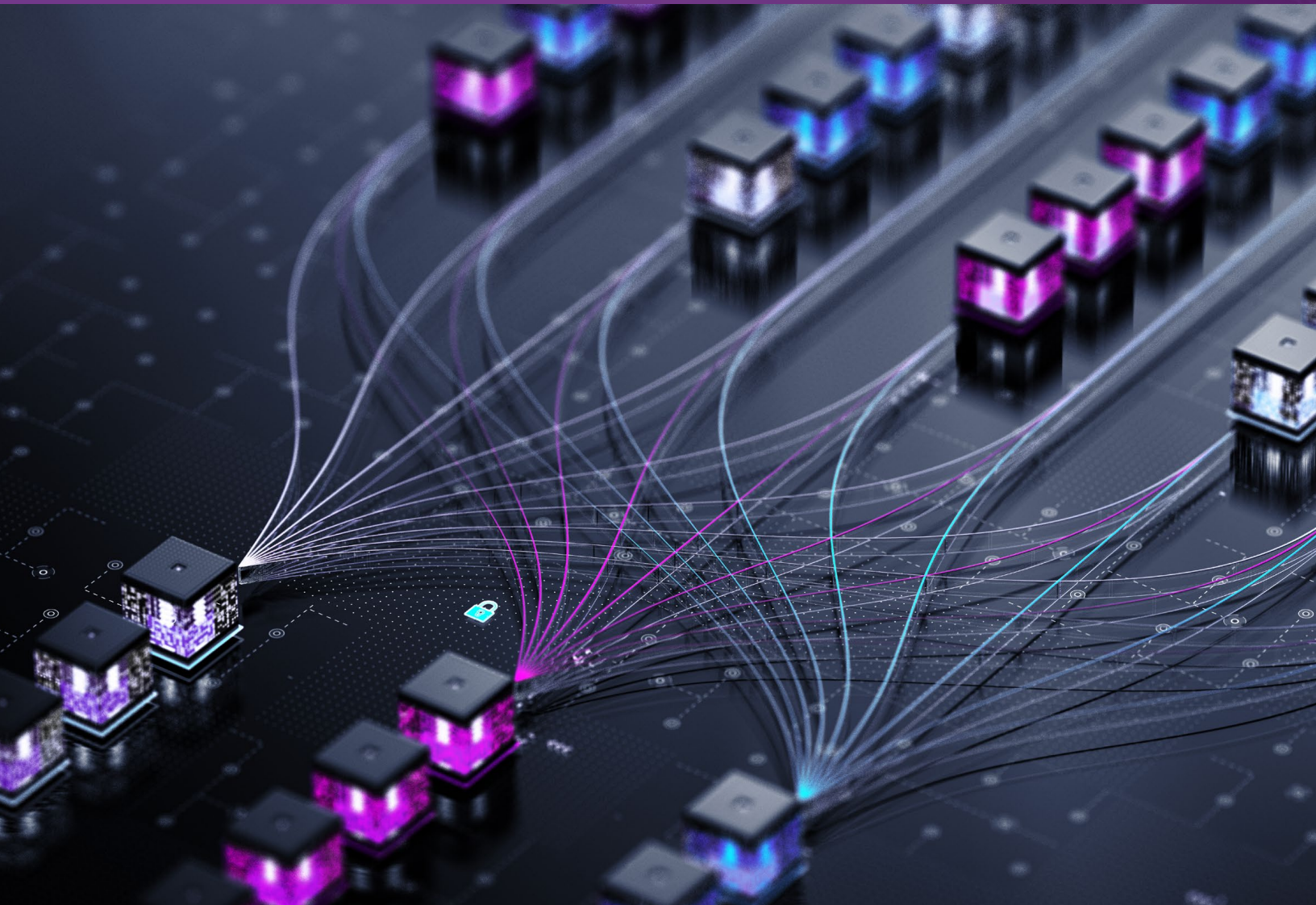


Moving From Cryptographic Visibility to Action with a CBOM

Map cryptographic assets to the business systems they protect, prioritize post-quantum migration, and support audit-readiness.



ENTRUST

SECURING A WORLD IN MOTION

Understand What Cryptography You Have and What It Protects

Cryptography protects nearly every digital business process today, from applications, APIs, identities, and customer data to financial transactions, cloud workloads, and software supply chains. Yet many organizations still struggle to answer a fundamental question:

What cryptography do we have, where is it used across our environment, and which business systems depend on it?

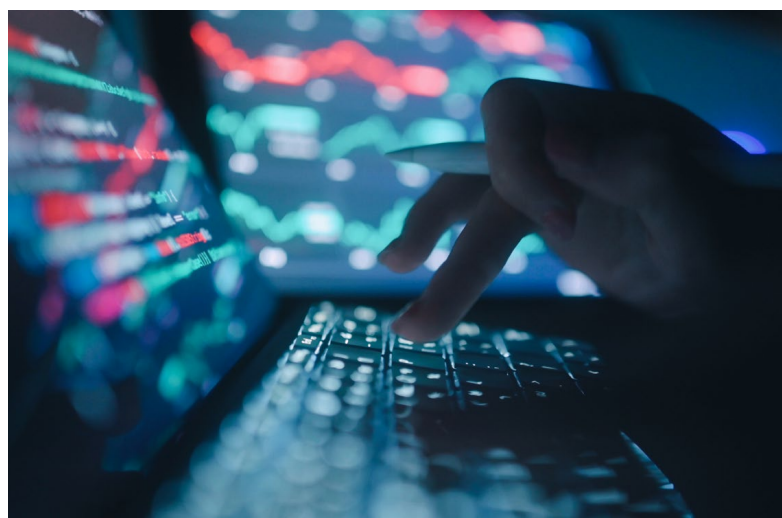
As certificate lifecycles shrink, machine identities multiply, regulatory requirements expand, and post-quantum migration timelines accelerate, organizations need a reliable inventory of their cryptographic assets. A Cryptographic Bill of Materials provides that visibility.

What Is a Cryptographic Bill of Materials?

A CBOM is a structured inventory of the cryptographic assets and dependencies operating across an environment. It can document:

- Certificates, cryptographic keys, secrets, and related metadata
- Cryptographic algorithms and parameters, including key sizes
- Cryptographic libraries and protocols
- Certificate authorities and roots of trust
- The applications, systems, and services using cryptography
- Dependencies that could be affected when cryptography expires, changes, or must be replaced

A CBOM helps organizations understand where cryptography is deployed and what business functions it protects. Think of it as the cryptographic equivalent of an SBOM (Software Bill of Materials). While an SBOM identifies software components and dependencies, a CBOM identifies the cryptographic controls that protect those components, services, and data.



Why CBOMs Matter Right Now

Post-Quantum Migration Starts With an Inventory

The transition to post-quantum cryptography (PQC) is no longer a future planning exercise. Migration begins with identifying quantum-vulnerable cryptography already in use. Security teams need to locate algorithms such as Rivest–Shamir–Adleman (RSA) and elliptic curve cryptography (ECC), determine which applications rely on them, and establish migration priorities. Without that inventory, they cannot accurately scope the work required.

Compliance Expectations Are Increasing

Organizations are facing growing expectations to maintain visibility into their cryptographic environments. Security and compliance teams need documented evidence of cryptographic controls. Requirements and guidance from PCI DSS, DORA, NIS2, U.S. federal post-quantum initiatives, and NIST transition frameworks all reinforce the need for documented cryptographic inventories and risk management processes.

Cryptographic Environments Are Growing More Complex

Machine identities, certificates, secrets, cloud keys, containerized workloads, distributed applications, and AI agents increase the number of cryptographic assets teams need to track. Spreadsheets and isolated management tools can quickly fall behind as those environments change.

Cryptographic Assets Have Business Dependencies

A certificate or cryptographic key rarely stands alone. Teams need to know which applications rely on it, which data and business services it supports, who owns the affected systems, and what may be disrupted when the asset changes. Those relationships provide the context needed to decide what to address first.



Preparing for Post-Quantum Migration

The Challenge

A global financial services organization operates thousands of systems across on-premises, cloud, and hybrid environments. Its security team needs to plan a post-quantum migration without disrupting critical payment services.

The team lacks a consistent view of:

- Where RSA and ECC algorithms are deployed
- Which certificates support critical payment systems
- Which applications depend on quantum-vulnerable cryptography
- Which business units own those systems

Without those relationships, the team cannot confidently scope or prioritize the migration.

The CBOM Approach

The organization brings discovered cryptographic assets across applications, cloud environments, certificate services, key stores, and infrastructure into a structured CBOM.

By mapping those assets to applications, business systems, dependencies and owners, the team can:

- Identify quantum-vulnerable cryptographic assets
- Trace dependencies across applications and systems
- Assess operational and business impact
- Prioritize migration activity according to risk and importance
- Track progress as cryptography changes



The Outcome

The team can build a phased migration plan based on system ownership, business dependencies, risk, and operational priority. As work progresses, a continuously updated inventory helps teams track completed changes and see where quantum-vulnerable cryptography remains.

Improving Audit and Compliance Readiness

The Challenge

A healthcare provider must demonstrate that cryptographic controls are consistently applied across certificates, keys, and secrets distributed throughout its environment.

Preparing for audits can require weeks of manual work to:

- Reconcile cryptographic information from separate inventories
- Confirm which teams and systems own or use specific assets
- Gather documentation from multiple sources
- Review cryptographic policy gaps and exceptions

Repeating that work for each review can make audit preparation unnecessarily manual.

The CBOM Approach

The provider uses a CBOM to maintain a structured view of cryptographic assets, ownership, system dependencies, and relevant policy requirements.

With maintained CBOM data, teams can:

- Review cryptographic assets through a consistent inventory
- Map assets to systems, dependencies, and accountable owners
- Evaluate assets against cryptographic policies and requirements
- Keep inventory, ownership, and lifecycle information current
- Use maintained records to support audit evidence and focus follow-up on gaps and exceptions



The Outcome

The provider can approach audits with a more current and consistent record of its cryptographic environment. Rather than rebuilding an inventory for each review, compliance teams can focus evidence gathering and remediation on policy gaps, exceptions, and areas of elevated risk.

How Entrust Helps Build and Manage a CBOM

The Entrust Cryptographic Security Platform (CSP) helps organizations import CBOM data generated by other tools and environments, combine it with discovered cryptographic assets, and map that inventory to the business systems that depend on it. By bringing CBOM data and ongoing discovery into a shared inventory, CSP helps teams maintain a more current view as cryptographic assets and dependencies change. Security and compliance teams can use that context to plan cryptographic changes, prioritize remediation, and support audit readiness.

Import and Export CBOM Data

Teams can import CBOM data generated by other tools and environments, combine it with discovered cryptographic assets, and export a more complete inventory for compliance teams, downstream processes, or other tools.

Connect Cryptography to Dependencies

Entrust CSP helps teams correlate cryptographic assets with applications, systems, owners, and available dependency information to understand exposure and potential operational impact. Teams can use that information to decide where to begin remediation or migration.

Gain Centralized Governance and Visibility

At the core of Entrust CSP is the Compliance Manager. Compliance Manager provides centralized visibility of an organization's cryptographic assets and helps assess and manage those assets against compliance requirements, policies, and risks. Through Compliance Manager and centralized cryptographic governance capabilities, organizations can inventory keys, certificates, secrets, protocols, libraries, and related metadata across distributed environments.

Security and compliance teams can evaluate assets against cryptographic policies, identify vulnerable or noncompliant cryptography, assess risk in context, and prioritize remediation or migration. Maintained inventory and policy records can also support audit readiness.

Turn Inventory into Action

A CBOM is a starting point – not a one-time exercise or the end goal. As cryptographic assets, dependencies, and risks change, organizations need to keep that inventory current and use it to guide action. Entrust CSP connects cryptographic inventory and risk context with governance and operational capabilities across PKI, certificate lifecycle management, keys and secrets management, HSMs, compliance management, and policy management. This helps organizations move from identifying cryptographic exposure to prioritizing and carrying out the appropriate remediation or migration activity.

Prepare for Post-Quantum Security

With Entrust CSP, teams can identify cryptographic assets and quantum-vulnerable algorithms, assess dependencies and business impact, and plan phased migrations to post-quantum cryptography. Centralized policies and controls also help organizations govern those transitions and support broader crypto-agility initiatives as standards and requirements evolve.

Build the Foundation for Crypto-Agility

Crypto-agility is the ability to adapt cryptographic algorithms and implementations as threats and requirements change. A well-maintained CBOM helps teams understand what is deployed, what depends on it, and what may be affected before making a change.

With CBOM import and export capabilities, centralized governance, cryptographic visibility, dependency tracking, lifecycle management, and post-quantum readiness features, the Entrust Cryptographic Security Platform helps organizations turn cryptographic inventories into actionable intelligence and build the operational foundation for long-term crypto-agility.



Explore the Entrust Cryptographic Security Platform

See how Entrust CSP helps organizations discover cryptographic assets, understand dependencies, and govern cryptographic change.

[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.