billion

CAGR: 12.8%

Global PKI Market (2031): \$22.99 billion (20.76% CAGR)

3.2 Why MSPs Are the Natural Delivery Vehicle

MSPs operate at the intersection of three capabilities that make them ideally suited to deliver managed PKI services:

- **Automation expertise:** MSPs already build and maintain automated workflows for patching, monitoring, backup, and endpoint management. Extending this operational model to certificate lifecycle management is a natural fit.
- **Multi-client operations:** MSPs are structured to manage dozens or hundreds of client environments simultaneously. The tooling, processes, and team structures are already in place to deliver multi-tenant services efficiently.
- **Trusted advisor relationships:** MSPs serve as the de facto IT department for many organizations. Clients already trust their MSP to manage critical infrastructure — certificate management is a logical extension of that trust.

As the CA/Browser Forum's lifespan reductions take effect, enterprise CISOs and IT directors will increasingly look to their MSPs for guidance and execution. MSSPs and MSPs will own the day-to-day execution of certificate management: monitoring automation health, validating renewal outcomes, managing exceptions and escalations, and providing governance oversight.

3.3 Certificate Management as Recurring Revenue

From a business model perspective, managed certificate services exhibit the characteristics MSPs value most:

- **Predictable recurring revenue:** Certificate management is an ongoing operational requirement, not a one-time project. Monthly or annual service agreements provide stable, forecastable revenue.
- **High retention:** Once an MSP is managing a client's certificate infrastructure, switching costs are significant. The service becomes deeply embedded in the client's operational fabric.
- **Scalability:** With the right platform, the marginal cost of adding a new client is low, creating strong unit economics at scale.
- **Upsell potential:** Certificate management serves as a gateway to broader security services including compliance reporting, vulnerability management, and security posture assessments.

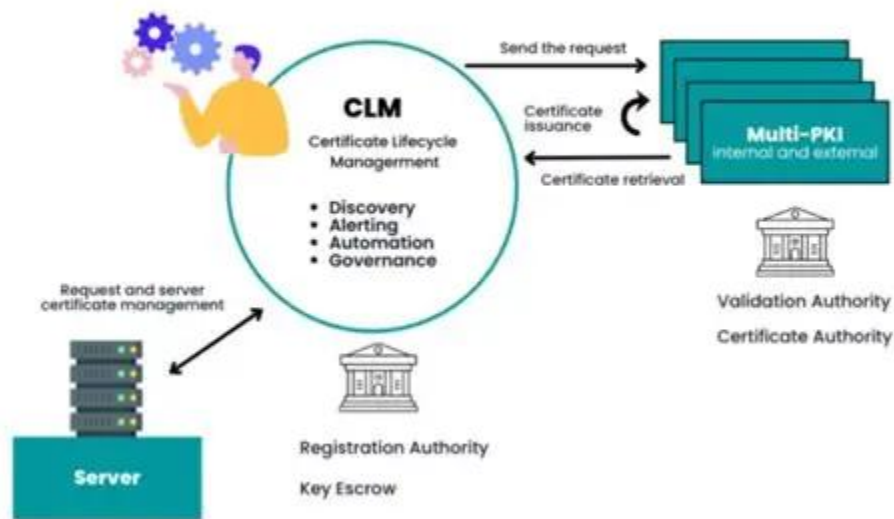
3.4 Differentiation Through Proactive Governance

The MSPs that will capture the greatest share of this market are those that move beyond reactive break-fix and position themselves as **proactive certificate governance partners**. This means not just renewing certificates when they are about to expire, but providing continuous visibility into certificate health, enforcing policy compliance across client environments, and delivering compliance-as-a-service aligned with frameworks such as **GDPR, HIPAA, PCI DSS, and SOC 2**.

The industry's shift from capital expenditure (capex) models to operational expenditure (opex) models further favors MSP delivery. Organizations increasingly prefer to consume security capabilities as a managed service rather than building and maintaining in-house teams and infrastructure. Certificate management is no exception.

