Brought to you by:

ENTRUST

SECURING A WORLD IN MOTION

Cryptography

for dummies®

A Wiley Brand

Recognize crypto criticality drivers

Understand the crypto agility imperative

Prepare for post-quantum crypto now

Entrust Special Edition

Lawrence Miller

About Entrust

Entrust keeps the world moving safely by enabling strong identities, secure payments, and protected data. We offer an unmatched breadth of solutions that are critical to the future of secure enterprises, governments, the people they serve, and the data and transactions associated with them. With our experts serving customers in more than 150 countries and a network of global partners, it's no wonder the world's most trusted organizations trust us. For more information, visit www.entrust.com.

Cryptography

Entrust Special Edition

by Lawrence Miller

for dummies®
A Wiley Brand

Cryptography For Dummies®, Entrust Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-394-37418-2 (pbk); ISBN 978-1-394-37419-9 (ePDF); ISBN 978-1-394-37420-5 (ePUB)

Publisher's Acknowledgments

Acquisitions Editor: Traci Martin
Senior Managing Editor: Rev Mengle
Client Account Manager: Jeremith Coward
Content Refinement Specialist: Bharaneedharan Murthy

Table of Contents

Introduction

Cryptography has long been used to ensure the confidentiality, integrity, and authenticity of digital communications and transactions, sensitive data, and identities. Every time you use a mobile banking app or purchase a product or service online, cryptography is used to secure your transaction. The modern digital world relies heavily on cryptographic hardware, software, and credentials (such as keys, certificates, and secrets), but challenges still exist.

Today's companies find that an increasing number of things must be secured against sophisticated attacks and highly motivated threat actors — such as state-sponsored organizations, ransomware gangs, hacking groups, and malicious insiders — while trying to keep up with complex regulatory requirements and rapidly evolving technologies such as artificial intelligence (AI), machine learning (ML), and quantum computing.

Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but this book assumes a few things nonetheless!

Mainly, it assumes that you're an IT leader looking for a solution to address your organization's cryptography challenges. Perhaps you're a DevOps Manager struggling to integrate security into your continuous integration/continuous delivery (CI/CD) pipelines and manage secrets across different environments. You may be an IT Operations Director working to reduce operational costs, simplify infrastructure management, and ensure high availability. Or a Compliance Manager interested in measuring and managing risks across multiple cryptographic solutions and ensuring regulatory compliance. As such, you have at least a working knowledge of cryptography fundamentals and concepts.

If any of these assumptions describe you, then this is the book for you! If none of these assumptions describe you, keep reading anyway. It's a great book and after reading it, your knowledge of cryptography will be expanded!

Icons Used in This Book

Throughout this book, a few special icons call attention to important information.

REMEMBER

This icon points out important information you should commit to your nonvolatile memory, your gray matter, or your noggin.

TECHNICAL STUFF

This icon explains the jargon beneath the jargon and is the stuff legends — well, legendary nerds — are made of.

TIP

Tips are appreciated, but never expected — perhaps you'll appreciate these useful nuggets of information.

WARNING

These alerts point out the stuff your mother warned you about (well, probably not), but they do offer practical advice.

Beyond the Book

There's only so much that can be covered in this short book, so if you find yourself at the end of this book wondering, "Where can I learn more?" go to `https://entrust.com`.

IN THIS CHAPTER

- Learning the basics of cryptography
- Differentiating between cryptography types
- Exploring common cryptography use cases

Chapter 1
Cryptography 101

This chapter covers the basics of cryptography including what it is, the different types of cryptography, and how cryptography is used in the digital world.

Defining Cryptography

Cryptography is everywhere.

It has become an integrated layer of defense within all of the digital transformation initiatives now collectively referred to as digital business. As the foundation of modern security systems, cryptography is used to secure transactions and communications, safeguard personal identifiable information (PII) and other confidential data, authenticate identity, prevent document tampering, and establish trust between servers.

Cryptography is one of the most important tools businesses use to secure the systems that hold their most important asset — data — whether it's at-rest or in-motion. Data is vital information in the form of customer PII, employee PII, intellectual property, business plans, and any other confidential information. Therefore, cryptography is critical infrastructure because, increasingly, the security of sensitive data relies on cryptographical solutions.

REMEMBER

Cryptography (from the Greek *kryptos*, meaning "hidden," and *graphia*, meaning "writing") is the science of encrypting and decrypting communications to make them incomprehensible to everyone but the intended recipient.

Cryptography can be used to achieve several goals of information security:

- **Confidentiality:** Cryptography protects the confidentiality or secrecy of information. Even when the transmission or storage medium has been compromised, the encrypted information is practically useless to unauthorized people who don't have the proper keys to decrypt the information.
- **Integrity:** Cryptography can also be used to ensure the integrity or accuracy of information using hashing algorithms and message digests to verify that information hasn't been altered by an unauthorized person.
- **Authentication:** Cryptography can be used for authentication and nonrepudiation services through digital signatures, digital certificates, or a public key infrastructure (PKI).

A QUICK CRYPTOGRAPHY PRIMER

Cryptographic techniques describe how algorithms are applied in practice to secure data or validate identity. These include:

- **Encryption** is the process of converting plaintext communications to ciphertext. **Decryption** reverses that process, converting ciphertext to plaintext.
- **Hashing** creates a fixed-length output from data to verify integrity. Even a small change in input results in a dramatically different output. Because it's a one-way function, hashing is used to verify data integrity, for example, checking if a file or password has been altered.
- **Digital signatures** use asymmetric cryptography to sign data with a private key. The recipient can then verify that signature using the sender's public key. This process proves both the authenticity of the sender and the integrity of the message, making it critical to secure communications, legal documents, software updates, and more.

- **Key exchange** techniques allow two parties to securely share an encryption key over a potentially untrusted network.

There are two primary types of encryption used in cryptographic systems:

- **Symmetric encryption** uses a single key to both encrypt and decrypt data. It's fast and efficient, making it ideal for encrypting large volumes of data at rest.
- **Asymmetric encryption,** also known as public key cryptography, uses a pair of keys: one public and one private. This model supports secure key exchange and digital signatures, which are foundational to protocols like Transport Layer Security (TLS) and systems like PKI.

Most enterprise environments rely on a hybrid model that combines both methods to maximize security and performance.

Understanding Different Cryptography Types

There are many different types of cryptography used today. These include PKIs, hardware security modules (HSMs), cryptographic keys, digital certificates, and secrets.

Public key infrastructure

PKI is the system that issues, manages, and revokes digital certificates. It enables secure authentication for users, devices, and services by tying public keys to verified identities. PKI is foundational to trust models in everything from website security to secure email and code signing.

There are four basic components of a PKI:

- **Certificate Authority (CA):** The CA is composed of hardware, software, and the personnel administering the PKI. It issues certificates, publishes status information and certificate revocation lists (CRLs), and maintains archives.

