WHITE PAPER

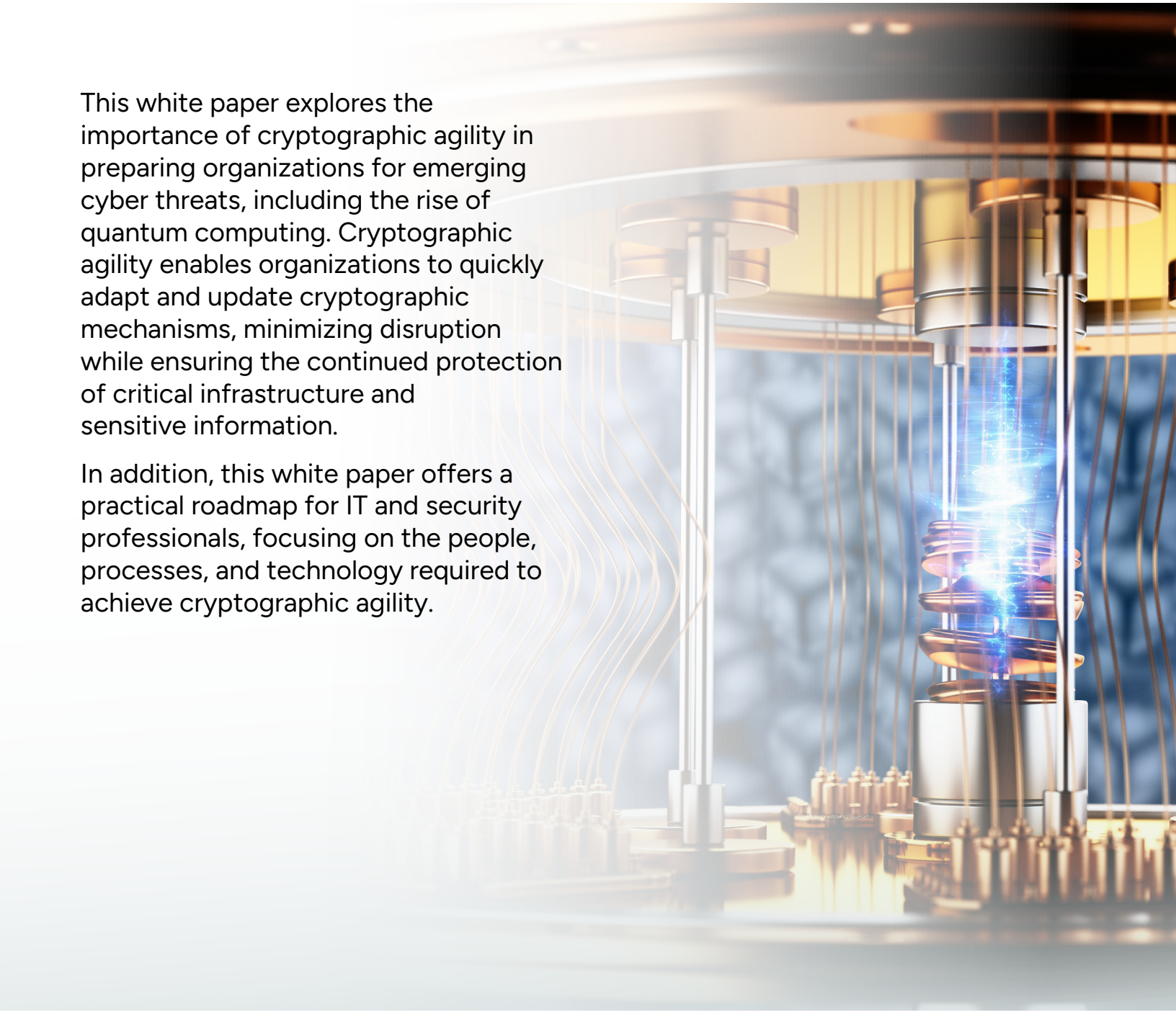
Organizational Cryptographic Agility

ENTRUST
SECURING A WORLD IN MOTION

Abstract:

This white paper explores the importance of cryptographic agility in preparing organizations for emerging cyber threats, including the rise of quantum computing. Cryptographic agility enables organizations to quickly adapt and update cryptographic mechanisms, minimizing disruption while ensuring the continued protection of critical infrastructure and sensitive information.

In addition, this white paper offers a practical roadmap for IT and security professionals, focusing on the people, processes, and technology required to achieve cryptographic agility.



