SOLUTION BRIEF

Entrust nShield Hardware Security Modules

The Cryptographic Foundation for Digital Trust at Scale

ENTRUST

SECURING A WORLD IN MOTION

Contents

Executive Summary

Entrust nShield Hardware Security Modules (HSMs) represent the gold standard in cryptographic protection, delivering FIPS 140-3 Level 3 and Common Criteria EAL4+ certified security for the most demanding enterprise environments. As quantum computing threatens to disrupt traditional cryptographic systems, organizations require a robust, future-ready solution that can adapt to evolving security needs. Our nShield platform provides unparalleled flexibility and performance, supporting diverse deployment models including on-premises, cloud, and hybrid architectures. With comprehensive API support, multi-tenancy capabilities, and proven interoperability across enterprise ecosystems, nShield HSMs enable organizations to protect sensitive cryptographic keys, accelerate secure transactions, and maintain compliance with stringent regulatory requirements. This document explores the strategic advantages of nShield HSMs, their role in post-quantum cryptography (PQC) readiness, and the technical capabilities that make them the trusted choice for global financial institutions, government agencies, and enterprise security leaders worldwide.

Modern Cryptography for the Quantum Era

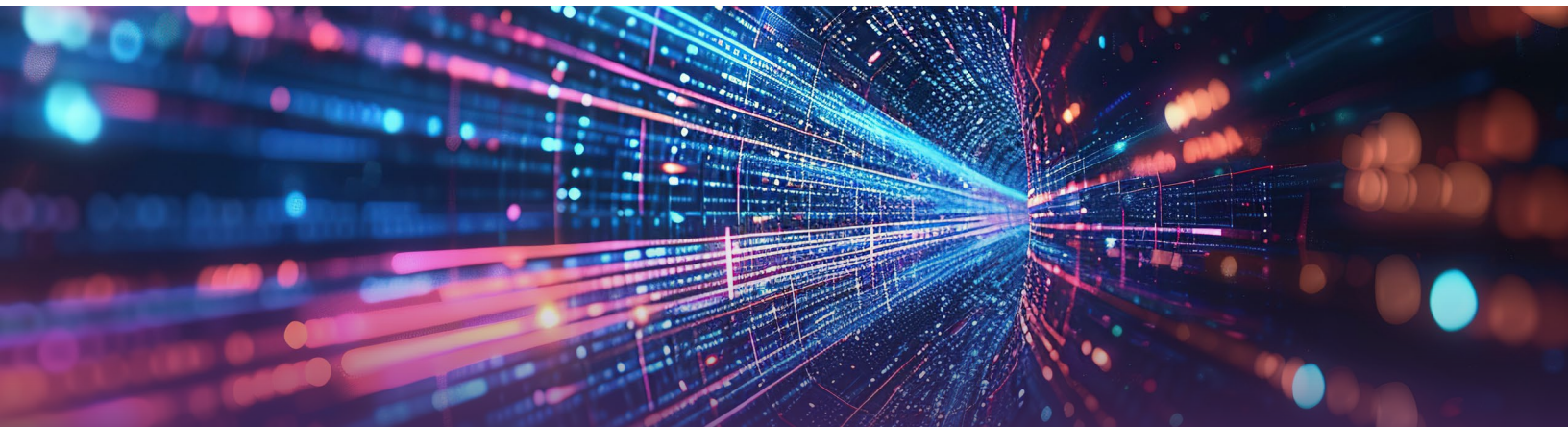
Quantum computing, expanding regulatory pressure, increasingly sophisticated cyber threats, and rapid cloud adoption are reshaping how organizations manage cryptography. The rapid advancement of AI is amplifying these risks – enabling faster attack development, large-scale automation, and more effective exploitation of cryptographic weaknesses. Approaches that rely solely on perimeter or software-based controls are no longer sufficient to protect today's distributed digital environments. At the center of modern cryptographic security is a fundamental requirement: **a trusted, hardware-based root of trust**. Entrust nShield HSMs provide this foundation, delivering FIPS 140-3 Level 3 and Common Criteria EAL4+ certified protection for the generation, safeguarding, and use of your most sensitive cryptographic keys.

Backed by more than 30 years of innovation, nShield HSMs help secure critical operations across on-premises, cloud, and hybrid environments. Our Security World architecture underpinning nShield HSM deployments delivers a unique combination of flexibility and resilience, allowing cryptographic services to scale across distributed infrastructures while maintaining strong separation of duties and centralized control. As organizations prepare for the transition to post-quantum cryptography, they require solutions that can evolve without disruption. nShield HSMs are built for **crypto-agility**, natively supporting NIST-standardized post-quantum algorithms and enabling new cryptographic methods to be adopted without costly hardware replacement.

At the same time, the scale and complexity of modern environments introduce new operational challenges. Cryptographic keys, certificates, and secrets are increasingly distributed across applications, cloud services, and infrastructure. This makes it more difficult to maintain consistent control and demonstrate compliance. To address this, Entrust extends nShield HSM capabilities with the **Entrust Cryptographic Security Platform (CSP)**, including **HSM Manager** for centralized visibility and control of your entire HSM estate. Organizations can operate, monitor, and govern their cryptographic infrastructure more efficiently while keeping nShield HSMs as the core root of trust within their security architecture.

Entrust nShield HSMs provide a hardened foundation for modern cryptography – combining high-assurance security, crypto-agility, and the flexibility to scale across today's increasingly complex and risk-driven environments.

A future-ready cryptographic foundation is essential for organizations modernizing at scale. Our Security World architecture offers unmatched flexibility and control, enabling cryptographic operations across distributed environments while maintaining centralized policy enforcement. Crypto-agility ensures seamless algorithm transitions, while CSP governance extends visibility across your entire cryptographic ecosystem.



Why You Need a Hardware Security Module

HSMs Protect the Keys That Protect Everything

HSMs are hardened, tamper-resistant devices designed to generate, protect, and manage cryptographic keys inside a secure boundary – reducing exposure to software-based attacks and insider threats. The figure below provides a visual reminder: without an HSM, encryption keys expand the attack surface by being distributed across software, memory, and various parts of a server environment. With an HSM, keys are confined within a FIPS-certified, tamper-resistant hardware boundary – drastically reducing the risk of theft or misuse.

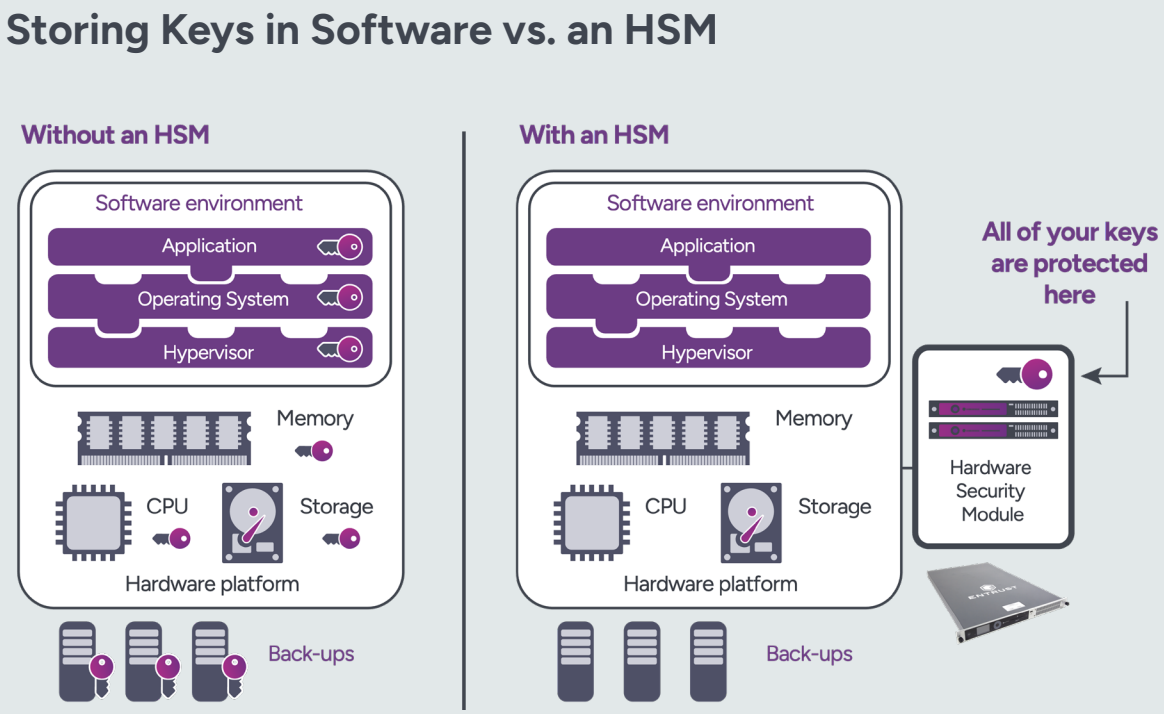


Figure 1: Illustration of keys stored and exposed in software vs. securely protected by an HSM.