- **Registration Authority (RA):** The RA is also composed of hardware, software, and the personnel administering the PKI. It's responsible for verifying certificate contents of the CA.
- **Repository:** A repository is a system that accesses certificates and CRLs from a CA and distributes them to authorized parties.
- **Validation Authority (VA):** An entity that provides a service used to verify the validity of a digital certificate.

Hardware security modules

Hardware security modules (HSMs), discussed in Chapter 5, are hardened, tamper-resistant hardware devices that secure cryptographic processes by generating, protecting, and managing keys used for encrypting and decrypting data and creating digital signatures and certificates.

HSMs act as a Root of Trust, provisioning and protecting keys for a wide ecosystem of industry standard applications including database protection, privileged access management, PKI, and many others. A Root of Trust is a foundational security component that ensures the integrity and authenticity of data and operations. HSMs are the gold standard for protecting private keys and associated cryptographic operations.

Cryptographic keys

Encryption (or cryptographic) keys are alphanumeric codes or sequences of characters that are used, together with an algorithm or mathematical process, to transform plaintext that anyone can read into scrambled ciphertext that is unreadable unless properly decrypted. Encryption keys are used to protect private and sensitive data in storage, in transit, and in use. Encrypted data, or ciphertext, can only be read after it is descrambled with its associated decryption key.

Encryption keys can be symmetric or asymmetric. When a symmetric encryption key is used, the same key is employed to encrypt and then decrypt the data back to readable text. When asymmetric keys are used, one publicly shared key (public key) encrypts the plaintext and a different key, one that is never shared and kept private (private key), is used to decrypt the ciphertext.

Digital certificates

PKIs use digital certificates to bind public keys to their associated user (owner of the private key). Digital certificates are the credentials that facilitate the verification of identities between users in a transaction. Much as a passport certifies one's identity as a citizen of a country, the purpose of a digital certificate is to establish the identity of users and machines — including mobile and Internet of Things (IoT) devices, as well as containers, virtual machines, and application workloads — within the ecosystem. Because digital certificates are used to identify the users and machines to whom encrypted data is sent, or to verify the identity of the signer of information, protecting the authenticity and integrity of the certificate is imperative to maintain the trustworthiness of the system.

TIP

U.S. and Canadian ePassports use PKI and digital certificates.

Secrets

Secrets permit access to critical business systems and sensitive information. There are many different types of secrets, but the most common include:

- **Passwords:** As the most basic type of secret, username-password credentials are a prime target for threat actors. Weak password management has been the root cause of many data breaches.
- **Application programming interface (API) keys:** APIs are software intermediaries that allow two computer programs to communicate. API keys, by extension, authenticate and authorize access to those services and applications.
- **Encryption keys:** An encryption key uses a cryptographic algorithm to encrypt and decrypt sensitive information. This type of credential is especially vital to data security, because it protects confidentiality.
- **Secure Shell (SSH) keys:** SSH is an Internet protocol used for managing networks, operating systems, and configurations. An SSH key secures remote communication between machines on an unprotected open network.
- **Open Authorization (OAuth) tokens:** OAuth tokens allow users to grant access to websites, applications, and services without sharing their passwords.

Looking at Cryptography Use Cases

Cryptography is a critical component of today's digital infrastructure. Over time, cryptography has become ubiquitous yet often unseen, embedded into the applications we use daily — such as computer operating systems, web and application servers, mobile devices and apps, IoT devices, electronic payments, and even passports.

Securing machine identities

As organizations accelerate their digital transformation with the increasing use of cloud services, containers, and automated systems, the rise in machine identities has brought both new opportunities and significant cybersecurity risks. In fact, machine identities now outnumber human identities 82 to 1 according to the CyberArk *2025 Identity Security Landscape* report. This huge number of machine identities expands the threat landscape and the risks associated with machine-to-machine (M2M) communication, which occurs without human intervention.

WARNING

Given the vast categories of machine identities, there is often no central oversight over securing and managing machine identities across an organization (due to siloed teams and fragmented tools), thereby creating additional risk.

Unfortunately, many organizations are still struggling with how to define and secure these identities, increasing the risk of potential data breach and system downtime — both of which can result in financial losses and damage to an organization's brand trust. Cryptography enables organizations to positively verify their machine identities with nonrepudiation.

TECHNICAL STUFF

Nonrepudiation means that an action (such as an online transaction or email communication) can't be easily denied. Nonrepudiation is a related function of identification and authentication, as well as accountability.

Safeguarding network communications

Applications, including messaging platforms, video conferencing tools, and email clients, rely on cryptographic protocols to encrypt messages and ensure that only the intended recipient can read them. In enterprise settings, secure communication is

essential for protecting intellectual property, trade secrets, and internal operations.

Protecting data confidentiality and integrity

Cryptography protects the confidentiality of information. It does so by encrypting the original plaintext data into ciphertext to prevent unauthorized individuals from viewing its contents. Cryptography also ensures the integrity of data by creating a hash or message digest from the original message using a one-way hash function. This hash can't be converted back to the original plaintext and any modification of the original plaintext, no matter how small or insignificant (for example, adding a single blank space in a paragraph), will drastically alter the resulting hash.

IN THIS CHAPTER

- Dealing with device and data sprawl
- Addressing organizational complexity
- Managing the shrinking lifecycle of digital certificates
- Quantifying post-quantum threats to cryptography
- Adopting zero trust as a best practice
- Complying with regulatory requirements and standards

Chapter 2
Recognizing the Drivers of Cryptographic Criticality

This chapter examines the many issues and challenges that organizations must address to secure their growing cryptographic estates.

Protecting More Devices and Data

The modern threat landscape is growing exponentially. Today, there are more than 75 billion connected devices on the Internet, up from 31 billion just 5 years ago, according to the National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (CCoE), and our digital data footprint is expected to grow from 175 zettabytes today to 421 zettabytes 5 years from now, according to IDC.

This explosion of data and devices means more cryptographic assets — including keys, certificates, secrets, and more — are required to secure them. At the same time, attacks on cryptographic systems are increasing in number and sophistication.

TECHNICAL STUFF

One zettabyte is equal to one billion terabytes!

Looking at Organizational Complexity

Simply put, organizational complexity is a very real challenge. Many disparate tools are used to manage modern systems, networks, data, and security — including cryptography — across diverse on-premises, private/public/edge cloud, hybrid, and multicloud environments.

REMEMBER

Most organizations struggle to manage the complexity of their cryptographic assets today. For example, outages caused by certificate expirations are an all-too-common, unforced error. Keys and certificates exist all over organizations, with no clear ownership or policies to support what they're used for. Without the right tools to provide complete visibility, centralized control, and automated lifecycle management, proper management of your cryptographic assets to mitigate these risks is practically impossible.

Managing Short-Life Certificates

Digital certificates are everywhere. In 2014, Google started using the Hypertext Transfer Protocol Secure (HTTPS, also known as HTTP over TLS, or Transport Layer Security) as a ranking factor in its search engine. Today, more than 96 percent of all traffic across Google is encrypted, according to the Google Transparency Report. The ubiquitous nature of digital certificates makes manual certificate management processes unsustainable. But the number of digital certificates in use today is only part of the story.

