

Managing Cryptographic Compliance With a Comprehensive Platform

Gain visibility, reduce risk, and demonstrate control over your cryptographic estate with the Entrust Cryptographic Security Platform.



ENTRUST
SECURING A WORLD IN MOTION

Modern organizations rely on cryptography to secure nearly every digital interaction. Encryption keys protect sensitive data. Certificates establish trust between users, systems, applications, APIs, and devices. Hardware security modules (HSMs) safeguard high-value cryptographic operations. Public key infrastructure (PKI) enables secure authentication, digital signatures, and machine identity management.

Yet for many organizations, cryptographic assets are distributed across business units, cloud providers, applications, DevOps pipelines, and security teams, while the tools and responsibilities for managing them remain fragmented. As regulatory requirements expand and cyber threats evolve, organizations need a comprehensive approach to cryptographic compliance management that provides visibility, governance, policy enforcement, and audit readiness across the enterprise.

The Entrust Cryptographic Security Platform (CSP) helps organizations discover, manage, govern, and assess cryptographic assets across hybrid and multi-cloud environments through a unified cryptographic trust layer that brings together PKI, key management, certificate lifecycle management, HSMs, compliance management, and policy enforcement.

Why Cryptographic Compliance Management Matters

Cryptography sits at the heart of today's security, privacy, and compliance requirements. Organizations depend on cryptographic controls to:

- Protect confidential and regulated data
- Secure cloud workloads and applications
- Authenticate users, machines, and services
- Enable digital signatures and trusted transactions
- Protect payment systems and financial services
- Support Zero Trust architectures
- Maintain data sovereignty and key sovereignty requirements

As organizations expand globally, compliance obligations become increasingly complex. Regulations, standards and frameworks such as GDPR, DORA, NIS2, HIPAA, PCI DSS, and FIPS 140-3 place growing expectations on organizations to protect sensitive data and demonstrate appropriate cryptographic controls.

The challenge is that compliance requires more than implementing cryptographic controls. Organizations must often demonstrate:

- Where cryptographic assets reside
- Who owns and manages them
- Whether they comply with internal policies
- Whether cryptographic keys are adequately protected
- Whether certificates are properly managed
- Whether approved algorithms and key lengths are being used
- Whether cryptographic assets are being monitored and audited
- Whether cryptographic controls can adapt to emerging threats, including post-quantum risks

Without centralized visibility and governance, answering these questions becomes difficult, costly, and risky.

The Growing Challenges of Cryptographic Compliance

Cryptographic Sprawl

Most enterprises have accumulated cryptographic assets across cloud, on-premises, and hybrid environments, as well as across business units, and technology platforms. These assets include keys, certificates, secrets, algorithms, and the hardware, software and services used to manage and protect them. Over time, this distributed cryptographic estate can become fragmented across legacy PKI, cloud services, HSMs, key management systems, applications, DevOps environments, and other infrastructure.

As a result, organizations frequently struggle to identify:

- Where cryptographic assets are deployed and what they protect
- Who manages and owns them
- Which applications, systems, and business processes depend on them
- Whether associated policies and configurations remain current and appropriate
- Whether keys, certificates, and secrets have sufficient metadata and documented ownership
- Whether obsolete, redundant or non-compliant assets remain in use
- Whether cryptographic controls can be consistently monitored, governed, and audited

Limited visibility creates security gaps and compliance risks. Organizations cannot effectively govern what they cannot see.

Evolving Regulatory Requirements

Regulatory expectations continue to increase globally. Security teams must navigate overlapping requirements across multiple jurisdictions, and industries, each with its own expectations for cryptographic controls, evidence and reporting.

Common compliance challenges include:

- Producing audit evidence
- Demonstrating policy enforcement
- Maintaining regional key control requirements
- Supporting data sovereignty initiatives
- Managing cryptographic controls across hybrid cloud environments
- Tracking compliance status across growing volumes of keys, certificates, and secrets

Manual processes quickly become unsustainable at enterprise scale.



Cryptographic Asset Lifecycle Risks

Many organizations continue to manage cryptographic assets using fragmented or manual processes.

This can lead to:

- Expired or improperly renewed certificates
- Outages to services or critical business systems
- Weak or outdated algorithms and cryptographic configurations
- Inconsistent policies and controls
- Inconsistent renewal processes
- Missing metadata, dependencies, or audit evidence
- Difficulty responding quickly to policy, regulatory, or cryptographic change

As the volume of certificates and other machine identities grows, shorter certificate validity periods and increasingly dynamic cloud, application, device, and AI environments make manual lifecycle management unsustainable. Automation and centralized governance are essential to maintain visibility, apply policy consistently, prevent disruption, and adapt as cryptographic requirements change.

Post-Quantum Readiness

The clock is ticking for organizations migrating to post-quantum cryptography to meet requirements and guidance set by regional and global regulations. Organizations are increasingly under pressure to identify cryptographic assets that could be vulnerable to future quantum computing threats.

Before migration can begin, organizations must first understand:

- What cryptography they use
- Where it is deployed
- Which applications depend on it
- Which algorithms may require replacement

Many organizations lack the inventory and governance capabilities necessary to begin post-quantum planning and migration.



A Unified Approach to Cryptographic Compliance

The Entrust Cryptographic Security Platform helps organizations establish enterprise-wide cryptographic control through centralized visibility, governance, automation, and compliance management. The platform unifies PKI, certificate lifecycle management, keys and secrets management, and HSM management within a single cryptographic trust layer.

Rather than relying on multiple disconnected tools, organizations gain a common platform for managing cryptographic operations, enforcing policies, and demonstrating compliance.

Discover Your Cryptographic Assets

Effective governance starts with visibility.

Entrust CSP helps organizations discover and inventory cryptographic assets across distributed environments, including:

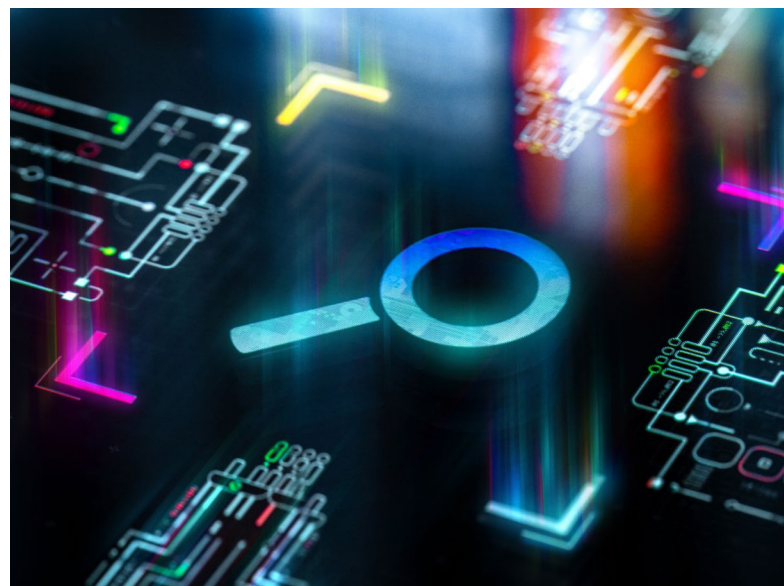
- Encryption keys
- Certificates
- Secrets
- PKI components
- HSMs
- Cryptographic services
- Third-party cryptographic assets
- Protocols and libraries

Compliance Manager and discovery capabilities collect metadata from multiple environments and aggregate it into a centralized cryptographic inventory. Organizations can gain visibility without requiring direct access to protected cryptographic assets themselves.

CBOM import and export capabilities help organizations consolidate and share cryptographic inventory data in a standardized format, providing greater context around assets, dependencies, and ownership.

