EBOOK

A Guide to Data Security

ENTRUST

SECURING A WORLD IN MOTION

INTRODUCTION

Data is everywhere – and so are the devices and systems collecting, storing, and transmitting it.

With an estimated 75 billion connected devices globally, the attack surface is expanding faster than many organizations can handle.[1] Each new device, transaction, and connection in use increases the volume of sensitive data in motion and, in turn, the risk of compromise.

Enter cryptography. For several decades, it has been the foundation of trust, protecting vital data, systems, identities, and communications using encryption, authentication, digital signing, and other security measures. But as data volumes grow and digital environments scale, organizations face a new challenge: managing an explosion of cryptographic assets – certificates, keys, and secrets – across increasingly fragmented tools and infrastructures.

This ebook explores the fundamentals of cryptographic data security and why it's an essential pillar of modern identity-centric security. From public key infrastructure (PKI) to post-quantum readiness, we'll break down the tools, technologies, and trends that help protect organizations from financial, reputational, and regulatory damage.

What Is Cryptography?

At its core, cryptography is the science of securing information, ensuring that only authorized parties can access, read, or act on sensitive data. It's the foundation of digital privacy, trust, and secure communication.

One of the most fundamental cryptographic operations is encryption – the process of converting readable data (plaintext) into an unreadable format (ciphertext). Decryption is the inverse workflow, transforming ciphertext back to its original form.

To enable these operations, cryptography relies on several core components:

Cryptographic keys

Strings of data that encrypt and decrypt information. Public and private keys are used in asymmetric encryption, while symmetric encryption uses the same key for both processes.

Secrets

Sensitive pieces of information – passwords, application programming interface (API) tokens, or access credentials – that must be securely stored and managed.

Cryptographic algorithms

Mathematical formulas that perform encryption, decryption, and other cryptographic functions. They maintain information's integrity, confidentiality, and authenticity, preventing data disclosure, tampering, or repudiation.

Digital certificates

Credentials that verify the identity of a user, device, or system. Certificates, issued by a certificate authority, contain the public keys that protect communication.

Beyond encryption, cryptography also supports authentication and digital signing. These processes use certificates to verify identities and ensure the integrity of digital interactions – enabling secure access for users, devices, and machine-to-machine communications across networks.

Hardware Security Modules (HSMs)

Cryptographic security depends heavily on how organizations generate, store, and use their keys.

Hardware security modules are dedicated devices that protect keys and provide a safe environment for performing cryptographic operations. They also support use cases like payment processing, database encryption, and secure code signing.

HSMs serve as a hardened root of trust, especially for public key infrastructure. In PKI, protecting the private key is paramount because it anchors the entire certificate chain, If the CA's private key is compromised, all certificates it issues – and the trust they represent – are no longer reliable.

Why Organizations Rely on HSMs

HSM adoption has steadily increased. Today, 55% of organizations use HSM devices compared to 47% in 2019.[2] Why? Consider these advantages:

- **Key protection by design:**

  Keys never leave the secure boundary of the hardware, minimizing exposure to bad actors.

- **Tamper resistance**

  Physical and logical protections prevent unauthorized access and manipulation.