Short-life certificates are coming. Publicly trusted certificates, like the ones you put on your web servers — you know, the ones that experience an outage every one or two years when that certificate expires — are about to start expiring even more quickly. The Certificate Authority/Browser (CAB) Forum recently reduced the validity periods for Secure Sockets Layer (SSL)/TLS certificates.

The validity period will shrink from 398 days today, to 200 days beginning in March 2026, down to 100 days beginning in March 2027, and eventually down to 47 days by March 2029. This means your certificate management challenges are about to massively increase over the next several years.

Understanding Post-Quantum Threats

Information security professionals and compliance/risk practitioners are set to face one of the most significant disruptive forces of their careers: quantum computing. Advancements in quantum technology are expected to produce a cryptographically relevant quantum computer (CRQC) within the next decade. However, post-quantum threats are here today, and organizations must prepare now.

Harvest now, decrypt later

Threat actors, particularly those sponsored by nation-states, are already working to collect treasure troves of valuable, sensitive encrypted data on governments, businesses, and individuals — just waiting for the arrival of post-quantum computing that will make child's play of many of today's most secure encryption algorithms.

Breaking bad (that is, weak) algorithms

Rivest-Shamir-Adleman (RSA), Diffie-Hellman (DH), and Elliptic Curve Cryptography (ECC) are cornerstones of most asymmetric cryptosystems today. In classical computing terms, these algorithms are neither bad nor weak. But quantum computing will render these algorithms obsolete and ineffective, requiring rapid and pervasive adoption of quantum-safe cryptographic algorithms in all cryptographic assets and applications.

Crypto key theft

Threat actors could steal various keys — master keys, code-signing keys, private keys — and other cryptographic assets, then use quantum computers to forge or spoof these assets. Similar to the "harvest now, decrypt later" concept, threat actors could steal digital signatures in a "sign now, forge later" scheme.

TIP

Chapter 4 discusses how you can start preparing your organization for post-quantum threats today.

Implementing Zero Trust

Modern digital architectures introduce additional threats, which place increasing assurance requirements on cryptography to facilitate identity-centric security.

Approaches such as adopting zero trust architectures rely less on the role of perimeter security controls and instead focus on authenticating and authorizing each transaction, based on the core zero trust principle of "never trust, always verify." Cryptography underpins the authentication of devices, applications, and users within such frameworks.

Addressing Compliance Mandates

Encryption is a key element of data security and privacy, as well as systems security, and it's addressed in many regulatory frameworks and security standards today. These various regulations and standards include the Federal Information Security Modernization Act (FISMA), Federal Information Processing Standards (FIPS), and NIST Special Publications in the U.S., and the General Data Protection Regulation (GDPR), Digital Operational Resilience Act (DORA) and Electronic Identification, Authentication, and Trust Services (eIDAS) in the European Union (EU), among many others. The following sections briefly cover a few of these regulations.

Security and Privacy Controls for Information Systems and Organizations (NIST 800-53)

FISMA requires government agencies to develop and enforce policies around secure configuration and deployment of information systems. These requirements are defined in Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements*, with further standards and guidelines published in NIST Special Publication (SP) 800-53, *Security and Privacy*

Controls for Information Systems and Organizations. Cryptography figures prominently in many of the security controls defined in NIST 800-53, including access control, audit and accountability, identification and authentication, and system and information integrity, among others.

Digital Operational Resilience Act (DORA)

DORA is an EU regulation that targets cyberrisk management in financial institutions and their information and communication technology (ICT) partners. DORA creates a binding oversight framework and establishes technical standards that EU financial entities and their service providers must implement in their ICT systems. DORA most directly applies to organizations that provide financial services in the EU, including banks, credit unions, investment firms, insurance companies, and other types of financial institutions. However, ICT service providers are also subject to DORA compliance and any ICT provider based outside the EU but still operating within its jurisdiction is subject to DORA.

REMEMBER

Numerous articles within DORA have important implications for cryptography and cryptographic solutions. For example, Article 9 (Protection and Prevention) requires organizations to:

- "*ensure the security of the means of transfer of data*" (Paragraph 3, Section a)
- "*prevent the lack of availability, the impairment of the authenticity and integrity, the breaches of confidentiality and loss of data*" Paragraph 3, Section c)
- "*Implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated control systems, and protection measures of cryptographic keys whereby data is encrypted based on results of approved data classification and ICT risk assessment processes*" (Paragraph 4, Section d)

European Digital Identity Regulation (eIDAS 2.0)

The eIDAS Regulation creates a common framework for digital identity, electronic signatures, digital certificates, and more.

Passed in 2014 and amended in 2024, eIDAS applies to government bodies and businesses that provide online services to EU citizens, and that recognize or use identities, authentication, or signatures.

eIDAS requires that government and public commercial services recognize standard signature formats and pan-European identities. This applies to services associated with tax statements, insurance contracts, banking agreements, business-to-business (B2B) electronic invoicing, and pharmaceutical records. It also applies to commercial services that require an EU identity, for example, so-called "know your customer" services in banking. In addition, any trust services associated with these activities will be regulated by eIDAS.


TIP

To learn more about eIDAS, download your free copy of *The eIDAS (2.0) Regulation For Dummies*, Entrust Special Edition at `https://go.entrust.com/eidas-regulation-for-dummies-registration-page`.

IN THIS CHAPTER

- Explaining cryptographic agility
- Understanding why cryptographic agility matters
- Aligning people, processes, and technology

Chapter 3
Getting Up to Speed on Cryptographic Agility

In this chapter you learn about cryptographic agility — what it is, why it's important, and how to get started.

Defining Cryptographic Agility

Cryptographic agility is an attribute of a system that allows it to transition from one cryptographic system to another, by configuration or policy, without impacting all the infrastructure around it. Simply put, cryptographic agility is the ability to replace cryptography with minimal impact on applications and systems.

Unfortunately, cryptographic agility isn't simple to achieved. As noted in U.S. National Institute of Standards and Technology (NIST) Special Publication (SP) 1800-38B (draft), "Almost all information systems lack cryptographic agility — that is, they are not designed to encourage support of the rapid adoption of new cryptographic primitives and algorithms without making significant changes to the system's infrastructure. As a result, an organization may not be able to easily alter or replace its cryptographic mechanisms when needed."

Recognizing the Importance of Cryptographic Agility

Cryptographic agility isn't a new concept. Notwithstanding NIST's warning regarding cryptographic agility (discussed earlier in this chapter), organizations have been able to replace cryptographic keys with relatively minimal impact on applications or infrastructure, such as the transition from 1,024-bit to 2,048-bit Rivest-Shamir-Adleman (RSA).

Many cryptographic algorithms have remained remarkably stable and secure over time. The RSA algorithm, introduced in the 1970s, is still relied upon and continues to underpin numerous Internet standards. The other widely used public key cryptographic algorithm, Elliptic Curve Cryptography (ECC), initially being proposed in the 1980s, has been widely used for more than 20 years.

