DATASHEET

Cryptographic Security Platform

Certificate Manager

Turn certificate chaos into control with unified lifecycle, visibility, and automation.

The Challenge

Certificates are multiplying across modern enterprises – spanning cloud environments, applications, devices, and machine identities. At the same time, certificate lifetimes are shrinking, operational demands are increasing, and ownership remains fragmented across teams.

The result?

- Limited visibility into where certificates exist and who owns them
- Manual processes that increase the risk of outages and service disruption
- Siloed tools that cannot scale across hybrid and multi-cloud environments
- Growing complexity managing multiple public and private certificate authorities
- Increasing pressure to prepare for post-quantum cryptography (PQC)

As organizations move toward shorter certificate lifecycles and more dynamic infrastructure, traditional approaches to certificate management can't keep up.

The Solution

Entrust Certificate Manager, part of the Entrust Cryptographic Security Platform (CSP), centralizes certificate discovery, lifecycle automation, and policy-based governance – giving organizations the visibility and control needed to manage certificates at enterprise scale.

By unifying certificate lifecycle management within a broader cryptographic control plane, Entrust enables organizations to reduce operational complexity, minimize risk, and build a foundation for crypto-agility and post-quantum readiness.

Core Capabilities

Unified Discovery & Inventory
Gain complete visibility across your certificate landscape.

- Discover certificates across cloud, network, and on-premises environments
- Integrate with vulnerability scanners, vaults, and CA systems
- Continuously monitor certificate usage, ownership, and expiration
- Extend discovery to any system with custom discovery plugins

Lifecycle Automation at Scale
Eliminate manual processes and reduce operational risk.

- Automate certificate issuance, renewal, and revocation
- Integrate with web servers, load balancers, cloud platforms, and applications
- Reduce outages caused by expired or misconfigured certificates
- Extend automation workflows through flexible, policy-driven integrations
- Support for extensible automation via Ansible playbooks (roadmap)

Multi-CA Orchestration
Simplify and control certificate operations across multiple certificate authorities.

- Centralized management of public and private CAs
- Support for third-party CAs including Sectigo, DigiCert, GlobalSign, EJBCA, and more
- Streamline certificate requests and issuance across environments
- Prepare for ACME-based automation and expanded CA integrations

Centralized Visibility & Control
Move from fragmented insights to enterprise-wide control.

- Maintain a unified inventory of all certificates across the organization
- Track certificate ownership, status, and dependencies
- Identify risks such as unknown, expired, or misconfigured certificates
- Enable proactive management instead of reactive firefighting

Governance & Compliance

Strengthen security posture and meet regulatory requirements.

- Enforce policy-based certificate management across environments
- Support audit readiness with centralized reporting and controls
- Integrate with Entrust Compliance Manager for enhanced oversight
- Align certificate lifecycle processes with enterprise security policies

Platform Extensibility

Adapt to your environment – not the other way around.

- Build custom discovery plugins using any programming language
- Leverage Entrust-provided examples via public GitHub repositories
- Execute plugins securely using containerized runtime environments
- Integrate with any third-party system through APIs

Result: Organizations are no longer limited by pre-built integrations – certificate discovery and management can evolve alongside their infrastructure.

Post-Quantum Readiness

Prepare your certificate strategy for the future of cryptography.

- Integrates with Entrust PQ-ready PKI
- Supports crypto-agility initiatives across certificate environments
- Enables organizations to begin transitioning to quantum-safe architectures today

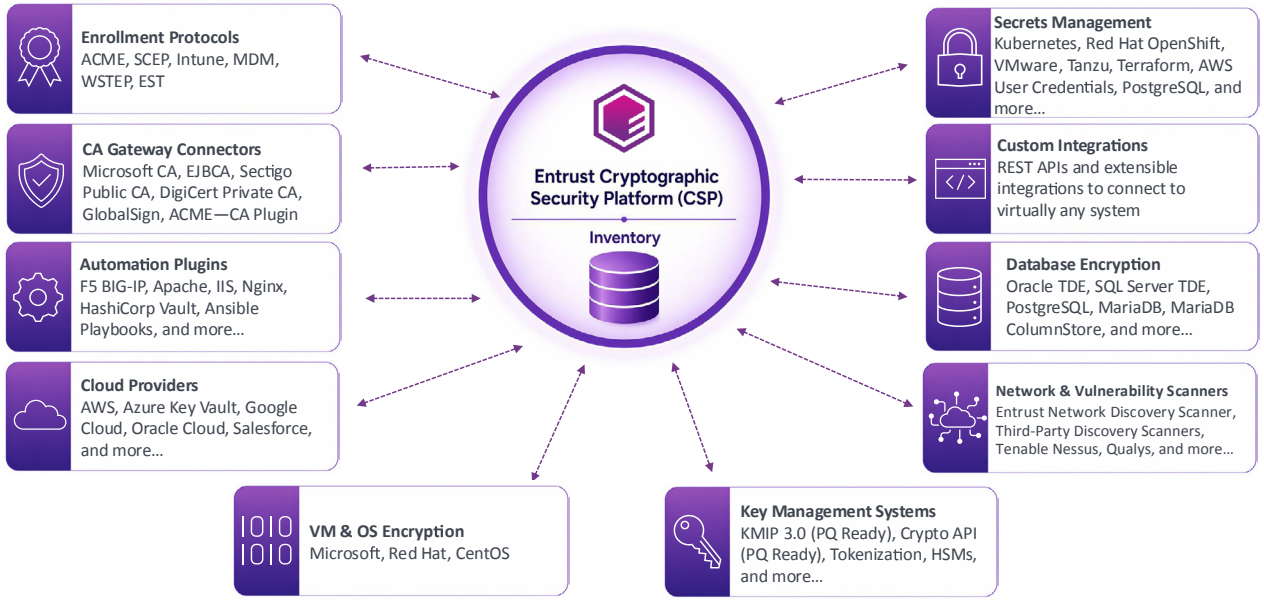
Business Value

Entrust Certificate Manager helps organizations:

- **Optimize operational efficiency** by automating certificate lifecycle processes
- **Reduce risk of outages and data loss** caused by expired or unmanaged certificates
- **Achieve compliance and audit readiness** through centralized visibility and control

Expanding Ecosystem of CSP Integrations

An extensible platform that connects to the tools and systems you rely on



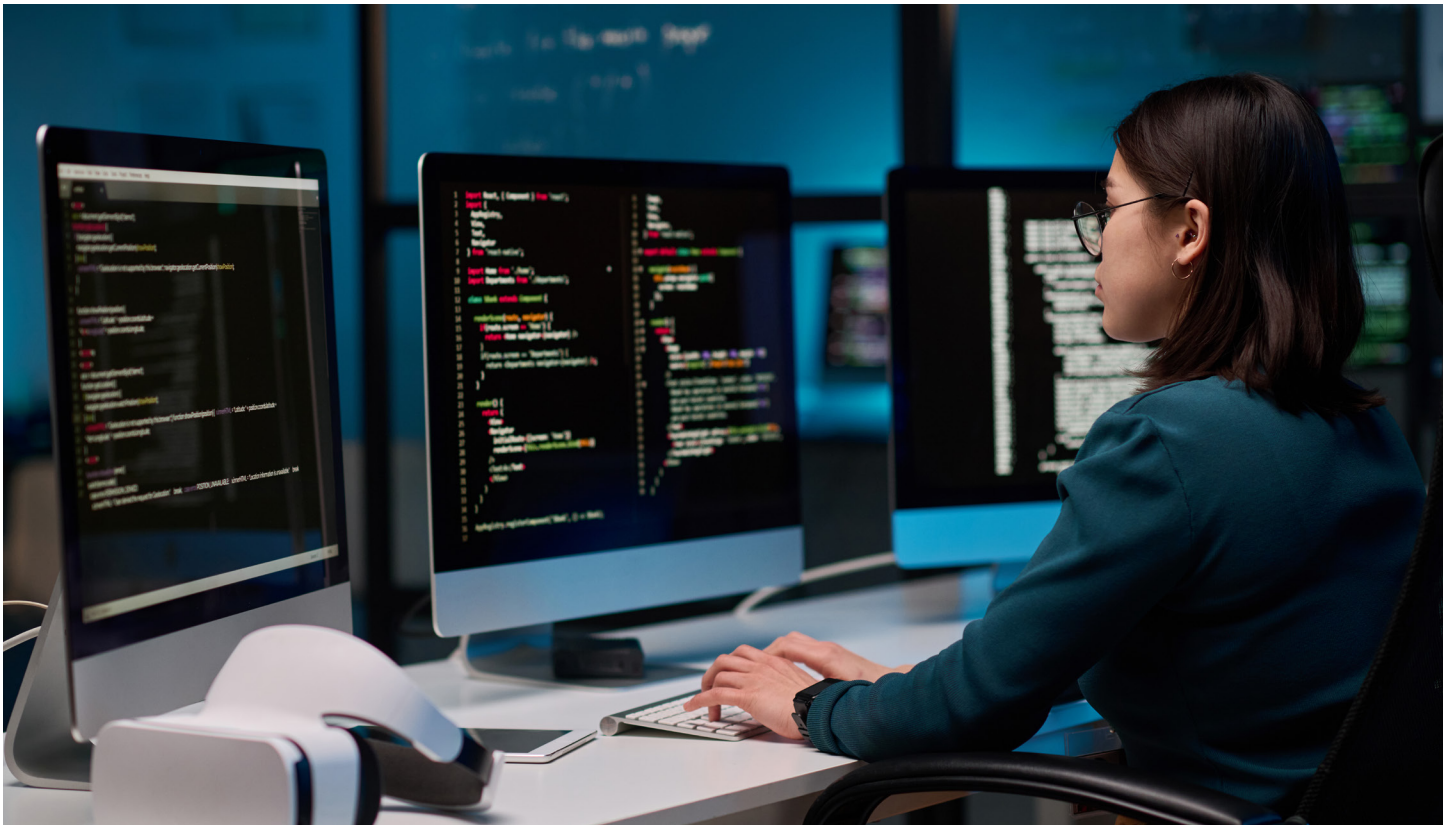
Why Entrust

Entrust delivers certificate lifecycle management as part of a comprehensive cryptographic security platform.

- Unified platform approach: Certificate lifecycle management integrated with PKI, key management, and HSM-based root of trust
- Proven expertise: Over 30 years of leadership in PKI and cryptographic security
- Enterprise scale: Designed for complex, global environments
- Post-quantum leadership: Built to support the transition to next-generation cryptography

Built for the Modern Certificate Lifecycle
As certificate lifetimes shrink and environments become more dynamic, organizations need more than automation – they need control.

Entrust Certificate Manager provides the visibility, orchestration, and extensibility required to manage certificates across the enterprise – today and into the post-quantum future.



entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION