DATASHEET

Cryptographic Security Platform – PKI and Certificate Lifecycle Management

An all-in-one, container-based PKI virtual appliance for simplified, scalable, and secure PKI and certificate lifecycle management (CLM)

BUSINESS CHALLENGE

PKI's Ever-Expanding Footprint

Over the past 30 years, public key infrastructure (PKI) has evolved and expanded, playing a critical role across a wide range of applications – from the cloud and edge networks to IoT, modern citizen identities, and digital signatures.

PKI's footprint continues to grow as it adapts to increasingly complex use cases, becoming a central component of our digital lives. However, as PKI scales and its use becomes more complex, a significant challenge emerges: the lack of clear ownership and responsibility for managing these changes.

Without visibility and understanding of how to control PKI in these new contexts, organizations struggle to maintain their security posture and infrastructure as they once did.

As PKI deployments continue to diversify and scale, another issue arises: The previous solution has often been to add another CA or source for certificates within the organization, but this approach has led to widespread certificate sprawl, creating a large maintenance problem and massive management overhead.

THE SOLUTION

Comprehensive Yet Simplified PKI

The Entrust Cryptographic Security Platform includes a comprehensive, high-performance, container-based PKI, CLM, and automation solution. It comprises all the components required to run a secure, quantumready PKI, deploy in a range of applications, and expand on demand.

Deployed as a pre-packaged virtual appliance that includes Compliance Manager, it enables customers to streamline PKI and CLM while providing the flexibility to scale across enterprise and cloud environments.

A complete PKI involves an integration of software, policies, and procedures that collectively establish and manage public key encryption. Included are all the components required to:

- Run a secure and quantum-ready PKI
- Deploy anywhere and however you need it
- Scale on demand

Cryptographic Security Platform – PKI and CLM

COMPONENTS OF THE PKI AND CLM COMPONENT

Certificate Authority

Entrust Cryptographic Security Platform provides a robust, scalable, secure solution for issuing digital certificates to ensure trusted identities across your organization. Deployed in a virtualized environment, this appliance streamlines certificate lifecycle management, supports compliance with regulatory requirements, and ensures secure communications.

- Multi-CA support for enterprise PKI deployments with automation of CLM for DevOps and microservices
- Two-tier CA hierarchy
- Dual-CA strategy enables your organization to seamlessly transition from Microsoft CAs to a modern, adaptable enterprise PKI
- Supports Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) for real-time certificate validation
- Integration with external databases and hardware security modules (HSMs) enhances security of private keys to align with industry compliance standards like FIPS

Automated Certificate Lifecycle Management

Thanks to advanced reporting, the platform's PKI Hub helps you discover all the users' and machines' digital identities across your organization from multiple CAs, includes comprehensive automation capabilities, and provides a simple and intuitive "single pane of glass" view.

- Certificate discovery via network scanning and automated import from CA databases and cloud services
- Centralized management of certificate policies, issuance, renewal, and revocation – regardless of CA vendor
- Ability to push certificates and manage key rotations and certificate profiles across endpoints
- Certificate import methods include:
  - Discovery scanner
  - Bulk import through import API
  - Manual upload though UI
  - Source sync with CA databases
  - Convenient admin controls, reporting, and notifications
- Role-based access control with customizable roles to help you with regulatory compliance, separation of duties, and delegation of responsibilities; authorization tags provide even more granular access

Learn more about Cryptographic Security Platform at entrust.com

Cryptographic Security Platform – PKI and CLM

Entrust Cryptographic Security Platform PKI and CLM Components:

- Certificate authority
- Automated certificate lifecycle management
- Enrollment services
- Online certificate status protocol (OCSP)
- Timestamping
- RESTful API (Entrust CA Gateway)
- Management Console
- Additional capabilities available within the Cryptographic Security Platform: key and secrets management, and hardware key protection

Enrollment Services

Our registration authority module for automated certificate enrollments and renewals supports Microsoft Active Directory auto-enrollment and all major industry protocols, including:

- Intune MDM
- ACMEv2
- Simple Certificate Enrollment Protocol (SCEP)
- EST
- CMPv2

Validation Authority

The Validation Authority provides real-time certificate validation via Online Certificate Status Protocol (OCSP) is built into the appliance. This validation authority supports third-party CA status checking and is designed to:

- Provide reliable information on the status of a digital certificate
- Process information from one or multiple CAs using CRLs or CA databases

Timestamping

Get maximum security and trustworthiness for your digital identities with verifiable, RFC3161-compliant timestamping of digital transactions and documents.

CA Gateway (RESTful API)

Entrust's RESTful API is a powerful interface that enables full certificate lifecycle management, reporting, trust policy, and operational management to the Cryptographic Security Platform and third-party CAs.

Management Console

Our centralized interface for deployment, configuration, and monitoring of all Cryptographic Security Platform components simplifies and streamlines management tasks for IT teams.

Cryptographic Security Platform – PKI and CLM

KEY FEATURES

Complete Technology Stack

The Entrust Cryptographic Security Platform minimizes the complexity of configuring and managing your organization's PKI. It includes a full software stack that includes Certificate Authority, automated certificate lifecycle management, enrollment services, online certificate status protocol (OCSP), timestamping, RESTful API, and management consoled with support for network-attached HSMs.

Multi-Platform Support

The platform is compatible with any virtualization platform, including but not limited to VMware, Hyper-V, cloud platform providers (Azure, AWS), and Kernel-based Virtual Machine (KVM). This ensures seamless integration into your existing IT infrastructure without additional configurations or adaptations.

Flexible and Quick Deployment

Whether on-premises or in the cloud, the platform offers deployment flexibility for diverse IT environments. Minimal setup time is required to configure and integrate into the enterprise infrastructure.

Intuitive User Interface for Simplified Management

Streamline certificate management and policy enforcement with a single, unified platform. The intuitive user interface simplifies configuration and ongoing operation.

High Availability

The platform's cluster configuration ensures your PKI solution remains operational – even during maintenance or unexpected failures – providing robust fault tolerance and business continuity.

Secure

Integrated security features such as HSM support, OCSP, and timestamping help ensure that your certificates and data remain safe.

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

ENTRUST
SECURING A WORLD IN MOTION