The security of RSA and ECC relies on the difficulty of solving complex mathematical problems. An important premise of this security is that brute force attacks, which attempt to guess keys, aren't feasible. As computing power has increased, this security has been maintained by increasing cryptographic key lengths.

For example, RSA keys were typically 1,024 bits long in the 1990s but are now often 4,096 bits to maintain security against modern computing power. A similar principle applies to symmetric algorithms, with key lengths and hashing algorithm digest lengths also increasing over time.

This has meant that over the last 30 years, a stable set of algorithms has been maintained by increasing security levels (that is, key lengths) without changing the underlying algorithm. However, many organizations still take considerable time to migrate to stronger algorithms.

REMEMBER

Secure Hash Algorithm (SHA)-1, first published in 1993, was quickly withdrawn and replaced after only two years. This is a reminder that cryptographic algorithms are never "one-and-done" and should always be expected to evolve. Creating this expectation of change over time can help create a cryptographic agile mindset in an organization.

Addressing People, Processes, and Technology

Understanding the different dimensions of cryptographic agility is essential for organizations aiming to enhance their security postures. These dimensions encompass people, processes, and technology (see Figure 3-1), providing a more useful organization-wide definition for cryptographic agility.

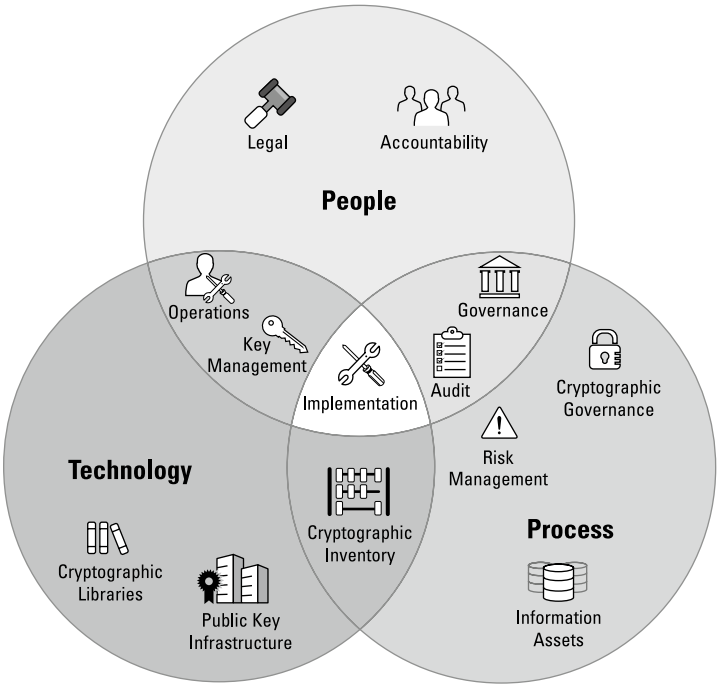

FIGURE 3-1: Cryptographic agility in relation to people, process, and technology.

People

Cryptographic agility starts with human capability and awareness. Some key elements of the people dimension include:

- **Accountability.** It all starts with accountability. Someone or some team needs to be responsible for strategy, policies, and practices covering management of cryptographic assets.

Cryptographic agility (or cryptographic management) should be part of their job descriptions.

- **Training and awareness.** IT development and operations teams need to understand cryptographic best practices, threats, and risks. Legal, compliance, and business owners need to collaborate to understand how data protection both constrains and enables the business.
- **Executive leadership.** Executives and boards own the growth strategy. They need product teams to be able to deliver more quickly while maintaining compliance. They need to understand and balance risk, and prioritize (that is, budget for) investment to develop organization-wide cryptographic agility.

REMEMBER

Even the best technology fails without informed and engaged teams.

Process

Processes provide the structure needed to manage cryptographic change systematically and repeatably. Processes are the backbone of effective cryptographic agility, informing how governance, compliance, and risk management practices influence an organization's ability to adapt to changing cryptographic needs. Some key elements in the process dimension include:

- **Policy management and governance:** Documented policies and practices for managing cryptographic assets.
- **Risk and compliance:** Cryptographic standards aligned with regulatory frameworks such as the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), NIST, and others.
- **Vendor and third-party requirements:** Disclosure of cryptographic mechanisms and support for algorithm agility.
- **Change management and incident response:** Plan for change, safely. Plan and prepare for cryptographic failures.
- **Traceability and audit:** Document and review decisions. Audit compliance.

Technology

Technology is the foundation that enables (or inhibits) cryptographic agility through system design and tooling. The following pillars represent the breadth of capability that organizations need to deploy to achieve cryptographic agility:

- **Find:** You can't fix a problem you can't see. Your technology needs to be able to provide an inventory of cryptographic assets — including keys, certificates, secrets, and cryptographic implementations — across your organization.
- **Control:** You need to be able to centrally manage policy in a dynamic way, apply those policies to the distributed points across the organizations where cryptography is used, and be able to evaluate compliance and identify risks.
- **Automate:** You need to be able to automate the life cycle of all your cryptographic assets.

REMEMBER

Cryptographic agility, when done right, isn't just about security. It's about resilience, efficiency, and business flexibility. Cryptographic agility is a business problem hiding behind a technical problem. Thus, you need to do a better job of describing the business value of cryptographic agility: Reducing risk, avoiding disruption, driving operational efficiency, delivering compliance, and enabling scalable innovation are all parts of that business value.

IN THIS CHAPTER

- Leaping forward with quantum computing
- Implementing quantum-safe cryptography
- Starting the journey to quantum-safe cryptography

Chapter 4
Preparing for Post Quantum Cryptography

In this chapter, you learn what quantum computing is and how it impacts cryptography, which algorithms have been identified as "quantum-safe," and how to start your journey to post-quantum cryptography (PQC).

What Is Quantum Computing?

Cryptographically relevant quantum computers (CRQCs, or simply, quantum computers) are on the horizon, requiring organizations everywhere to undergo a fundamental cryptographic refresh. An organization's ability to update its cryptography (that is, its cryptographic agility, discussed in Chapter 3) will be key in maintaining trust in its digital infrastructure, applications, and data security. With the advent of quantum computers, the risk increases significantly for any data protected by classic cryptography into the early 2030s.

WARNING

This U.S. National Institute of Standards and Technology (NIST) has published a draft timeline for deprecating the Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC) algorithms by 2030 and disallowing them completely by 2035.

Whereas a classical computer operates on binary code (that is, zeroes and ones), quantum computers encode data into qubits.

A qubit is a superposition of all points in between, allowing it to represent either a zero, one, or a linear combination of the two. In simple terms, applying quantum mechanics to computing allows a quantum computer to perform calculations much faster than a traditional one.

Quantum computing will usher in major changes for society — impacting everything from the automotive industry to chemistry, biology, and physics:

- **Automotive:** Quantum computers could be applied to the manufacturing process, decreasing costs and shortening cycle times by optimizing productivity.
- **Finance:** Financial institutions will be able to leverage quantum technology for advanced portfolio and risk management.
- **Artificial intelligence (AI):** Combining quantum computing with an AI and deep learning algorithm can greatly expedite data analysis, reduce training times, and optimize supply chain operations.
- **Pharmaceuticals:** Quantum computers have the potential to rapidly accelerate research and development (R&D). Moreover, they may reduce the reliance on trial and error to greatly improve R&D efficiency.