This enables security, compliance, and governance teams to answer fundamental questions:

- What cryptographic assets exist?
- Where are they located?
- Who owns them?
- What are they protecting?
- Are they compliant?



Centralize Governance and Policy Management

Entrust CSP enables organizations to move beyond simple inventory management toward active governance.

Through Compliance Manager, organizations can:

- Define cryptographic policies
- Apply compliance requirements across environments
- Monitor adherence to standards and best practices
- Maintain centralized records for audit readiness
- Track exceptions and remediation activities
- Apply consistent governance across distributed systems

The platform includes support for built-in policies and customizable compliance requirements aligned with organizational needs.

Assess Compliance and Reduce Risk

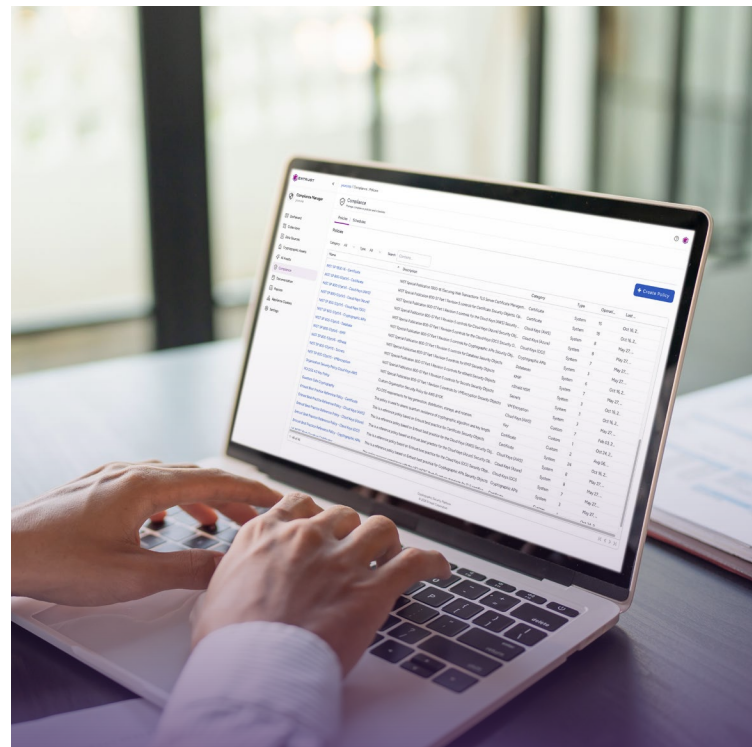
Compliance Manager assesses cryptographic assets against defined requirements, standards, and policies through scheduled or recurring assessments.

This enables organizations to:

- Identify non-compliant assets
- Detect weak or vulnerable cryptography
- Prioritize remediation efforts
- Measure compliance posture
- Generate audit evidence
- Demonstrate governance controls

CBOM data can also provide a consistent record of cryptographic assets and dependencies to support compliance reporting and audit evidence.

Security and compliance teams can quickly determine where risks exist and focus resources on the areas requiring immediate attention.



CSP enables organizations to define policies for best practices, corporate policies, and regulatory compliance requirements and schedule regular assessments of cryptographic assets against those policies.

Key Management and Major Regulations

Regulatory frameworks and industry standards such as PCI DSS, eIDAS, and FedRAMP establish requirements or expectations for protecting and managing cryptographic keys. Entrust CSP helps organizations assess keys against defined policies and requirements, maintain supporting documentation, and produce evidence for audits and compliance reviews.

Manage Cryptographic Assets Across Their Lifecycle

The Entrust Cryptographic Security Platform helps automate the management of cryptographic assets throughout their lifecycle.

Through its connected platform capabilities, organizations can:

- Discover assets
- Issue certificates
- Rotate keys
- Renew certificates
- Revoke credentials
- Retire assets
- Maintain policy compliance

Automation reduces operational overhead while helping prevent outages, security gaps, and compliance failures resulting from manual processes.