Business Drivers

Organizations adopt HSMs to:

- **Increase trust and data security** by isolating cryptographic keys from general-purpose servers and applications.
- **Meet compliance requirements** by using independently validated cryptographic modules.
- **Modernize safely** as cryptography expands across cloud and distributed infrastructure.

Post-Quantum Urgency

Quantum computing will challenge widely used public-key cryptography, making post-quantum readiness an urgent priority. Entrust nShield HSMs help organizations prepare with NIST-standardized post-quantum algorithms that support crypto-agility. These quantum-ready options enable you to adopt emerging encryption methods without disruptive redesigns or costly hardware replacements.

The HSMs We Offer

The Entrust nShield Portfolio for Every Environment

Entrust nShield general-purpose HSMs are available in multiple form factors so you can match performance, operational model, and deployment method to your environment:

Network-Attached HSMs

nShield 5c HSMs provide cryptographic services to applications distributed across the network and are available in a range of performance models to meet varying throughput needs.

Figure 2: nShield 5c HSM

PCIe Embedded HSMs

nShield 5s HSMs are low-profile PCIe cards for server-hosted applications, offering high-performance local cryptographic processing in a variety of performance models.

Figure 3: nShield 5s PCIe HSM

Portable USB HSMs

nShield Edge devices are portable USB-connected HSMs ideal for development, small-scale deployments, and offline key generation.

Figure 4: nShield Edge USB attached HSM

Key Differentiators

- **Security World architecture for simplified scalability:** Unlike traditional HSM models that rely on complex clustering and manual key replication, our unique Security World architecture enables cryptographic services to scale seamlessly across multiple HSMs. Keys are not bound to individual devices, allowing organizations to add, replace, or upgrade HSMs without disruption and without the key storage limitations of traditional designs.
- **Crypto-agility without hardware refresh:** nShield HSMs are designed for long-term adaptability. New algorithms, including NIST-standardized post-quantum cryptography, can be adopted through in-field software updates. This helps organizations avoid costly hardware replacement cycles while reducing operational risk.
- **Trusted execution inside the HSM with CodeSafe:** The CodeSafe SDK enables secure execution of sensitive application code within the HSM's protective boundary, shielding critical operations from host-based threats such as malware, tampering, or insider attacks. This capability extends the root of trust beyond key protection to include critical business logic, all without compromising HSM certifications or requiring separate hardware.
- **Flexible deployment across any environment:** Support for on-premises, hybrid, and cloud-based "as a Service" deployments enables organizations to align cryptographic controls with evolving infrastructure strategies without vendor lock-in or architectural compromise.
- **High-performance cryptographic services at scale:** nShield HSMs deliver consistent, high-speed cryptographic performance across distributed environments, supporting demanding workloads such as high-volume transactions, PKI, identity management, and complex signing operations. The nShield architecture even supports **field-upgradable performance enhancements** to meet growing demand, and post-quantum algorithms are hardware-accelerated for optimized speed.
- **Open integration and broad ecosystem compatibility:** Extensive API support and a global partner network (with more than **150** validated integrations) enable seamless interoperability with leading enterprise applications, cloud platforms, and security solutions – accelerating deployment and reducing integration complexity.
- **Extending trust beyond the HSM:** Entrust nShield HSMs integrate with the Entrust Cryptographic Security Platform, including **HSM Manager (KeySafe™ 5)**, to provide centralized monitoring, management, and governance across your entire HSM estate. This holistic approach ensures you can operate and scale your cryptographic services more easily while maintaining consistent policies and strong hardware-based security.

Deployment Methods

Use nShield HSMs Wherever Your Business Runs

Modern environments need cryptographic controls that move with the business without compromising security or sovereignty. Entrust offers multiple deployment models to fit your needs:

On-Premises Deployments: Use network-attached HSMs for centralized cryptographic services shared across multiple applications; PCIe-embedded HSM cards for high-performance, local cryptographic processing within servers or appliances; and portable USB HSMs (nShield Edge) for offline use cases and development.

Cloud and Hybrid Deployments: Choose **nShield as a Service** (nSaaS) for cloud-first strategies to deliver FIPS-certified HSM services via a cloud subscription without sacrificing control or post-quantum algorithm support. Regional deployment options provide geo-fencing and data sovereignty by allowing you to select from multiple service datacenters around the world. nSaaS is unique as the only HSM as a Service solution offering a trusted execution environment running inside the HSM.

Cloud-Friendly Integration Options: nShield Web Services (a RESTful API) reduces tight coupling to specific operating systems or architectures. Our nShield Container Option Pack simplifies integration into containerized and microservices environments, making it easy to incorporate HSMs into modern DevOps workflows.

Remote Operations at Scale: nShield HSMs support secure remote management and monitoring to reduce operational overhead. **HSM Manager (KeySafe 5)** provides a single pane of glass for configuring and tracking all your HSMs – on-premises and in the cloud – ensuring consistent oversight of your cryptographic infrastructure.

These flexible deployment options enable nShield HSMs to support a wide range of critical security use cases, whether you're protecting a local data center or a global multi-cloud environment.

Use Cases

What nShield HSMs Empower

Entrust customers use nShield HSMs as the root of trust in their business-critical applications. These include both well-established core security services and emerging digital initiatives, including:

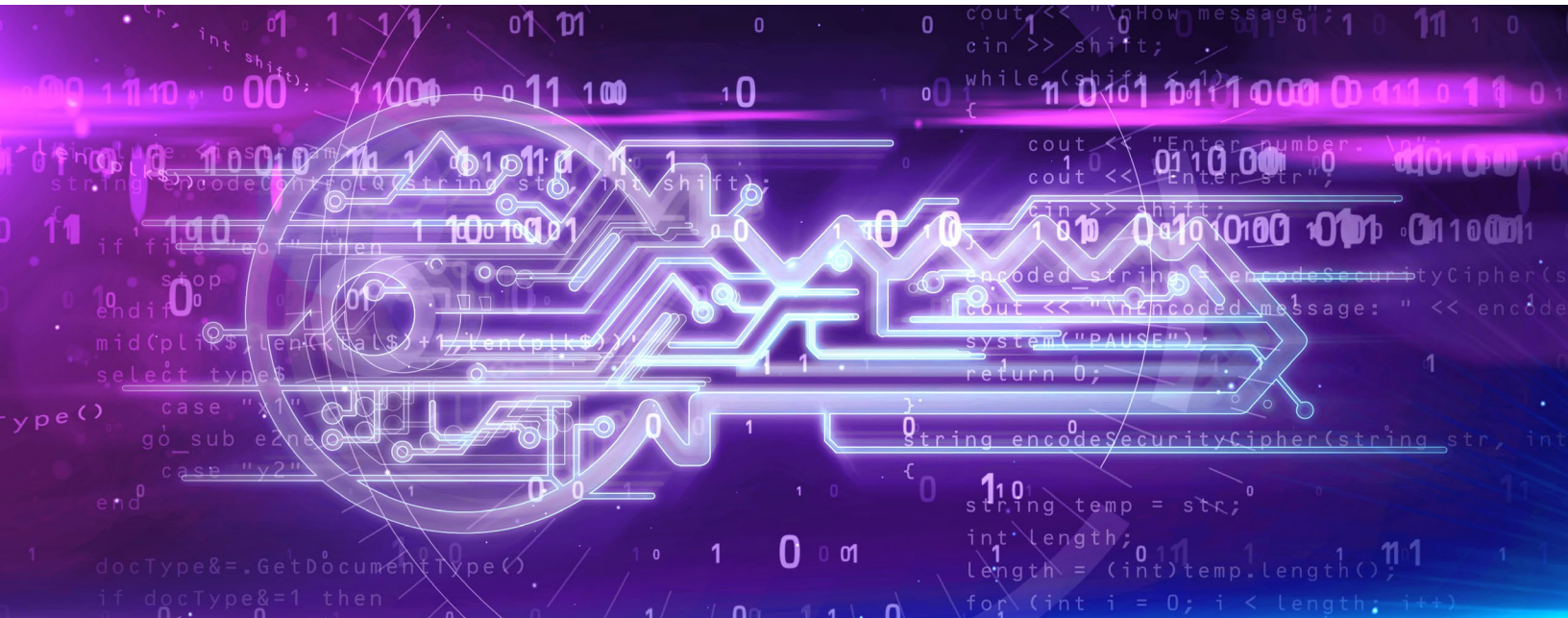
Core Security Services: Provide the hardware root of trust for public key infrastructures (PKIs) and Certification Authorities (CAs), secure millions of daily TLS/SSL communications by safeguarding server certificates, ensure software integrity with code signing and digital signing, and protect privileged access management systems.

Emerging Technologies: Enable secure 5G telecom infrastructure with hardware-protected keys, protect blockchain and cryptocurrency assets by safeguarding private keys and transactions, and strengthen IoT device identity and integrity with embedded hardware root of trust.

Cloud Key Control: Facilitate cloud adoption while retaining control of your keys. Use Bring Your Own Key (BYOK) integrations to generate and manage keys on-premises and then transfer them securely to cloud services, or Hold Your Own Key (HYOK) approaches to ensure sensitive keys never leave your custody, satisfying stringent regulatory and data sovereignty requirements.

Agentic AI: Agentic systems demand defense-in-depth, combining human authorization for critical operations with delegated cryptographic identities, signed audit logs, and isolated code and secrets managed outside untrusted environments. In Agentic AI architectures, the gateway governs intent while the HSM cryptographically authorizes irreversible actions. This separation helps contain the impact of orchestration- or agent-layer compromise, strengthening trust in autonomous operations.

These use cases highlight how nShield HSMs help organizations achieve security and compliance goals today while maintaining the flexibility and assurance needed for tomorrow's challenges.



Partner Integrations

Place nShield Within Your Existing Ecosystem

Entrust nShield HSMs integrate seamlessly with the tools and platforms you already rely on, so you can strengthen security without disrupting operations. With a broad partner program and extensive API support, nShield offers a wide range of pre-certified integrations across major technology providers, including cloud services, identity and access management solutions, enterprise applications, databases, code signing tools, blockchain platforms, and more.

Figure 5: nShield HSM Partner Integration wheel illustrating a subset of third-party integrations by use case.

Key examples include:

- **Cloud & SaaS Integrations:** nShield HSMs support seamless Bring Your Own Key (BYOK) and external key management integrations with major cloud providers like AWS, Microsoft Azure, Google Cloud, and Salesforce. nShield also integrates with AWS Key Management Service External Key Store (XKS) for customer-controlled keys and supports advanced cloud security features such as Azure's Double Key Encryption for Microsoft 365.
- **Enterprise Applications & Platforms:** nShield is pre-integrated with a broad ecosystem of partner solutions for **PKI & credential management, database encryption, code signing and digital signatures, privileged access management, application delivery**, and more – allowing you to add hardware-based encryption and key protection to critical systems with minimal effort.

Certifications & Compliance

Validated to the Highest Security Standards

Entrust nShield HSMs help organizations meet rigorous regulatory and security requirements by providing independently validated, high-assurance cryptographic protection:

FIPS 140-3

nShield 5 HSMs (nShield 5c and 5s models) are certified to **FIPS 140-3 Level 3**, with continued support for customers maintaining FIPS 140-2. This ensures compliance with US government and international security standards for cryptographic modules.

Common Criteria and eIDAS/QSCD

nShield HSMs are certified to Common Criteria EAL4+ and recognized as Qualified Signature Creation Devices (QSCDs) under the EU eIDAS regulation, meeting stringent global requirements for cryptographic trust. nShield also aligns with EN 419 221-5, supporting regulated digital trust services.

Compliance Confidence: Deploying validated HSMs gives you and your auditors confidence that your cryptographic operations meet the highest industry and regulatory standards for security, reliability, and trust.

> With Entrust nShield HSMs, we've achieved the perfect balance of security and flexibility. The Security World architecture made our cloud migration seamless.
>
> **ENTERPRISE SECURITY ARCHITECT, GLOBAL FINANCIAL SERVICES**

Why Entrust nShield

30+ Years of HSM Innovation and Market Leadership

Over three decades of HSM development and thousands of successful deployments have made Entrust nShield one of the world's most trusted hardware security solutions.

- **Proven Track Record:** Entrust nShield HSMs have delivered a reliable cryptographic foundation for thousands of organizations, including global banks, technology companies, and governments, safeguarding their most sensitive data and transactions.
- **Future-Ready Architecture:** Built on the unique Security World architecture for flexible scalability and crypto-agile design, nShield HSMs let you add capacity or adopt new algorithms (including post-quantum cryptography) without costly disruptions or forklift hardware upgrades.
- **Comprehensive Capabilities:** We offer global deployment options (on-premises, cloud, hybrid) to suit any environment, an extensive partner ecosystem for easy integration with existing solutions, and adherence to the industry's leading security certifications (FIPS, Common Criteria, eIDAS) to ensure compliance.
- **Market Leadership:** Entrust continues to drive innovation in HSMs – expanding hardware security seamlessly into cloud and hybrid environments, enabling enterprise-wide cryptographic risk visibility and remediation through solutions like Entrust CSP, and leading the industry in post-quantum preparedness with proven crypto-agility.

Extending Beyond the HSM

Visibility and Governance with the Entrust Cryptographic Security Platform

As cryptography proliferates across cloud services, applications, and globally distributed teams, many organizations struggle with visibility into where keys, secrets, and certificates reside – and how they are managed. The **Entrust Cryptographic Security Platform (CSP)**, anchored by an nShield HSM root of trust, provides an enterprise-wide approach to key and secret management. It combines decentralized, vault-based security with centralized policy and compliance management.

Entrust Cryptographic Security Platform

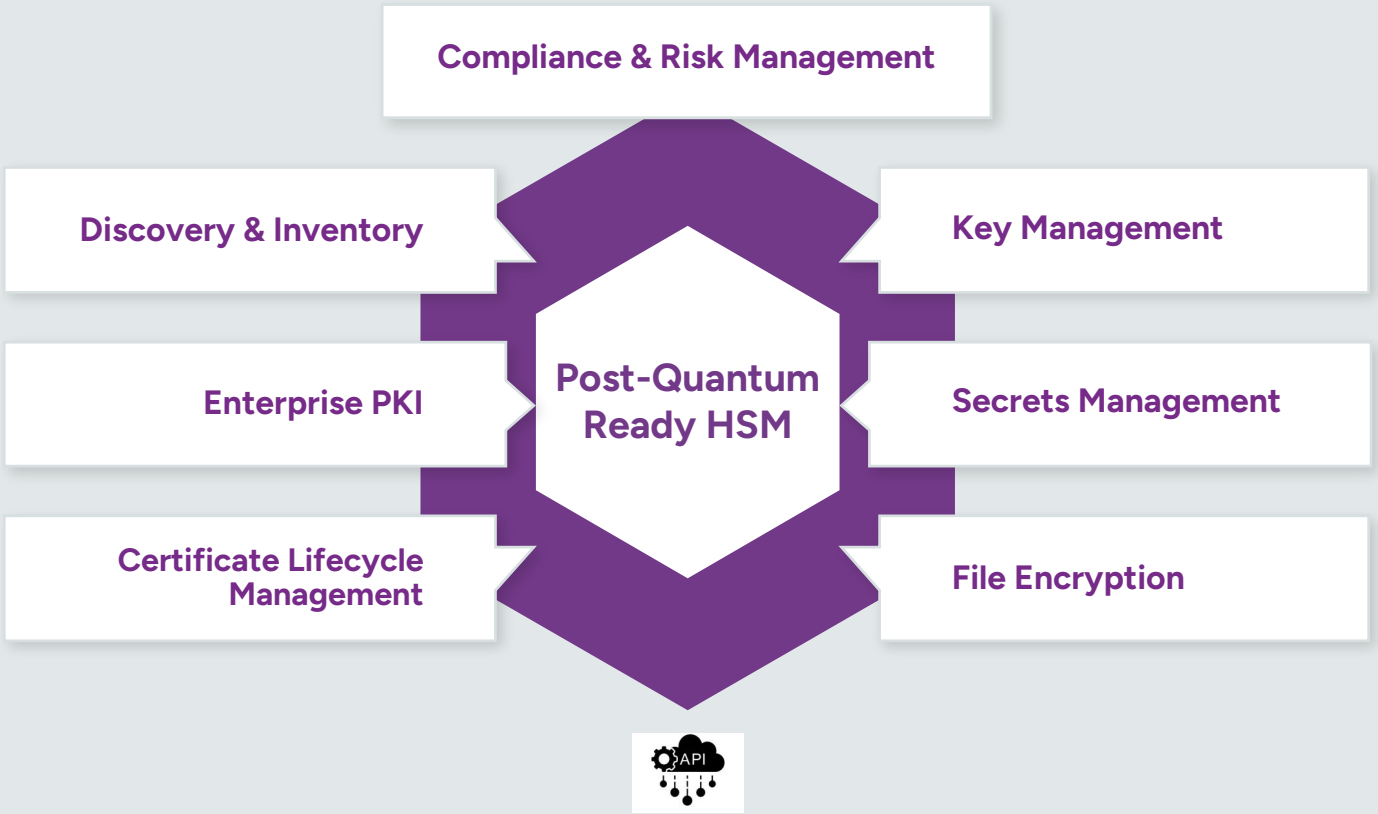
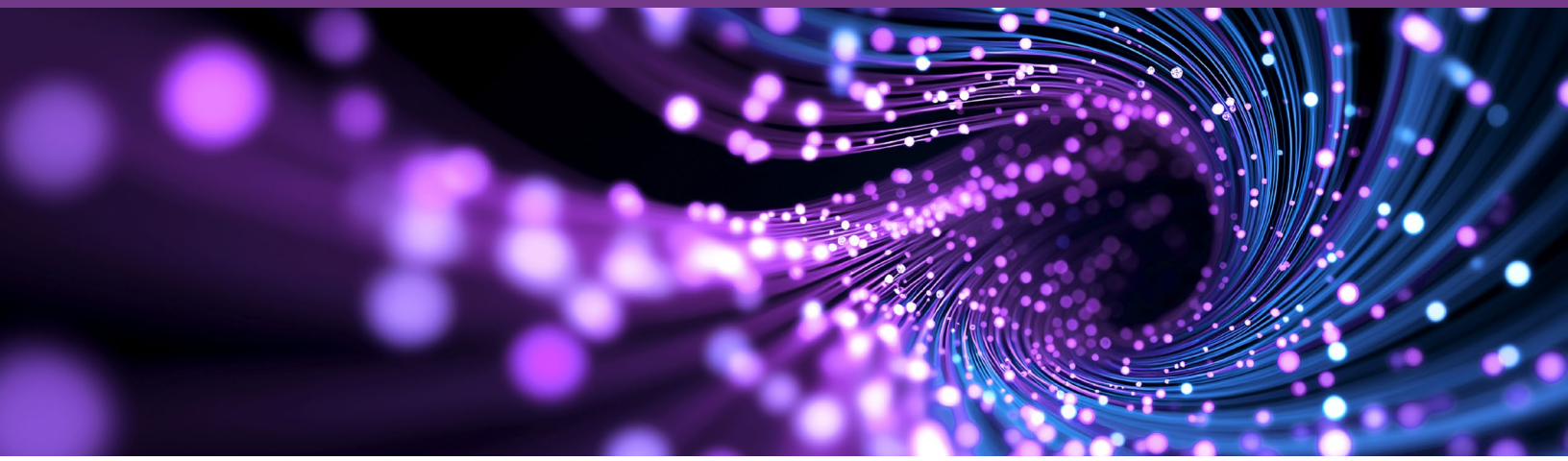