However, quantum computing is also a major threat to cryptographic systems in use today, such as public key infrastructure (PKI). With their ability to calculate at lightning speed, quantum computers will be able to crack today's standard encryption methods, which are widely used to protect sensitive data and safeguard against theft, fraud, and exploitation.

Adopting NIST PQC Standards and Guidance

PQC, also known as "quantum-resistant" or "quantum-safe" cryptography, will replace the hardware or software of the cryptographic systems currently in use, to protect data and information against a quantum attack. In essence, PQC algorithms rely on

mathematical equations — such as lattice-based or multivariate cryptography — that are believed to be too difficult for quantum computers to solve. A PQC algorithm compares measurements taken at both ends of a transmission, thereby allowing you to know if the key has been compromised.

TECHNICAL STUFF

As defined by Caltech, PQC aims to create encryption methods that can't be broken by a quantum algorithm. It uses the laws of quantum physics to transmit private data in an undetectable manner. This process is known as quantum key distribution.

NIST has facilitated the development of quantum-resistant algorithms and PQC standards through a multi-year competition. Although NIST is a U.S. institution, the competition they've been running is global.

In July 2022, NIST selected the first four PQC algorithms to standardize after several rounds of competition. The selection included one public key encryption algorithm (CRYSTALS-Kyber) and three digital signature algorithms (CRYSTALS-Dilithium, SPHINCS+, and FALCON). Since these were first announced, the algorithms have been renamed as follows:

- **CRYSTALS-Kyber:** Now Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM), Federal Information Processing Standard (FIPS) 203
- **CRYSTALS-Dilithium:** Now Module-Lattice-Based Digital Signature Standard (ML-DSA), FIPS 204
- **SPHINCS+:** Now Stateless Hash-Based Digital Signature Standard (SLH-DSA), FIPS 205
- **FALCON:** Now fast-Fourier transform (FFT) over Number Theory Research Unit (NTRU, also Number Theorists 'R' Us) Lattice-Based Digital Signature Standard (FN-DSA)

FN-DSA (FALCON) has been indefinitely shelved due to implementation and deployment difficulties. In March 2025, Hamming Quasi-Cyclic (HQC), a code-based public key encryption algorithm, was selected for standardization by NIST.

WARNING

Early PQC candidate algorithms SIKE and Rainbow were withdrawn due to weaknesses exposed as a result of cryptanalysis. You should fully expect that the current NIST PQC standard algorithms may also need refinement or even replacement as viable attacks or weaknesses are discovered.

Planning Your Journey to Quantum Safe

Finalizing the first NIST PQC standards is a significant milestone on the path to PQ readiness, but the hard work is just beginning.

Cryptographic transitions have happened before, like the move from RSA to ECC, or Secure Hash Algorithm (SHA)-1 to SHA-2. In particular, the latter shift was intended to be a simple transition, yet many organizations really struggled. It took more time than expected, required more resources, and years later, there are still some outliers. The transition to PQC promises to be much more complex and time consuming, touching every piece of cryptography and every cryptographic system. It will need to be actively managed.


TIP

Organizations need to move today's public key cryptographic systems from where they are today — using RSA and ECC algorithms — to new quantum-safe algorithms. Although that might seem simple on the surface, it's a big job entailing complete cryptographic inventories of assets and technology, mapping this to sensitive data, and developing and executing a PQC migration strategy. It's a full-scale project that will touch every piece of IT infrastructure and span several years.

IN THIS CHAPTER

- Defining cryptographic security posture management
- Establishing Root of Trust with hardware security modules (HSMs)
- Looking at the Entrust Cryptographic Security Platform

Chapter 5
Exploring Cryptographic Security Posture Management

In this chapter you learn about cryptographic security posture management, hardware security modules (HSMs) and Root of Trust, and the Entrust Cryptographic Security Platform.

What Is Cryptographic Security Posture Management?

Cryptographic security posture management continuously monitors and assesses an organization's cryptographic practices to identify vulnerabilities and ensure compliance with security policies, regulatory requirements, and industry standards.

Organizations need to prioritize cryptographic security posture management to ensure they can mitigate security, compliance, and operational risks across their entire cryptographic estate as attacks on cryptography increase and the pace of change accelerates.

Using Hardware Security Modules as a Root of Trust

Root of Trust is the foundation of security upon which your computing systems and connected mobile devices depend. It's the basis of your security system because it's where your security is rooted (as may be apparent from the name). A Root of Trust is hardened to minimize the attack surface and make it tamper resistant (or as close as possible). It can be hardware-, software-, or firmware-based and provides a set of trustworthy functions that the rest of the device or system can use to establish strong levels of security.

Root of Trust components generally include technologies like an HSM. HSMs securely generate, store, and manage cryptographic keys within a hardened, isolated environment. They ensure operations are performed within the device, preventing keys from being exposed to external threats or software attacks. HSMs are tested, validated, and certified to the highest security standards including Federal Information Processing Standards (FIPS) 140-2 and Common Criteria.

REMEMBER

Although no device is invincible, FIPS-certified HSMs are designed to resist both physical tampering and cyberattacks. They meet stringent standards for security and integrity, and breaches are very rare when properly deployed.

Root of Trust is becoming increasingly important for many different use cases, including:

- **Connected mobile devices.** Root of Trust in mobile devices poses several challenges, including a greater risk of physical attacks, multiple semi-independent processors and interfaces, and power and space constraints. Bring Your Own Device (BYOD) policies pose additional challenges in assuring that personally owned devices comply with corporate policies.
- **Public Key Infrastructure (PKI).** In PKI, Root of Trust is used to generate and protect root and certificate authority keys; to ensure software remains secure, unaltered and authentic

through code signing; and to create digital certificates and machine identities for credentialing and authenticating proprietary electronic devices for Internet of Things (IoT) applications and other network deployments.

- **Key management.** Root of Trust is a critical part of key management. As multicloud deployments become more common, organizations struggle to maintain control over their critical keys. Dispersed keys lack clear ownership or a scalable management policy.
- **IoT.** IoT devices can vary widely in terms of application and processor types, so there isn't a standard method for implementing Root of Trust with IoT. Generally, Root of Trust is secured with an HSM, but it can also be secured via software. The IoT Root of Trust helps build trust in the entire computing ecosystem by safeguarding the security of data and applications within it.

Discovering the Entrust Cryptographic Security Platform

The Entrust Cryptographic Security Platform unifies cryptographic management by combining the rich capabilities used to operate PKI, certificate lifecycle management (CLM), key and secrets management, and a strong HSM Root of Trust, all from a single, comprehensive solution.