4. Introducing Securetron PKI Trust Manager

Securetron PKI Trust Manager is a comprehensive, enterprise-ready PKI management solution designed to simplify certificate lifecycle management, enhance security posture, and streamline cryptographic operations across complex, multi-environment deployments. Purpose-built for the demands of modern MSP operations, it delivers the automation, visibility, and multi-tenancy that service providers need to offer certificate management as a scalable managed service.



Comprehensive certificate lifecycle management from discovery to automation to compliance reporting.

4.1 Three Simple Steps to Get Started

Securetron PKI Trust Manager is designed for rapid deployment and immediate value realization.

Whether an MSP is onboarding its first client or its hundredth, the path to production is straightforward:

Step	Action	Description
1	Deploy	Choose your deployment model — on-premises, Azure Cloud, Docker, or SaaS — and provision the platform in minutes to days depending on environment complexity.
2	Gain Visibility	Discover and inventory every certificate across client environments. Identify expired, expiring, misconfigured, and shadow certificates with automated scanning.
3	Gain Control	Automate certificate issuance, renewal, and revocation. Establish policies, configure notifications, and deliver ongoing governance through a unified dashboard.

4.2 Single Pane of Glass

At the heart of Securetron PKI Trust Manager is a **unified management portal** that provides a single pane of glass across all certificate authorities, all protocols, and all client environments. MSPs no longer need to log into multiple CA portals, maintain separate tracking systems, or reconcile data across disconnected tools. Every certificate — regardless of issuing CA or deployment location — is visible, manageable, and reportable from one interface.

4.3 Broad Integration Ecosystem

Securetron PKI Trust Manager integrates with the certificate authorities and infrastructure platforms that MSPs and their clients already use:

Certificate Authority Integrations

- **Active Directory Certificate Services (ADCS/MSCA)** — the most widely deployed enterprise CA
- **Let's Encrypt** — automated, free DV certificates for web-facing services
- **DigiCert** — enterprise-grade OV and EV certificates
- **ACME-compatible CAs** — any CA supporting the ACME protocol
- Extensible connector framework for additional CA integrations

Protocol Support

- **SCEP** (Simple Certificate Enrollment Protocol) — for MDM and network device enrollment
- **EST** (Enrollment over Secure Transport) — modern, TLS-secured enrollment
- **ACME** (Automated Certificate Management Environment) — automated DV certificate lifecycle
- **RESTful API** — programmatic access for custom integrations and automation workflows

4.4 Use Cases Across the Enterprise

Securetron PKI Trust Manager addresses the full spectrum of certificate management requirements that MSPs encounter across their client base:

Use Case	Capabilities
Certificate Discovery	Network scanning, endpoint inspection, cloud workload enumeration, shadow certificate detection
Certificate Automation	Automated issuance, renewal, and revocation with policy-driven workflows
Certificate Notification	Configurable expiry alerts, escalation paths, and dashboard-driven health monitoring
MDM Integration	Microsoft Intune integration, SCEP for mobile device certificate provisioning
Kubernetes & Cloud-Native	Certificate management for containerized workloads and cloud-native architectures
Network Access Control	EAP-TLS, 802.1X wireless authentication, NAC integration
Code Signing	Secure code signing certificate management and workflow enforcement
S/MIME & Email Security	Email encryption and digital signature certificate management
Smart Credentials	Smartcard, PIV, Virtual Smartcard, YubiKey, and Windows Hello for Business