Strengthen Data Sovereignty and Regulatory Compliance

Many organizations must ensure cryptographic controls remain aligned with regional and industry-specific requirements.

Entrust CSP helps organizations:

- Understand where cryptographic assets reside
- Organize assets by region or jurisdiction
- Support customer-controlled key models
- Maintain centralized oversight across distributed environments
- Demonstrate compliance with sovereignty and governance requirements

This visibility is increasingly important as organizations navigate GDPR, DORA, NIS2, public-sector regulations, and evolving global data residency mandates.

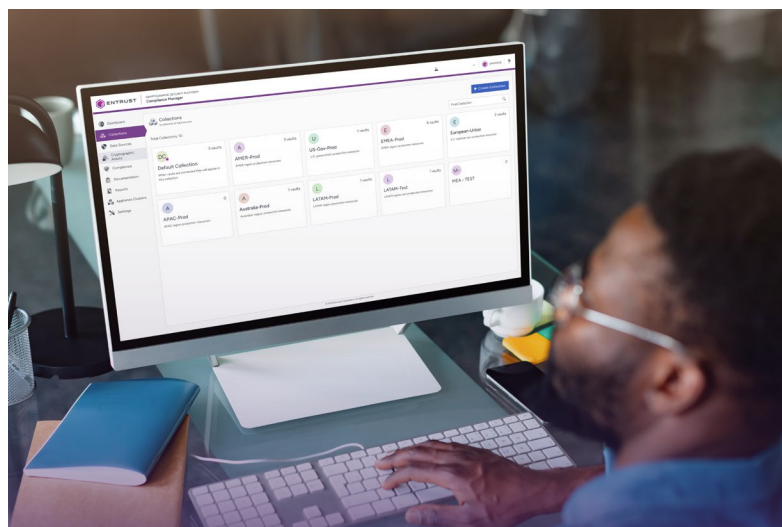
Build a Foundation for Crypto-Agility and Post-Quantum Security

Cryptographic compliance is not only about today's requirements. Organizations must also prepare for future threats.

Entrust CSP helps organizations:

- Identify cryptographic assets and dependencies
- Inventory algorithms and key usage
- Assess quantum-vulnerable cryptography
- Understand business impact
- Prioritize migration activities
- Govern cryptographic modernization initiatives

By combining discovery, governance, compliance management, and cryptographic inventory capabilities, organizations can establish the crypto-agility required for long-term resilience.



CSP's Compliance Manager provides visibility into and centralized oversight of assets in different regions, including separate region-specific vaults for keys, secrets, and other cryptographic assets.

Entrust Solutions for Managing Cryptographic Compliance

The Entrust Cryptographic Security Platform brings together the essential capabilities organizations need to manage cryptographic risk and compliance at enterprise scale:

- Cryptographic asset discovery, inventory, and CBOM import and export
- PKI and certificate lifecycle management
- Key and secrets management
- File encryption and data protection
- HSM management and monitoring
- Centralized compliance management
- Policy enforcement and governance
- Audit readiness reporting
- Data sovereignty support
- Crypto-agility and post-quantum readiness

The result is a unified platform that helps organizations gain visibility into their cryptographic estate, enforce consistent policies, reduce operational risk, support regulatory compliance, and build a stronger foundation for future cryptographic security requirements.

Cryptographic compliance management is no longer optional. As cryptographic assets continue to grow in number, importance, and regulatory scrutiny, organizations need a centralized approach to discovery, governance, and compliance. The Entrust Cryptographic Security Platform helps turn cryptographic complexity into cryptographic control.

Learn more about the Entrust Cryptographic Security Platform (CSP) or Contact Entrust Sales to discuss your use cases and compliance obligations.

Explore the Cryptographic Security Platform

ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit www.entrust.com.