Contents

Introduction

Cryptography secures the digital world in which we live and work, facilitating digital transformation by reducing risk. Every time you use mobile banking, purchase a product or service online, or send a message from your mobile device, cryptography is used to secure your transaction. However, the threat landscape is evolving, and cyberattacks are becoming more prevalent and sophisticated.

Threat actors, whether from state-sponsored organizations and hacking groups or insiders with malicious or ideological motives, are increasingly targeting organizations. In response, organizations, industries, and governments are prioritizing robust measures to protect organizational and customer data. Resilience to attacks and the ability to recover, particularly for critical infrastructure, are top of mind for many governments. Resisting these attacks and protecting governments, critical infrastructure, and organizations' data motivates enterprises to keep their cryptography up to date. In addition, ongoing developments in computing speed and architectures require cryptographic updates to remain effective.

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. Cryptography underpins the authentication of devices, applications, and users within such frameworks.

Cryptographic agility – the ability to replace cryptography with minimal impact on applications and systems – has been required for decades. Yet replacing weak cryptography is not always achieved successfully even for relatively simple changes. As noted in NIST Special Publication 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."

With the impending development of cryptanalytically relevant quantum computers (CRQCs), also sometimes written as cryptographically relevant quantum computers, a fundamental cryptographic refresh will be required. An organization's ability to update its cryptography will be key in maintaining trust in its digital infrastructure, applications, and data security.

This paper examines the requirements for cryptographic agility, and explores the people, process, and technology aspects organizations should consider as they measure their current state of maturity and build roadmaps for improvement.

Target Audience

This paper is suitable for any IT/information security and compliance/risk professional or practitioner interested in maintaining a strong information security posture to effectively manage risk over time. Understanding the implementation of cryptographic algorithms is not required.

Scope

This paper serves as a practical guide to achieving and maintaining cryptographic agility at the organizational level, encompassing the people, processes, and technology involved.

The Role of Cryptography

Cryptography is, in many senses, a critical component of our digital infrastructure. Over time, it 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.

The pervasive nature of cryptography impacts multiple stakeholders. For risk and compliance officers, cryptography mitigates risks associated with internet-based business processes. IT security teams are responsible for implementing cryptography and integrating it into business systems. Application developers must architect security from the start of new applications and update algorithms over time. Users, while shielded from any complexity introduced using cryptography, should still be trained to recognize security check failures, such as visiting untrusted websites. As perimeter security controls are no longer sufficient to protect corporate IT assets, the value of Zero Trust principles has gained widespread recognition. Zero Trust assumes the network is breached and requires verification of the identity and authorization of any person, system, or device requesting access to IT resources – ideally for each request and as close to the resource as possible. This authentication often leverages public key cryptography, especially for requests from applications and devices. In this sense, the cryptography underlying this identitycentric security represents a critical link in the Zero Trust chain.

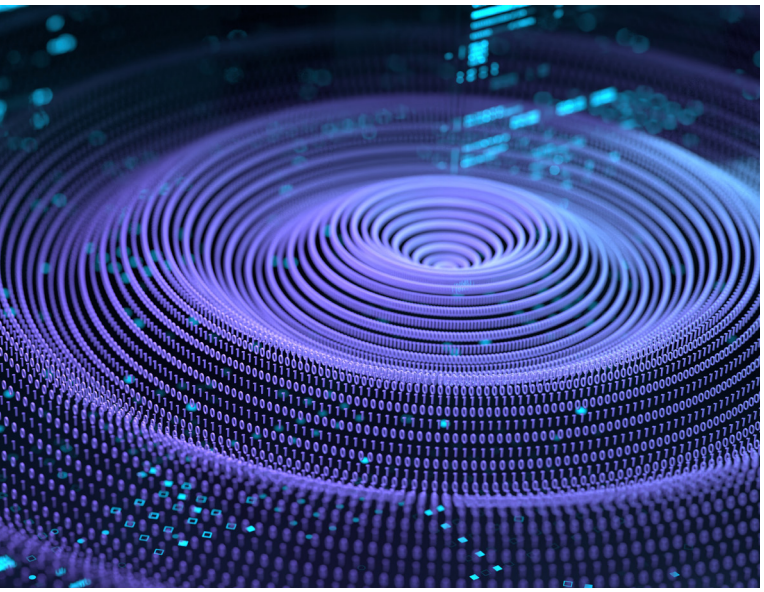
The below quote from CISA resonates well with cryptoagility, recognizing the need for security policies that evolve alongside algorithms. This paper refers to this as a focus on people, processes, and technology, emphasizing their importance in an organization's security philosophy and culture.