The platform addresses the growing need for robust cryptographic asset management in an increasingly complex digital landscape. By integrating these critical components (see Figure 5-1), the Cryptographic Security Platform offers unparalleled security, compliance support, and operational efficiency for organizations dealing with securing an increasing number of machine identities, protecting sensitive data, and navigating complex cryptographic requirements.

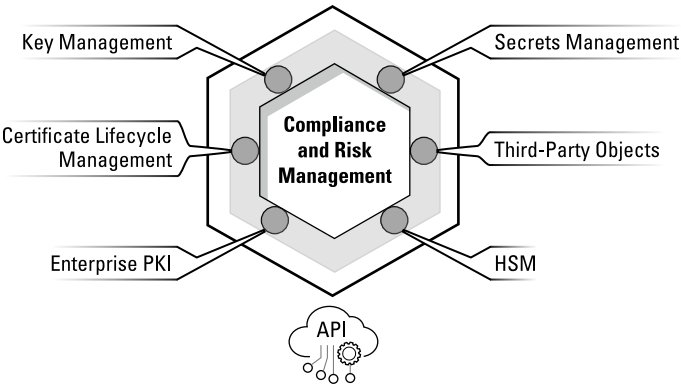

FIGURE 5-1: Core components and capabilities of the Entrust Cryptographic Security Platform.

Key features of the Entrust Cryptographic Security Platform include:

- Scalable, cost-effective, enterprise-ready key management system that supports a wide range of use cases
- Unified dashboard for fine-grained visibility of keys and secrets
- Detailed metrics to identify level of compliance and alert on prohibited key usage
- Decentralized vault-based architecture
- Full key lifecycle management
- Full high availability (HA) configuration for resilient backup and recovery
- Optional upgrade to FIPS 140-3 Level 3 Root of Trust through seamless integration with Entrust nShield HSM
- Post-quantum (PQ) ready stack of cryptographic solutions available from unified platform

Core components of the Entrust Cryptographic Security Platform include compliance management, PKI and CLM, key and secrets management, and HSMs.

Compliance management

The Compliance Manager provides a powerful compliance dashboard with granular policy management and control over the cryptographic assets across your enterprise, offering full visibility, traceability, compliance tracking, risk scoring, and an immutable audit trail of all keys and secrets. The unified dashboard allows you to view and monitor your organization's cryptographic assets in vaults configured locally or geographically distributed.

PKI and CLM

The Entrust Cryptographic Security Platform includes a comprehensive, high-performance, container-based PKI, CLM, and automation solution. It comprises all the components required to run a secure, post-quantum (PQ)-ready PKI, deploy in a range of applications, and expand on demand.

Deployed as a prepackaged virtual appliance that includes a Compliance Manager, it enables customers to streamline PKI and CLM while providing the flexibility to scale across enterprise and cloud environments.

Key and secrets management

A robust key and secret lifecycle management system with a decentralized vault-based architecture provides centralized visibility and compliance management. It ensures that management practices align with stringent regulatory and corporate requirements, enabling keys and secrets to be geolocated and managed in accordance with data sovereignty mandates.

HSMs

The inclusion of HSMs with the Cryptographic Security Platform delivers cryptographic services to applications across the network, in the cloud, and in hybrid environments. These HSMs are hardened, tamper-resistant, FIPS 140-3 Level 3 certified security appliances that perform encryption, digital signing, and key generation and protection. With their comprehensive capabilities, flexible hybrid deployments, quantum crypto-agility, and 100 percent compatibility with existing nShield HSM deployments and APIs, these HSMs can support an extensive range of applications, including certificate authorities, code signing, and

more. They also support all the National Institute of Standards and Technology (NIST) approved (PQ) algorithms.

TIP

The Entrust Cryptographic Security Platform delivers many important benefits for organizations, including:

- **Enterprise-wide cryptographic security management.** Rich capabilities to operate PKI, HSMs, and key-, certificate-, and secrets-management in a complex enterprise environment.
- **Single pane-of-glass visibility.** An intuitive dashboard provides centralized visibility of your full cryptographic estate including keys, certificates, and secrets.
- **Compliance and risk management.** Enterprise-wide compliance policy definition, enforcement, management, and reporting across your cryptographic estate.
- **Post-Quantum secure.** The combination of PKI and HSMs provides high-performance post-quantum cryptography (PQC)-certificate issuance capabilities to help future-proof your organization against the post-quantum threat.
- **Scalable architecture.** High-volume, high-performance cryptographic asset management and built-in HSM protection with unparalleled scale.
- **Interoperability.** Enable extensive integrations with top security, identity, and IT management systems while enabling customization through open application programming interfaces (APIs). Extensive partner ecosystem and protocol support enable seamless integration with your organization's existing and future infrastructure.

IN THIS CHAPTER

- Managing public key infrastructure (PKI) at scale
- Automating certificate lifecycle management (CLM)
- Establishing Root of Trust with hardware security modules (HSMs)
- Securing your keys and secrets
- Ensuring compliance
- Delivering interoperability, scalability, and automation in an enterprise solution

Chapter 6
Six Essential Components of a Cryptographic Security Platform

Here are six essential components that you need to look for in a cryptographic security platform for your organization.

Public Key Infrastructure (PKI)

The footprint of enterprise PKI deployments continues to grow as it adapts to increasingly complex use cases, becoming a central component of digital lives. However, as PKI scales and its use becomes more complex, a significant challenge emerges: the lack of clear ownership and responsibility for managing these changes.

Without visibility and understanding of how to control PKI in these new contexts, organizations struggle to maintain their security posture and infrastructure as they once did.


TIP

A complete PKI involves an integration of software, policies, and procedures that collectively establish and manage public key encryption. Look for the following PKI capabilities and features in a cryptographic security platform:

- Multi-Certificate Authority (CA) support for enterprise PKI deployments with automation of certificate lifecycle management (CLM, discussed later in this chapter) for DevOps and microservices
- Two-tier CA hierarchy for scalability and flexibility
- Dual-CA strategy to enable seamless transition from Microsoft CAs to a modern, adaptable enterprise PKI
- Support for real-time certificate validation including Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP)
- Integration with external databases and hardware security modules (HSMs) to enhance security of private keys and align with industry compliance standards
- Quantum-ready PKI with the ability to issue quantum safe certificates
- On-demand scalability

Certificate Lifecycle Management (CLM)

Automation is a key requirement for CLM to ensure seamless certificate enrollment and revocation processes, and will be absolutely necessary when making a cryptographic transition like the one to post-quantum cryptography (PQC). Having a complete CLM solution that provides full visibility into the certificate estate and enables automation is key to having control and ensuring compliance across your digital certificate estate.


TIP

Look for the following CLM capabilities and features in a cryptographic security platform:

- Certificate discovery via network scanning and automated import from CA databases and cloud services
- Centralized management of certificate policies, issuance, renewal, and revocation — regardless of CA vendor
- Ability to push certificates and manage key rotations and certificate profiles across endpoints
- Flexible certificate import methods including discovery scanner, bulk import via application programming interface (API), manual upload through user interface (UI), and source sync with CA databases
- Convenient admin controls, reporting, and notifications
- Role-based access control (RBAC) with customizable roles to help you with regulatory compliance, separation of duties, and delegation of responsibilities

Hardware Security Module (HSM)

HSMs are hardened, tamper-resistant hardware devices that secure cryptographic processes by generating, protecting, and managing keys used for encrypting and decrypting data and creating digital signatures and certificates.