4.5 Free Community Edition

Start for Free — No Risk, No Commitment

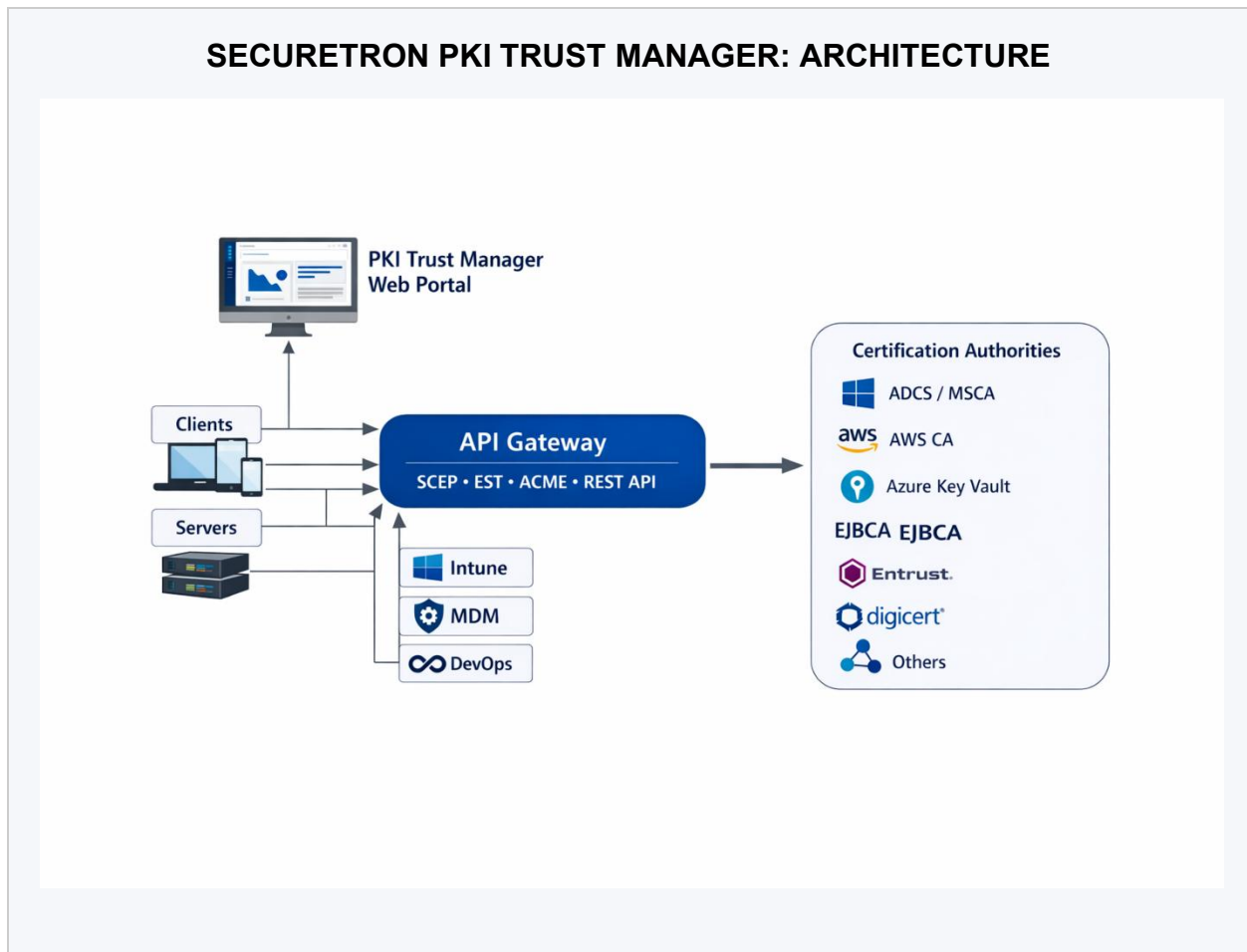
The **Securetron PKI Trust Manager Community Edition** supports management of up to **500 certificates at no cost**. This makes it ideal for MSPs looking to build a proof-of-concept, demonstrate value to prospective clients, or onboard smaller accounts before scaling to an enterprise license. The Community Edition includes the full management portal, certificate discovery, and core automation capabilities.

5. Architecture & Multi-Tenancy for MSPs

Securetron PKI Trust Manager is built on a modern, modular architecture designed for the operational realities of managed service delivery. Every architectural decision — from the microservices foundation to the role-based access model reflects the requirements of MSPs managing diverse client portfolios at scale.