> This shift provides the visibility needed to support the development, implementation, enforcement, and evolution of security policies. Fundamentally, zero trust may require a change in an organization's cybersecurity philosophy and culture.
>
> **CISA ZERO TRUST MATURITY MODEL**

The Need for Cryptographic Agility

Over the last 30 years, since the introduction and ubiquitous adoption of the internet, cryptography has remained remarkably stable. The Rivest- Shamir-Adleman (RSA) algorithm, invented in the 1970s, is still relied upon and continues to underpin numerous internet standards almost 50 years since it was introduced. The other widely used public key cryptographic algorithm, elliptic curve cryptography (ECC), has been widely used for 20 years after initially being proposed in the 1980s.

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, are not feasible. As computing power has increased, we've been able to maintain this security 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, we have largely been able to rely on a stable set of algorithms by increasing security levels (e.g., key lengths) without changing the underlying model.



Cryptographic Agility is Not New

Cryptographic agility has been around for decades. Organizations have been able to replace cryptographic algorithms with minimal impact on applications or infrastructure. Typically, newer, stronger algorithms share similar properties with those being replaced, such as the transition from the 1,024-bit RSA algorithm to the 2,048-bit version. However, some organizations still take a considerable length of time to migrate to stronger algorithms, perhaps best exemplified by the SHA-1 secure hashing algorithm migration to SHA-2.

Never One and Done

SHA-1 (often referred to as SHA-0), 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 inform a crypto-agile mindset in an organization. Reflecting on NIST's postquantum cryptography (PQC) algorithm selection process, where candidate algorithms SIKE and Rainbow were withdrawn due to weaknesses exposed as a result of cryptoanalysis. With the first batch of NIST PQC algorithms now standardized, we should fully expect that these may also need refinement or even replacement as viable attacks or weaknesses are discovered.

Migrating Algorithms Takes Time

SHA-1 (often referred to as SHA-0), 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 inform a crypto-agile mindset in an organization. Reflecting on NIST's postquantum cryptography (PQC) algorithm selection process, where candidate algorithms SIKE and Rainbow were withdrawn due to weaknesses exposed as a result of cryptoanalysis. With the first batch of NIST PQC algorithms now standardized, we should fully expect that these may also need refinement or even replacement as viable attacks or weaknesses are discovered.

Preparing for Post-Quantum Cryptography

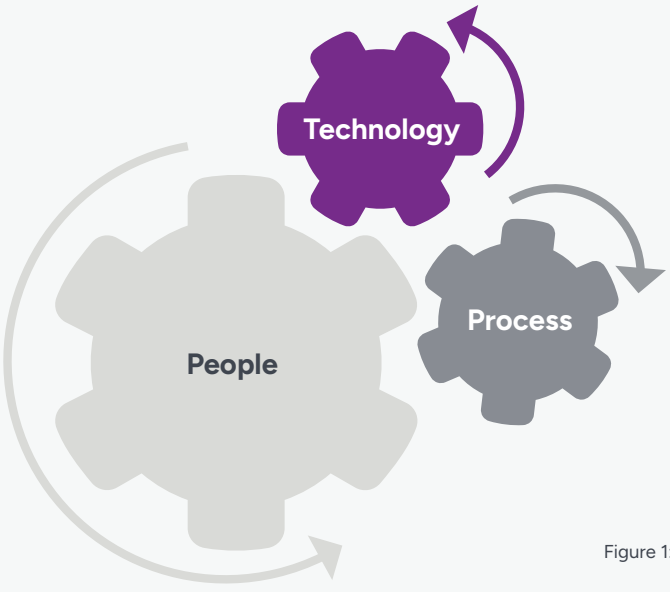
Information security and compliance/risk practitioners are set to face one of the most significant disruptive forces of their careers: quantum computing. Advancements in quantum technology are expected to produce a cryptographically relevant quantum computer (CRQC) within the next decade. This shifts the risk landscape. Our current working assumption is that the risk of compromise of any encrypted data is negligible for the next 20 years (based on a brute force attack using "conventional computers" evolving to Moore's Law). However, with the advent of quantum computers, the risk increases significantly for any data protected by classic cryptography into the early 2030s. Therefore, we now need a plan to mitigate those risks for any sensitive data with a lifetime extending beyond the current decade.

> "Organizations should make the migration to post-quantum cryptography (PQC) about lifecycle management, not crisis management.
>
> **MICHELE MOSCA, CO-FOUNDER OF THE INSTITUTE FOR QUANTUM COMPUTING, UNIVERSITY OF WATERLOO**

Governments and national security agencies strongly recommend initiating efforts now toward the migration of cryptographic systems to post-quantum cryptography. NIST has clearly drawn a line in the sand with their **Transition to Post-Quantum Cryptography Standards**, which specifies that classical algorithms such as RSA and Elliptic Curve will be disallowed by 2035. This information in combination with the new PQC algorithms published by NIST means there are no excuses preventing organizations developing their migration plan to post-quantum cryptography.