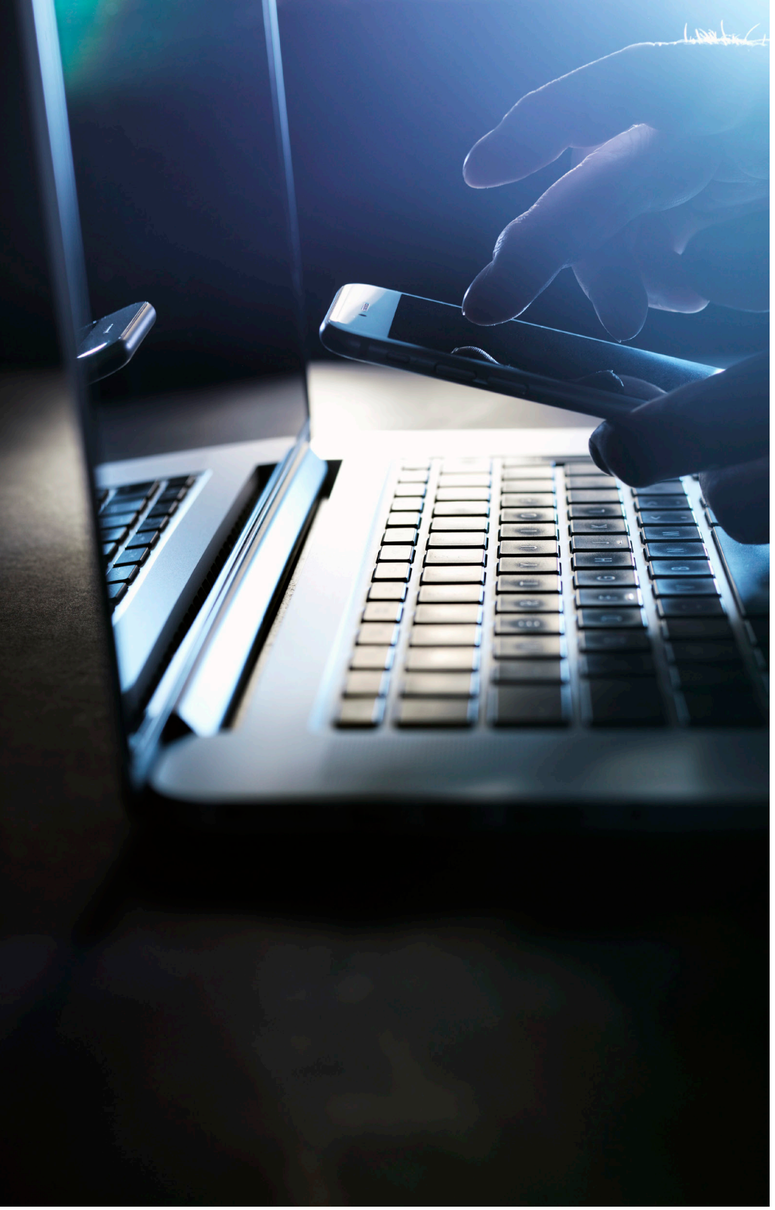
- **Performance at scale**

  Hardware acceleration enables high-volume encryption and signing operations.

HSMs also help organizations navigate regulatory complexity and avoid costly penalties. With data protection laws becoming stricter at global, regional, and industry-specific levels, HSMs provide a verifiable foundation for compliance – and peace of mind in the face of evolving threats.

55%

of organizations use HSM devices.[2]



Certificate, Key, and Secret Lifecycle Management

Digital trust is only as strong as the tools used to manage it. As organizations scale, so does the volume of certificates, keys, and secrets – each with its own expiration date, compliance requirements, and security risk. Without proper handling, these assets can quickly become liabilities.

Lifecycle management includes the issuance, renewal, rotation, revocation, and decommissioning of cryptographic assets. Traditionally, businesses relied on manual oversight for this process – and some still do. But that's no longer sustainable, especially when outages, failed authentications, or expired certificates can lead to costly downtime and damaged reputations.

Common challenges include:

- Lack of visibility across the cryptographic estate
- Inconsistent policies across teams and systems
- Delays and human errors resulting from manual processes

Fortunately, modern management tools automate the effort. They provide centralized control, policy enforcement, and real-time monitoring, helping reduce risk, improve audit readiness, and keep cryptographic assets secure throughout the entire lifecycle.

Trends in Cryptographic Security

The cryptographic landscape is shifting – and fast. Emerging technologies, evolving threats, and stricter regulations are driving a new era of data security complexity.

Robust identity security, with identity and access management (IAM), empowers organizations to secure the workforce without compromising efficiency. Solutions like advanced biometric verification, role-based access controls (RBAC), and adaptive MFA ensure users can quickly access only what they're authorized to – no more, no less.

1. Post-Quantum Cryptography

Quantum computing is perhaps the most disruptive force on the horizon. It is expected that within the next several years, a quantum computer will have the processing power and speed to break widely used encryption algorithms like RSA and ECC, putting today's data at risk tomorrow. That's why organizations are turning to post-quantum cryptography (PQC) – algorithms designed to resist quantum attacks – and building roadmaps to become post-quantum secure. In fact, 61% of businesses plan to adopt PQC within the next five years.[3]

2. Changing Regulations

The pace of regulation is accelerating. New data privacy and cybersecurity laws are emerging at global, regional, and industry levels – many with steep penalties for non-compliance. Staying ahead requires not only strong cryptography but also proactive visibility and governance over your cryptographic systems and assets.