5.1 Architecture Overview

The platform follows a layered microservices architecture that separates concerns cleanly and enables independent scaling of each component:



5.2 Multi-Tenancy: Built for MSPs

Multi-tenancy is not an afterthought in Securetron PKI Trust Manager, it is a foundational design principle. Each client environment operates as an **isolated tenant** with complete separation of data, configurations, policies, and audit logs. This isolation ensures that:

- **Client data is never commingled.** Certificate inventories, configurations, and audit trails are strictly partitioned between tenants.
- **Policies are tenant-specific.** Each client can have unique certificate policies, notification thresholds, and approval workflows without affecting other tenants.
- **Onboarding is rapid.** New tenants can be provisioned in minutes, with pre-configured templates accelerating time-to-value.
- **Compliance is simplified.** Per-tenant audit logs and reporting make it straightforward to demonstrate compliance to individual clients and their auditors.

5.3 Role-Based Access Control (RBAC)

Securetron provides granular **Role-Based Access Control** that maps naturally to MSP organizational structures. Permissions can be assigned at multiple levels:

Role Level	Typical Assignment	Permissions
Global Administrator	MSP Principal / Security Director	Full platform access, tenant provisioning, global configuration
Tenant Administrator	Client Account Manager	Full access within assigned tenant(s), policy management, reporting
Operator	NOC / SOC Engineer	Certificate operations, monitoring, incident response within assigned tenants
Read-Only Auditor	Client Compliance Team	View-only access to certificate inventory, audit logs, and compliance reports

5.4 Audit Trail & Compliance

Every action within the platform is logged with a **complete, immutable audit trail**. Certificate issuances, renewals, revocations, policy changes, user logins, and configuration modifications are all recorded with timestamps, user identity, and contextual details. These logs are indispensable for compliance reporting and incident investigation, providing the evidentiary foundation that auditors require.

5.5 HSM Integration

For high-assurance deployments particularly in regulated industries such as financial services, healthcare, and government; Securetron PKI Trust Manager supports integration with **Hardware Security Modules (HSMs)**. HSMs provide tamper-resistant key storage and cryptographic operations, ensuring that private keys never exist in software and are protected to the highest industry standards.

5.6 Deployment Flexibility

Securetron PKI Trust Manager can be deployed in the model that best fits each MSP's operational strategy and client requirements. Whether running on-premises for maximum control, in Azure Cloud for elastic scalability, in Docker containers for DevOps-oriented workflows, or as a fully managed SaaS offering, the platform delivers consistent functionality across all deployment models.

6. Key Capabilities Deep Dive

Securetron PKI Trust Manager provides an integrated suite of capabilities that address every stage of the certificate lifecycle. Each capability is designed with MSP operations in mind enabling service providers to deliver consistent, efficient, and auditable certificate management across their entire client portfolio.

6.1 Smart Certificate Discovery

You cannot manage what you cannot see. **Smart Certificate Discovery** provides MSPs with comprehensive visibility into every certificate across client environments including those that have been provisioned outside of standard processes and exist as "shadow" certificates unknown to IT teams.

- **Non-intrusive network scanning:** Discover certificates across networks, endpoints, and cloud workloads without impacting business operations or triggering security alerts.
- **Comprehensive coverage:** Scan IP ranges, DNS names, cloud platforms, load balancers, CDNs, and internal services to identify every certificate in the environment.
- **Shadow certificate detection:** Identify certificates issued by unauthorized CAs, self-signed certificates in production environments, and certificates provisioned through informal channels.
- **Risk scoring and categorization:** Automatically classify discovered certificates by risk level based on factors such as key strength, algorithm, expiry proximity, and issuing CA trust status.
- **Continuous monitoring:** Schedule recurring discovery scans to ensure that the certificate inventory remains accurate as environments evolve.

MSP Value

For MSPs, discovery is often the most powerful client engagement tool. Running a discovery scan against a prospective client's environment frequently reveals dozens of unknown, expired, or at-risk certificates providing immediate, tangible evidence of the value the MSP can deliver. Many

MSPs use the Community Edition's discovery capabilities as a free assessment tool to open new client conversations.