HSMs are tested, validated and certified to the highest security standards including Federal Information Processing Standards (FIPS) 140-2 and Common Criteria.

HSMs enable organizations to:

- Meet and exceed established and emerging regulatory standards for cybersecurity, including the General Data Protection Regulation (GDPR), Electronic Identification, Authentication, and Trust Services (eIDAS), Payment Card Industry Data Security Standards (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), and more
- Achieve higher levels of data security and trust
- Maintain high service levels and business agility
- Support for the National Institute of Standards and Technology (NIST) approved PQC algorithms

Key and Secrets Management

As enterprises increasingly use cryptographic keys and secrets at scale to protect applications, workloads, and data, traditional key management solutions often struggle with tracking and controlling the use of keys or secrets throughout their lifecycles. These solutions also often lack advanced features that enable enterprises to deliver on their compliance mandates and security policy requirements.

TIP

Look for the following key and secrets management capabilities and features in a cryptographic security platform:

- Compliance and policy management to assess the compliance of keys, secrets, and certificates with regulations, standards, and corporate policies
- Built-in compliance policies to evaluate various key types, such as Key Management Interoperability Protocol (KMIP) keys, transparent data encryption (TDE) keys, and API keys
- Flexibility to deploy keys and secrets vaults using either a single centralized approach or a decentralized model more suited to local regulations or security posture
- Support for a range of cloud-native and DevOps integrations including Ansible, Jenkins, Datadog, Terraform, Kubernetes, Red Hat OpenShift, and VMware Tanzu
- Privileged account and session management (PASM) to secure, control, and monitor the use of privileged accounts that have access to keys and secrets
- Bring your own key (BYOK) capability for Microsoft Azure, Google Cloud Platform (GCP), Amazon Web Services (AWS), Oracle Cloud Infrastructure (OCI), and Salesforce cloud environments to maintain the creation and control of your cryptographic keys

Compliance Management

Beyond cyberthreats, an increasingly complex regulatory environment brings its own risks to businesses. Ensuring compliance with legal requirements and industry standards is challenging

when there is no centralized visibility into keys and/or keys are poorly documented.

As organizations manage an increasing number and diversity of cryptographic assets such as keys, secrets, and certificates, a consistent global strategy for managing these assets across IT infrastructure should include full visibility as well as all related information such as the owner, the usage, the history, how the cryptographic asset was generated, and for what purpose.

WARNING

Manual processes for creating and managing cryptographic assets often lead to poor key hygiene, including lack of key documentation, compliance, and key rotation, which further increases the risk of data breaches.

TECHNICAL STUFF

Look for the following compliance management capabilities and features in a cryptographic security platform:

- Key, secret, and certificate inventory across on-premises and cloud key management systems
- Support for all types of keys and secrets including (KMIP, TDE, Secure Shell (SSH), cloud and application keys, passwords, tokens, and more
- Support for public cloud services including AWS Key Management Service (KMS), Azure Key Vault, GCP, OCI, and others
- Cryptographic asset documentation workflows
- Key reporting and alerting
- Flexible deployment options including as a virtual appliance on premises or in the cloud, via a cloud-as-a-service model, or as a managed service
- High-availability support with active-active clustering
- Support for separation of duties, least privilege, dual control, and multitenancy
- Audit logs and forensic export
- Automated compliance engine for Payment Card Industry Data Security Standards (PCI DSS), NIST 800-130, NIST 800-57, and other standards plus support for customized compliance operations

Interoperability, Scalability, and Automation

Any enterprise IT or security solution needs to provide interoperability, scalability, and automation — and a cryptographic security platform is no different.

TIP

Look for a cryptographic security platform that provides the following enterprise capabilities and features:

- Extensive partner ecosystem and protocol support to enable seamless integration with your organization's existing and future infrastructure
- Scalable architecture to support high-volume, high-performance cryptographic asset management and built-in HSM protection with unparalleled scale
- Robust API support to enable seamless integrations and automation

Glossary

Advanced Encryption Standard (AES): A variant of the Rijndael block cipher selected by NIST in 2001 for the encryption of electronic data. *See also* National Institute of Standards and Technology (NIST).

application programming interface (API): A set of protocols, routines and tools used to develop and integrate applications.

asymmetric cryptography: A cryptographic system that uses two separate keys: one key to encrypt information and a different key to decrypt information. These key pairs are known as public key and private keys. *See also* public key *and* private key.

bring your own key (BYOK): The ability for an organization to generate a cryptographic key externally to the cloud platform and import it into the cloud for use, typically for a cloud-hosted application.

Certificate Authority (CA): A component of a PKI that digitally signs subscriber certificates. *See also* public key infrastructure (PKI).

Certificate Lifecycle Management (CLM): A process, usually fulfilled by a product or set of products, for managing the lifecycle of digital certificates.

Certificate Revocation List (CRL): A list of digital certificates which have been revoked by the CA before their scheduled expiration date and should no longer be trusted. *See also* Certificate Authority (CA).

continuous integration/continuous delivery (CI/CD): A DevOps environment supported by automation such that changes to application source code and infrastructure configuration are built, integrated, and deployed automatically. *See also* DevOps.

Common Criteria: An international initiative to standardize and improve existing European an North American information systems security evaluation criteria.

Cryptanalytically (or Cryptographically) Relevant Quantum Computer (CRQC): A quantum computer with sufficient scale to implement algorithms (such as Grover's or Shor's) that break or weaken classic cryptographic algorithms. Both terms mean the same thing and are used interchangeably in industry and government publications.

cryptographic agility: The ability to easily replace cryptographic algorithms with minimal impact on business applications.

cryptographic security posture management: The continuous monitoring and assessment of an organization's cryptographic practices to identify vulnerabilities and ensure compliance with security policies, regulatory requirements, and industry standards.

DevOps: The culture and practice of improved collaboration between software developers and IT operations.

digital certificate: An electronic file containing a public key along with information about the subject of the certificate, validity dates, and the security functions it should be used for. Digital certificates are digitally signed by a CA and typically comply with the X.509 standard defined by the International Telecommunication Union (ITU). *See also* Certificate Authority (CA).

Digital Operational Resilience Act (DORA): A European Union (EU) regulation that targets how financial institutions and their information and communication technology (ICT) partners manage cyber risk. It creates a binding oversight framework and establishes technical standards that EU financial entities and their service providers must implement in their ICT systems.

Electronic Identification, Authentication, and Trust Services (eIDAS): A European Union (EU) regulation developed to help establish a single European market for secure electronic commerce.

Elliptic Curve Cryptography (ECC): A class of classical asymmetric algorithms, ECC is an alternative technique to RSA. It generates security between key pairs for public key encryption by using the mathematics of elliptic curves. *See also* asymmetric cryptography *and* Rivest-Shamir-Adleman (RSA).