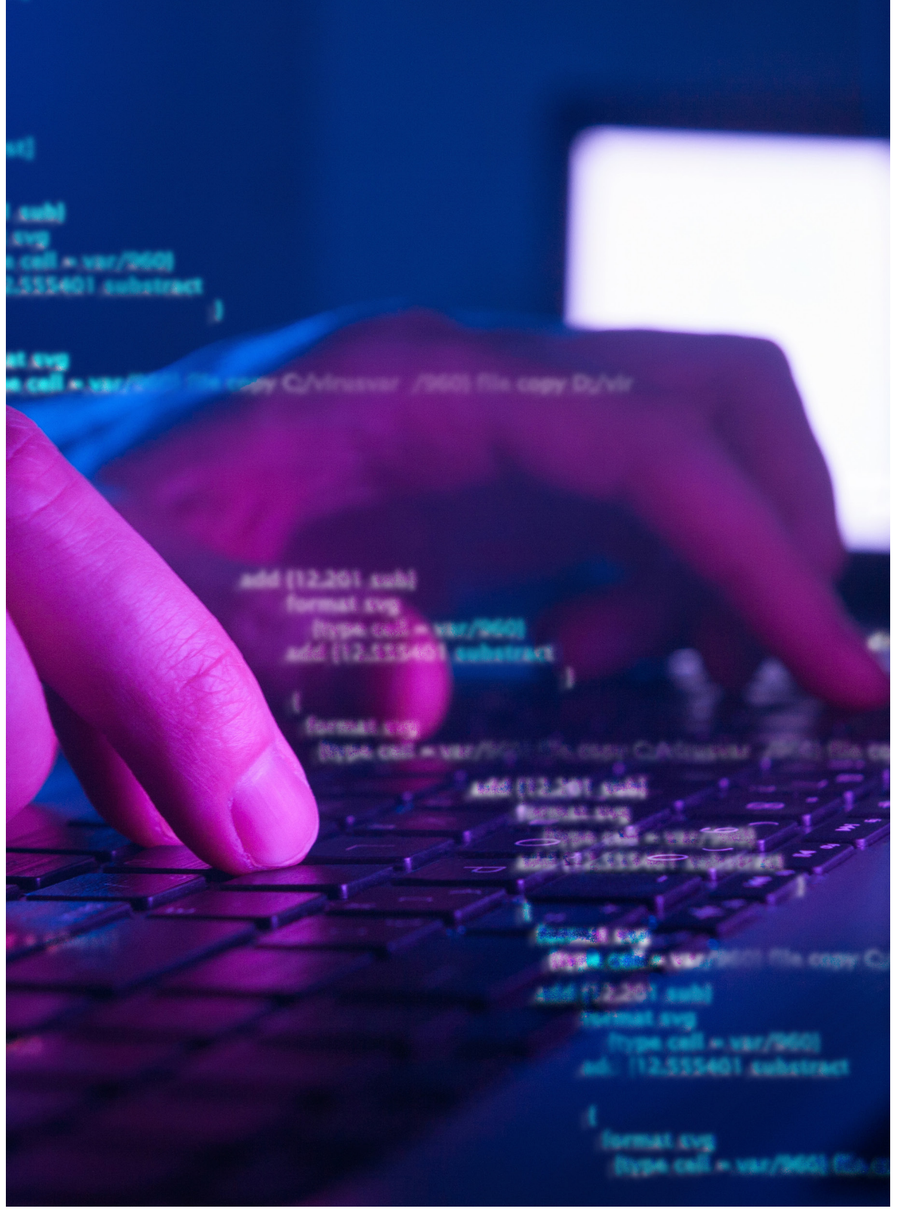
3. Organizational Complexity

Years of layered tooling have created fragmented environments: siloed teams, redundant solutions, and inconsistent policies. The result? Limited visibility and diminished agility.

To stay resilient, organizations need crypto-agility – the ability to update algorithms, rotate keys, and adapt to new risks without disrupting operations. The good news: Entrust helps counteract this complexity by unifying these tasks into a single, manageable platform built for the future.

61%

of businesses plan to adopt PQC within the next five years.[3]



Raising the Bar for Cryptographic Security

As cryptographic environments grow more complex, securing data requires more than strong algorithms – it takes visibility, automation, and trusted infrastructure. Entrust is meeting that challenge with a unified Cryptographic Security Platform (CSP) that simplifies operations across PKI, HSM, and cryptographic lifecycle management.

It also includes compliance management via a centralized dashboard that gives organizations oversight of their entire cryptographic estate. It provides real-time monitoring, policy enforcement, and audit-ready reporting across certificates, keys, and secrets – helping teams stay compliant, reduce risk, and act with confidence.

Organizations can also leverage Entrust's Cryptographic Center of Excellence – a consulting-led approach to help them assess the health of crypto systems like PKI and HSMs, navigate regulatory requirements, and build long-term resilience. From post-quantum planning to crypto-agility maturity strategy, our experts empower teams to make informed decisions and future-proof their infrastructure.

Whether you're modernizing PKI, deploying HSMs, or gaining control over cryptographic sprawl, Entrust delivers the expertise and tools to raise the bar on cryptographic security – and keep it there.

Protect Your Data With Entrust

From protecting data and verifying trust to navigating compliance and preparing for quantum threats, cryptographic security plays a critical role at every level of the modern organization.

Entrust helps you take control of this complexity. With decades of experience and innovation in PKI, HSM, and cryptography, we deliver the solutions you need to secure your most sensitive systems and adapt as new challenges emerge. Our identity-centric security offers:

- Unified visibility and control across certificates, keys, and secrets
- Compliance monitoring and automation
- Post-quantum security and built-in crypto-agility
- Advisory services to build a long-term, adaptive crypto strategy

Data moves fast, and so should your security.

Contact Entrust today and learn how you can modernize your cryptographic environment – and protect what matters most.

Get in touch

Sources

1. https://www.sciencedirect.com/science/article/pii/S1574013722000120#b5
2. https://www.entrust.com/resources/reports/2024-state-of-zero-trust-and-encryption-study
3. https://www.entrust.com/resources/reports/ponemon-post-quantum-report?edc_sfid=701Vn00000CocrBIAR

ENTRUST

SECURING A WORLD IN MOTION