6.2 Automated Certificate Lifecycle Management

Automation is the core of Securetron PKI Trust Manager and the capability that transforms certificate management from an unsustainable manual burden into a scalable managed service.

- **Automated issuance:** Provision new certificates through policy-driven workflows that enforce organizational standards for key length, algorithm, subject naming, SAN configuration, and CA selection.
- **Scheduled renewal:** Certificates are automatically renewed before expiration based on configurable lead times, eliminating the risk of outages from expired certificates.
- **Automated revocation:** Revoke compromised or decommissioned certificates through controlled workflows that update CRL and OCSP responders.
- **CRL and OCSP management:** Comprehensive revocation infrastructure management ensures that certificate status information is always current and accessible.
- **Cross-environment support:** Automate certificate operations across on-premises infrastructure, cloud platforms, CDN providers, and container orchestration systems from a single workflow engine.

Under the new 47-day maximum lifespan regime, automation is not a nice-to-have rather it is an operational imperative. Securetron PKI Trust Manager's automation engine handles the high-volume, high-frequency renewal cycles that shorter lifespans demand, ensuring that MSPs can manage thousands of certificates across hundreds of clients without proportional increases in staffing.

6.3 Proactive Expiry Notification & Alerting

Even with comprehensive automation, visibility into certificate health is essential. Securetron's notification and alerting system ensures that MSP operators are always aware of certificate status across all managed environments.

- **Configurable notification thresholds:** Set multiple alert levels (e.g., 60 days, 30 days, 14 days, 7 days before expiry) with different notification channels and escalation paths for each.
- **Multi-channel alerting:** Deliver alerts via email, webhook integrations (Slack, Microsoft Teams), SIEM integration, and in-platform dashboard notifications.
- **Escalation paths:** Automatically escalate unresolved certificate issues from L1 operators to senior engineers to management based on time-to-expiry and risk severity.
- **Dashboard-driven visibility:** Real-time dashboards provide at-a-glance views of certificate health across all tenants, with drill-down capabilities for investigating specific issues.
- **Per-tenant and aggregate views:** MSP operators can monitor individual client environments or view aggregate certificate health across the entire portfolio.

6.4 Bulk Operations & Templates

MSPs managing large certificate estates need the ability to operate at scale. Securetron's bulk operations and template capabilities enable efficient management of high-volume certificate environments.

- **Mass certificate issuance:** Issue hundreds or thousands of certificates in a single operation using pre-configured parameters and CSV-driven batch processing.
- **Certificate templates:** Create and maintain standardized certificate templates that enforce consistent configurations across client environments including key length, algorithm, validity period, and extension settings.
- **Template inheritance:** Define MSP-level templates that serve as baselines, with per-tenant overrides for client-specific requirements.

- **Standardized workflows:** Apply consistent certificate management workflows across all client environments, reducing training requirements and ensuring operational consistency.

6.5 Comprehensive Reporting & Compliance

Reporting is where MSPs demonstrate the ongoing value of their certificate management service.

Securetron provides a robust reporting framework that serves both operational and compliance needs.

- **Certificate inventory reports:** Complete, exportable inventories of all certificates across a tenant, including certificate details, issuing CA, expiry dates, deployment locations, and risk assessments.
- **Compliance-aligned reports:** Pre-built report templates aligned with common regulatory frameworks including GDPR, HIPAA, PCI DSS, and SOC 2, enabling MSPs to deliver compliance evidence as part of their service.
- **Audit trail reports:** Detailed records of all certificate operations, policy changes, and access events — formatted for auditor consumption.
- **Trend analysis:** Track certificate growth, renewal volumes, and operational metrics over time to support capacity planning and demonstrate service improvement.
- **Scheduled report generation:** Automate report generation and delivery on daily, weekly, monthly, or quarterly schedules to support client governance review cycles.

7. MSP-Specific Benefits

While Securetron PKI Trust Manager delivers value to any organization managing certificates, its architecture and feature set are specifically optimized for the MSP business model. The following value framework outlines how the platform translates into measurable business outcomes for service providers.