Federal Information Processing Standards (FIPS): Standards and guidelines published by NIST for federal computer systems. *See also* National Institute of Standards and Technology (NIST).

Federal Information Security Modernization Act (FISMA): Federal legislation that defines a framework of guidelines and security standards to protect government information and operations.

General Data Protection Regulation (GDPR): A law that strengthens data protection for European Union (EU) residents and addresses the export of personal data outside the EU.

hardware security module (HSM): A physical hardware appliance that secures the generation and use of cryptographic keys, ensuring that the plaintext version of the key is never accessible outside its secure environment. HSMs have a hardware entropy source, providing high-quality random numbers for cryptographic key generation.

Health Insurance Portability and Accountability Act (HIPAA): A U.S. federal act that addresses security and privacy requirements for medical systems and information.

Hypertext Transfer Protocol Secure (HTTP/S): HTTP is an application protocol used to transfer data between web servers and web browsers. HTTPS is an encrypted version of HTTP that uses SSL or TLS encryption to secure data in transit. *See also* Secure Sockets Layer (SSL) *and* Transport Layer Security (TLS).

identity and access management (IAM): The processes and procedures that support the lifecycle of identities and access privileges.

Key Management Interoperability Protocol (KMIP): An extensible communication protocol that defines message formats for the manipulation of cryptographic keys on a key management server.

National Institute of Standards and Technology (NIST): A U.S. government body within the Department of Commerce, responsible for working with industry and academia to define and approve a wide range of standards, including cryptographic algorithms such as AES and the ongoing PQC standardization process. *See also* Advanced Encryption Standard (AES) *and* post-quantum cryptography (PQC).

Online Certificate Status Protocol (OCSP): An alternative protocol created as an alternative to CRLs, used to determine the revocation status of digital certificates. *See also* Certificate Revocation List (CRL).

one-way hash function: An algorithm that takes an input of any length and produces a hash of fixed length, serving as a digital fingerprint of the input data. Any modification to the input data would result in a different hash value. SHA-2 is an example of a family of hashing algorithms. *See also* Secure Hash Algorithm (SHA).

Payment Card Industry Data Security Standards (PCI DSS): An industry standard that mandates compliance for businesses that handle payment card transactions (such as debit cards and credit cards) and is enforced by the payment card brands (American Express, MasterCard, Visa, and so on).

Personally identifiable information (PII): Information (such as name, address, Social Security number, birthdate, place of employment, and so on) that can be used on its own or with other information to identify, contact, or locate a person.

Policy Authority (PA): A body within an organization, also known as a policy management authority, that is responsible for defining and publishing cryptographic policy documentation, including a certificate policy and certificate practice statement. This role is commonly performed by an existing body responsible for defining IT security policies and comprised of members from IT security, compliance, and/or risk functions.

post-quantum cryptography (PQC): Cryptographic algorithms that are resistant to both classic and quantum computers.

private key: A secret cryptographic key that must be exchanged between parties to securely communicate in symmetric cryptography. *See also* symmetric cryptography.

Privileged Account and Session Management (PASM): An identity security solution that focuses on securely managing and monitoring accounts with elevated access rights.

public key cryptography: A cryptographic system leveraging key pairs — a public key and an associated private key — eliminating the need to distribute a shared key to both parties in a secure electronic transaction. RSA and ECC are examples of public key cryptographic systems. *See also* private key, Rivest-Shamir-Adleman (RSA), *and* Elliptic Curve Cryptography (ECC).

public key infrastructure (PKI): A collection of processes and technologies used to manage digital certificates and keys, allowing relying parties to trust digital transactions.

quantum computing: In quantum computing information is encoded as qubits and quantum mechanical properties are used to make calculations on data that are essentially impossible for conventional computers. *See also* qubit.

qubit: The basic unit of information in quantum computing, similar to a bit in classical computing. Unlike a classical bit that can be either 0 or 1, a qubit can exist in a superposition of both states simultaneously, allowing for more complex computations. *See also* quantum computing.

Registration Authority (RA): The RA is composed of hardware, software, and the personnel administering the PKI. It's responsible for verifying certificate contents of the CA. *See also* Public Key Infrastructure (PKI) *and* Certificate Authority (CA).

repository: In a PKI, a repository is a system that accesses certificates and CRLs from a CA and distributes them to authorized parties. *See also* Public Key Infrastructure (PKI), Certificate Revocation List (CRL), *and* Certificate Authority (CA).

Rivest-Shamir-Adleman (RSA): A key transport algorithm based on the difficulty of factoring a number that's the product of two large prime numbers.

Root of Trust: A source that is trusted by default within a cryptographic system. The most secure implementation of Root of Trust typically includes an HSM, which generates and protects keys and performs cryptographic functions within a secure environment. *See also* hardware security module (HSM).

Secure Hash Algorithm (SHA): A family of one-way hash functions designed by the U.S. National Security Agency (NSA) and published by NIST. *See also* one-way hash function *and* National Institute of Standards and Technology (NIST).

Secure Shell (SSH): A network protocol used to securely access and manage remote computers over a network. SSH uses encryption to protect data in transit and is commonly used for remote login and command execution

Secure Sockets Layer (SSL): A deprecated Transport Layer protocol that provides session-based encryption and authentication for secure communication between clients and servers on the Internet. *See also* Transport Layer Security (TLS).

symmetric cryptography: A cryptographic system in which both parties to an electronic transaction require a copy of a shared (secret) key. AES is an example of a symmetric cryptographic system. *See also* Advanced Encryption Standard (AES).

transparent data encryption (TDE): A technology used to encrypt databases at the file level. TDE protects data at rest, but it does not protect data in transit or data in use.

Transport Layer Security (TLS): A Transport Layer protocol that provides session-based encryption and authentication for secure communication between clients and servers on the Internet.

Validation Authority (VA): In PKI, a VA is an entity that provides a service used to verify the validity of a digital certificate. *See also* Public Key Infrastructure.

zero trust: A strategy designed to mitigate cyberattacks by eliminating the assumption of implicit trust within digital systems. It is built around the principles of verify explicitly, least privilege access, and assume breach.

About the Author

Lawrence Miller served as a Chief Petty Officer in the U.S. Navy and has worked in information technology in various industries for more than 25 years. He is the co-author of CISSP For Dummies and has written more than 300 For Dummies books on numerous technology and security topics.

Get ready for the future with crypto agility

Organizations' environments have become more complex as the digitization of all corners of business is leading to an explosion of data and devices that need to be secured — and that is done with cryptography. More things to secure means more credentials — such as keys, certificates, and secrets — to manage. In this guide, you'll learn about the many challenges driving crypto criticality, the need for crypto agility, how to prepare for post-quantum cryptography, and how a cryptographic security posture management solution can help your organization.

Inside...

- Understand different crypto types
- Implement zero trust
- Explore industry use cases
- Address compliance mandates
- Plan your journey to quantum safe
- Discover cryptographic security posture management

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-394-37418-2
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.