Figure 6: Entrust Cryptographic Security Platform architecture diagram, illustrating nShield HSM as the root of trust at the center of a unified key, secrets, and certificate management ecosystem for enterprise compliance and risk management.



What CSP Provides:

- **Centralized visibility** across all your distributed cryptographic assets, so you know where keys, secrets, and certificates are and who controls them.
- **Unified policy enforcement** for keys, secrets, and certificates to maintain consistent security standards.
- **Compliance reporting and audit trails** for easier proof of protection to regulators and auditors.
- **Cryptographic risk remediation** with advanced insights, helping prioritize and address vulnerabilities as you prepare for the post-quantum future.

The CSP Advantage: By pairing your nShield HSMs' hardened root of trust with enterprise-wide key and secret governance, CSP helps reduce cryptographic risk on every front. Organizations gain comprehensive visibility and control over their cryptographic estate while maintaining hardware-backed security – ensuring that as cryptographic practices evolve, your organization stays protected and compliant.

Prepare for the Future of Post-Quantum Today with HSMs

Now is the time to strengthen your cryptographic foundation for the future. **Deploy Entrust nShield HSMs** as your future-ready security backbone. Extend their reach with Entrust CSP to enhance governance, reduce risk, and meet compliance with confidence.

Contact us now to learn more about Entrust nShield HSMs

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.

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

ENTRUST

SECURING A WORLD IN MOTION