7.1 Operational Efficiency

Key Metric

Up to 90% Reduction in Manual Certificate Management Effort

- **Consolidated management:** A single dashboard replaces the multiple CA portals, spreadsheets, and monitoring tools that MSPs currently juggle across client environments. Operators manage certificates across all clients from one interface.
- **Automated workflows:** Certificate issuance, renewal, and revocation workflows execute automatically based on defined policies, eliminating the repetitive manual tasks that consume operator time and introduce human error.
- **Reduced Mean Time to Resolution (MTTR):** When certificate issues do arise, centralized visibility and automated diagnostics enable faster identification and resolution reducing the impact on client operations and the MSP's support burden.

- **Standardized operations:** Template-driven provisioning and consistent workflows across client environments reduce training requirements and ensure that any operator can effectively manage any client's certificate estate.

7.2 Revenue Generation

Securetron PKI Trust Manager enables MSPs to build a profitable, tiered certificate management service offering:

Service Tier	Included Capabilities	Target Client
Basic	Certificate discovery, inventory management, expiry alerting, monthly health reports	Small businesses, organizations beginning their PKI journey
Standard	All Basic capabilities + automated renewal, policy enforcement, multi-CA management, quarterly compliance reports	Mid-market organizations, regulated industries
Premium	All Standard capabilities + compliance-as-a-service reporting, crypto-agility advisory, PQC readiness assessment, dedicated account governance	Enterprise clients, financial services, healthcare, government

The **Community Edition** (free for up to 500 certificates) serves as a powerful onramp, allowing MSPs to demonstrate value with a free assessment before upselling to paid service tiers. This land-and-expand model minimizes client acquisition friction while building the foundation for long-term recurring revenue.

7.3 Client Retention

- **Proactive security posture:** Clients see measurable improvement in their certificate hygiene and security posture, reinforcing the MSP's value and justifying ongoing service fees.

- **Deep infrastructure integration:** Certificate management touches every layer of a client's infrastructure — web servers, load balancers, VPNs, APIs, email systems, mobile devices, and more. This deep integration creates natural switching costs that strengthen client retention.
- **Demonstrable value:** Compliance-ready reports, trend analyses, and risk reduction metrics provide clients with concrete evidence of the MSP's contribution to their security and compliance objectives.

7.4 Scalability

- **Rapid client onboarding:** Multi-tenant architecture and template-driven provisioning enable MSPs to onboard new clients in hours rather than weeks.
- **Linear scaling:** The platform's architecture supports growth from 10 clients to 10,000 clients without requiring fundamental changes to infrastructure, processes, or team structure.
- **Operational leverage:** Automation ensures that certificate management effort scales sublinearly with client count — adding clients increases revenue without proportional increases in operational cost.

7.5 Training and Cross-Team Enablement

Securetron goes beyond delivering software; We invest in the success of our MSP partners through comprehensive training and hands-on enablement programs. Securetron provides dedicated training to MSPs, ensuring their teams are fully equipped to deploy, manage, and optimize the PKI Trust Manager platform across diverse client environments.

Critically, Securetron helps bridge the gap between PKI services and the broader organizational teams that depend on certificate infrastructure. Infrastructure teams, application development groups, DevOps engineers, and platform engineering teams all rely on certificates to secure their workloads yet PKI is rarely their core competency. Securetron works alongside MSPs to engage these cross-functional

teams directly, facilitating the onboarding of their applications, services, and automation pipelines onto the PKI Trust Manager platform.

This collaborative onboarding approach delivers several strategic advantages:

- **Accelerated Adoption:** By engaging infrastructure, application, DevOps, and engineering teams early, Securetron eliminates the friction that typically delays PKI automation rollouts.
- **Deep Integration:** When certificate management is woven into CI/CD pipelines, container orchestration, endpoint management, and application deployment workflows, it becomes an indispensable part of the client's operational fabric.
- **Organizational Stickiness:** As more teams across the client organization depend on the PKI Trust Manager platform for their day-to-day operations, switching costs increase significantly ensuring that both the product and the MSP partner become deeply embedded within the client environment.
- **Reduced Support Burden:** Well-trained teams generate fewer support tickets and escalations, allowing MSPs to scale their client base without proportionally increasing support overhead.

The result is a partnership model where Securetron and the MSP operate as a unified enablement force, driving adoption across every team that touches certificates, from network engineers configuring EAP-TLS authentication to DevOps teams automating TLS for Kubernetes workloads. This ensures that the MSP's value proposition extends far beyond initial deployment, creating lasting, multi-departmental relationships that are resilient to competitive displacement.

8. Deployment Models for MSPs

Securetron PKI Trust Manager supports multiple deployment models, ensuring that MSPs can choose the architecture that best aligns with their operational strategy, client requirements, and regulatory obligations. Each deployment model delivers the full functionality of the platform while optimizing for different operational priorities.

Feature	On-Premises	Azure Cloud	Docker	SaaS
Control	Full	High	High	Managed
Setup Time	Days	Hours	Hours	Minutes
Scalability	Manual	Auto-scale	Container orchestration	Elastic
Maintenance	MSP-managed	Shared responsibility	MSP-managed	Securetron-managed
Data Residency	Full MSP control	Azure region selection	Full MSP control	Securetron-managed
HSM Support	Physical & network HSM	Azure Key Vault / HSM	Network HSM	Cloud HSM
Best For	Regulated industries, sovereign data requirements	Cloud-first MSPs, hybrid environments	DevOps-oriented MSPs, CI/CD integration	Rapid deployment, minimal infrastructure overhead

Deployment Recommendation for MSPs

Most MSPs entering the certificate management market benefit from starting with the **SaaS deployment** for rapid time-to-value, then evolving to Azure Cloud or on-premises deployments as their practice matures and client requirements demand additional control. The platform's consistent feature set across all deployment models ensures that this migration is seamless and does not disrupt existing client service delivery.

Regardless of deployment model, Securetron PKI Trust Manager provides full multi-tenancy, RBAC, audit logging, and integration capabilities. MSPs can also operate in a **hybrid mode**, running different deployment models for different client segments — for example, SaaS for standard clients and on-premises for clients in regulated industries with strict data sovereignty requirements.

9. Future-Proofing: Post-Quantum Cryptography Readiness

While the immediate challenge for MSPs is managing the transition to shorter certificate lifespans, a larger cryptographic transformation is on the horizon. The advent of cryptographically relevant quantum computers threatens to render current public-key algorithms including RSA and Elliptic Curve Cryptography (ECC) vulnerable to attack. MSPs that prepare their clients for this transition today will establish themselves as trusted advisors for years to come.



The post-quantum cryptography transition represents the next major inflection point in certificate management.

9.1 The Quantum Computing Threat

Quantum computers capable of running Shor's algorithm at scale will be able to break RSA and ECC in polynomial time effectively rendering the cryptographic foundation of today's PKI infrastructure obsolete. While the timeline for achieving this capability remains uncertain, the threat is acknowledged by every major government and standards body worldwide. The "harvest now, decrypt later" attack model means that adversaries are already collecting encrypted data today with the intention of decrypting it once quantum capabilities mature.

9.2 NIST Post-Quantum Standards

In August 2024, the U.S. National Institute of Standards and Technology (NIST) published its first three **post-quantum cryptography (PQC) standards**: ML-KEM (formerly CRYSTALS-Kyber) for key encapsulation, and ML-DSA (formerly CRYSTALS-Dilithium) and SLH-DSA (formerly SPHINCS+) for digital signatures. These standards establish the algorithmic foundation for the industry's transition to quantum-resistant cryptography.

9.3 Crypto-Agility: The Essential Capability

The transition to post-quantum algorithms will not happen overnight. Organizations will need to operate in a **hybrid cryptographic environment** supporting both classical and quantum-resistant algorithms simultaneously for an extended period. This requires **crypto-agility**: the ability to rapidly discover, inventory, and replace cryptographic assets as algorithmic standards evolve.

