DATA SHEET

Entrust Cryptographic Security Platform Compliance Pack

Facilitating compliance of key management with industry-specific, national, and international standards and regulations.

OVERVIEW

When faced with a range of business applications utilizing numerous keys and secrets, maintaining compliance of key management with industry-specific standards or international regulations can be non-trivial. Robust key documentation is critical for achieving compliance with regulations and compliance standards. Without clear and complete documentation of keys, it can be extremely challenging to achieve compliance.

The Entrust Cryptographic Security Platform Compliance Pack, when activated and used in conjunction with the platform's Compliance Manager and Key Management Vaults, helps security officers evaluate the compliance of cryptographic keys used by applications on-premises and in the hybrid and public cloud with a range of standards or an organization's internal security policy. This evaluation of their cryptographic key inventory is compliant with standards such as the Payment Card Industry Data Security Standard and the NIST SP 800-57 Recommendation for Key Management, either manually or automatically.

KEY FEATURES

- Protection of AWS customer managed keys using FIPS 140-3 Level 3 certified assurance
- Single pane of glass for the management of keys across multiple organization accounts
- Full key management lifecycle of customer managed keys
- Deployed as a virtual appliance
- High-availability (HA) support with active-active cluster
- Support separation of duties, least privilege, dual control, and multitenancy
- Automated compliance engine for NIST SP 800-130, HIPAA, and other standards
- Hardware key protection using FIPS 140-3 Level 3 certified HSMs

ENTRUST
SECURING A WORLD IN MOTION

The compliance pack offers a set of customizable documentation forms and compliance templates that can help fill any gaps in your existing key documentation and enable effective risk and compliance management. By utilizing these forms, organizations can strengthen their documentation and compliance processes, helping to ensure that an environment is well-prepared for regulatory compliance audits across different types of keys, including KMIP, TDE, and API. Aligning your security requirements with customizable templates provides a unique flexibility for your organization.

Compliance policies can be enforced to cryptographic keys based on various criteria, such as the geographic location of keys, the type of key, or the business application utilizing the keys. The solution, which comprises a centralized, unified dashboard, enables organizations to view and track the compliance level of their cryptographic assets located in one or multiple vaults, whether they are configured locally or distributed geographically.

Compliance reports can be automatically generated and distributed to all relevant parties. Executive summary reports are generated and provided to C-level management for their review and decision-making needs. Detailed reports are generated for operational teams to ensure they have the necessary information for their specific compliance tasks and responsibilities.

Feature	Cryptographic Security Platform Compliance Manager	Cryptographic Security Platform Compliance Pack
Key/Secret Unified Visibility	√	√
Key/Secret Lifecycle History	√	√
Key/Secret Documentation Enforcement	X	√
Key/Secret Metadata Customization	X	√
Regulatory Compliance Assessment	X	√
Compliance Built-in Policies	X	NIST SP 800-57 NIST SP 800-130 Entrust Best Practices for Key Mgmt
Compliance Custom Policies	X	√
Compliance Reporting	X	√

Benefits

Facilitates continuous compliance with regulatory requirements and standards

Beyond the cyber-threat risk, an increasingly complex regulatory environment brings its own risks to businesses.

Ensuring compliance with legal requirements or standards is not always possible when keys aren't sufficiently documented or there is no centralized visibility into keys. Additionally, as the number of keys increases, meeting compliance requirements will consume more and more resources, increasing the overall cost for compliance.

While the Entrust platform's key management vault offers a single dashboard view of the management of cryptographic keys and secrets, the Entrust platform's Compliance Manager, when used in conjunction with the platform's Compliance Packs, extends this capability by providing an automatic approach to help support visibility, reporting, and compliance with industry standards such as NIST SP 800-130 or NIST 800-57.

These capabilities provide a quick payback by reducing the need for staff and helping to ensure keys are always documented and managed in accordance with a particular security policy or an industry-specific standard. Staff can now be deployed to higher value tasks, as key management is automated.

Thus, the Entrust Cryptographic Security Platform's Compliance Manager makes an ideal complementary tool by making it easier to demonstrate compliance to auditors, not only for one key management system but for all key management systems across your organization.

Wherever you operate and whatever the regulation, the Entrust platform's Compliance Manager can help you achieve and maintain compliance, improving your security and managing your risks.

Improves visibility and operational awareness on cryptographic key compliance and risk

As the infrastructure continues to grow, it is crucial for an organization to continuously monitor the compliance status and associated risk levels of their cryptographic assets, helping to ensure the security and integrity of the system.

The Cryptographic Security Platform Compliance Pack automates the collection and analysis of key information generated in the cloud or on-premises. This allows for real-time security assessments and risk scoring of keys.

The solution's intuitive dashboard offers operators a centralized, real-time view of key risk levels and compliance status, providing actionable insights for proactively managing and maintaining compliance.

Technical Specifications

Standard support:

- Entrust Best Practices for Key Management
- NIST SP 800-130 - A Framework for Designing Cryptographic Key Management Systems
- NIST SP 800-57 (Part 1, Rev 5) - Recommendation for Key Management

Key & Secret support:

- KMIP keys, Oracle TDE keys, MS SQL Keys, SSH Keys, API keys, tokenization keys, passwords, container secrets, database secrets

Supported public cloud key management systems:

- AWS KMS, Azure Key Vault, GCP KMS

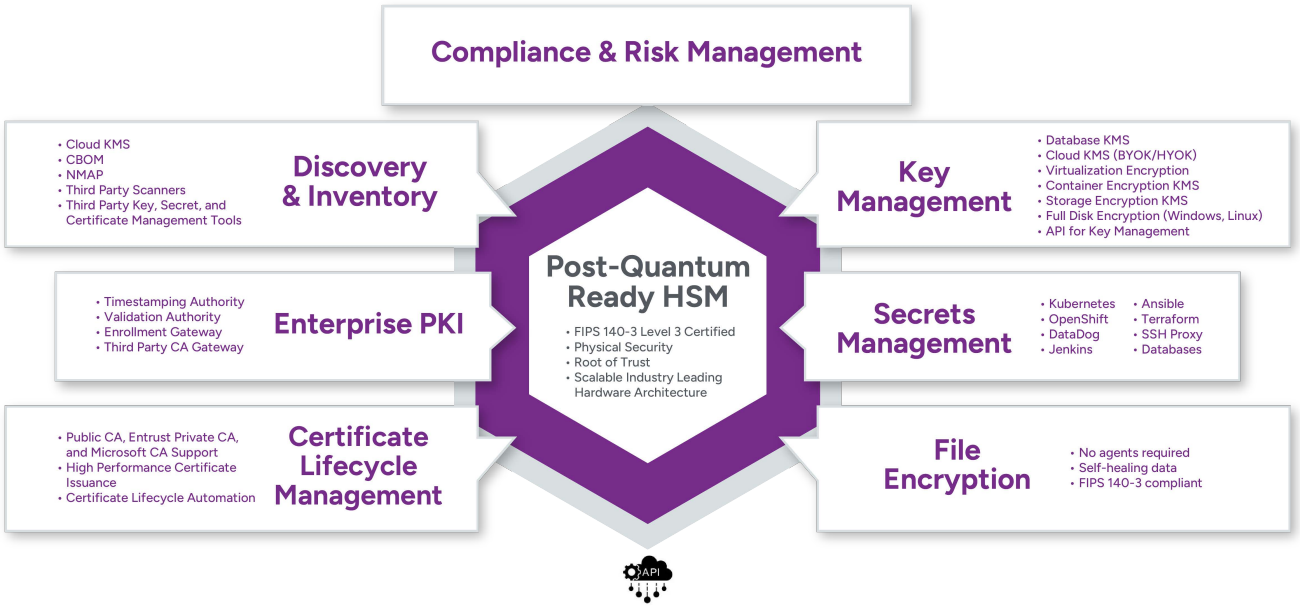
Management and Monitoring:

- Centralized management with Web UI and Rest API

Entrust Cryptographic Security Platform

The Entrust Cryptographic Security Platform provides a comprehensive solution for discovering and managing the lifecycles of certificates, cryptographic keys, secrets, tokens, libraries, protocols, and configurations.

By centralizing cryptographic asset management, it enhances security, helps ensure compliance, and streamlines operations, enabling seamless integration across both on-premises and cloud environments.



For more details on the Cryptographic Security Platform, Cryptographic Security Platform Compliance Manager, and the range of vaults download the **Entrust Cryptographic Security Platform – Key and Secrets Management brochure.**

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

ENTRUST
SECURING A WORLD IN MOTION