Securetron's PQC Commitment

Securetron is committed to supporting the industry's transition to quantum-resistant cryptography. The PKI Trust Manager platform is being designed with crypto-agility as a core principle ensuring that MSPs can:

- Inventory all cryptographic assets and identify algorithm dependencies across client environments
- Test and validate post-quantum certificate profiles in non-production environments
- Execute phased migrations from classical to quantum-resistant algorithms using automated workflows
- Support hybrid certificates that embed both classical and PQC algorithms during the transition period

9.4 The MSP Advisory Opportunity

Post-quantum readiness represents a significant advisory and services opportunity for MSPs. Most organizations lack the internal expertise to assess their quantum risk exposure, develop a migration strategy, and execute the transition. MSPs that build PQC readiness assessment and migration planning into their service offerings today will be positioned as indispensable partners when the transition accelerates.

Key advisory services MSPs can offer include:

- **Cryptographic inventory assessment:** Cataloging all cryptographic dependencies across client environments
 - **Quantum risk scoring:** Evaluating the sensitivity and longevity of data protected by current algorithms
 - **Migration roadmap development:** Creating phased plans for transitioning to PQC-compliant certificate infrastructure
 - **Compliance alignment:** Ensuring PQC migration plans align with evolving regulatory requirements and industry guidance
-

10. Getting Started with Securetron

The path from evaluating Securetron PKI Trust Manager to delivering certificate management as a managed service is designed to be as frictionless as possible. Whether you are an MSP exploring PKI services for the first time or an established provider looking to scale your existing practice, we have a clear pathway to get you started.

Step	Action	Details
1	Download the Free Community Edition	Manage up to 500 certificates at no cost. Experience the full management portal, certificate discovery, and core automation capabilities. Build a proof-of-concept and demonstrate value to prospective clients with zero financial risk.
2	Register for a Live Demo	See Securetron PKI Trust Manager in action. Our solutions engineers will walk you through multi-tenant management, automated certificate lifecycle workflows, and compliance reporting tailored to MSP operations. Register at securetron.net .
3	Explore MSP Partnership Opportunities	Contact the Securetron team to discuss MSP partnership programs, volume licensing, co-marketing opportunities, and white-label options. We are committed to helping MSPs build profitable, scalable PKI practices.

Contact Us

Web: [securetron.net](#)

Email: info@securetron.net

Securetron: Enabling the Next Generation of PKI

11. About Securetron Inc.

Securetron Inc. is a cybersecurity company headquartered in **Toronto, Canada**, specializing in Public Key Infrastructure (PKI) solutions for enterprises and managed service providers worldwide.

Founded with the mission to simplify enterprise PKI management and make certificate lifecycle management accessible, automated, and secure, Securetron has built the **PKI Trust Manager Suite**: A comprehensive platform trusted by organizations seeking to gain visibility into their certificate landscape, automate lifecycle operations, and align with evolving compliance and security standards.

Securetron's approach is rooted in the conviction that effective PKI management should not require an army of specialized engineers or a patchwork of disconnected tools. By delivering a unified, multi-tenant platform with enterprise-grade automation and compliance capabilities, Securetron enables organizations of all sizes and the MSPs that serve them to manage their cryptographic infrastructure with confidence.

Company Detail	Information
Headquarters	Toronto, Ontario, Canada
Focus Area	Public Key Infrastructure (PKI) & Certificate Lifecycle Management
Flagship Product	Securetron PKI Trust Manager Suite
Certifications	ISO 27001 Certified
Cloud Partnerships	Azure and AWS
Website	securetron.net

Securetron — Enabling the Next Generation of PKI



Disclaimer: This document is provided for informational purposes only and does not constitute a binding offer or commitment. Product features, capabilities, and roadmap items described herein are subject to change without notice. All trademarks, trade names, and product names referenced in this document are the property of their respective owners. Market data and projections cited are based on publicly available industry research and are provided for contextual reference only. Securetron Inc. makes no representations or warranties regarding the accuracy of third-party data.

© 2026 Securetron Inc. All rights reserved. | securetron.net | Document Classification: Confidential