Elements of Cryptographic Agility

To maintain appropriate risk mitigation using cryptography, we need to remain agile. But how should we measure cryptographic agility at an organizational level? The factors that may facilitate or inhibit our agility can be categorized into process, people, and technology. These elements are interconnected, much like the "gears of a machine" as illustrated below.



Process - how governance, compliance, policies, processes, and procedures influence cryptographic agility

People - role that people play in an organization's cryptographic agility

Technology - the influence and importance of technology on cryptographic agility

Figure 1: Crypto-agility requires the meshing of Process, People, and Technology

Organizations need to take a holistic approach to agility to maximize success. While these gears inevitably mesh, each must be considered to successfully explore cryptographic agility. This paper will further investigate each of these gears in detail, while also considering the interplay of people, process, and technology, which influence crypto-agility as illustrated below.

Figure 2: Venn diagram illustrating crypto-agility attributes in relation to People, Process, and Technology

Process

Process informs how governance, compliance, policies, processes, and procedures influence cryptographic agility.

Governance

Effective governance is the essential first step on the path to gaining control, and therefore agility, of your cryptographic estate. Governance addresses what policies and processes are adopted to manage risk associated with information assets.

For many organizations, cryptography is not treated as critical infrastructure. Many on-premises and cloud applications are deployed without an analysis of the embedded cryptography. Organizations accumulate a heterogeneous environment of cryptographic artifacts, including algorithms and keys, which ultimately protect sensitive data and transactions.

Certificate authorities (CAs) are deployed by business units often with little oversight. A CA is a system that issues digital credentials automatically trusted by infrastructure and applications. Such systems require strong governance to ensure they are used appropriately and deliberately. Understanding what digital certificates are being used for and what data and transactions they are protecting is essential.

Cryptography is decentralized. While an IT security department can deliver (and mandate use of) services providing a trust fabric through CAs and key management systems, the actual cryptographic functions happen within business applications. It is therefore critical to maintain centrally defined policies dictating approved cryptographic standards and systems for use within the organization.

Accountability for cryptographic maintenance should be shared between IT security teams and business unit IT teams who manage the applications that use central cryptographic services (such as PKI) and embed cryptographic implementations. One reason the SHA-2 migration took so long was the lack of clearly defined policies and organizational accountability for compliance.

Effective governance determines:

- Data Protection: What types of data must be protected by cryptography, both in transit and at rest
- Algorithm and System Selection: What cryptographic algorithms and key management systems apply for each classification of data, documented in a cryptographic policy
- System Updates: How new cryptographic systems are introduced and existing ones are updated to prevent the proliferation of disparate cryptographic systems that inhibit cryptographic agility. Cryptographic requirements should be referenced within agreements with suppliers of products and cloud services
- PKI Management: Documenting the use of certificates in a certificate policy (CP) and managing certificate authority in accordance with a published certificate practice statement (CPS)

The governance body, known as the Policy Authority (PA), is responsible for defining cryptographic policy within an organization. Below are some of the questions addressing areas that would be in scope of an audit related to the management of cryptographic assets.

- How do you know if you are compliant with corporate security and data protection policies?
- Where are your keys and secrets being stored?
- Are you following industry best practices when managing keys and secrets?
- Who created this key?
- Who has permissions to access those keys?
- How do you know these keys cannot be exported to another country, violating data sovereignty mandates?
- What data or workload are the keys being used to protect?
- Do we have any critical high-value keys that require hardware protection?
- Do we have granular documentation with an accurate audit trail of your keys and secrets?
- What type of key and security strength is specified?
- Why is this key being used in a production environment when it was created solely for test purposes?
- When do the keys need to be rotated/retired?

Figure 4 - Can you answer these questions on behalf of your organization?

Catalog Information Assets

Cataloging information assets is a crucial practice in information security. It involves recognizing the value of various assets within an organization and systematically organizing them to enhance security measures. It is only possible to determine the adequacy of cryptography if we know the type of data that it protects. It is therefore critical that we understand our data.

Such metadata is essential to achieve effective risk management. The lifetime of the data, for instance, helps inform the strength of cryptography required to protect that data through its lifetime, and highlights data affected by the threat of CRQCs. In regulated industries and the public sector, certain types of data require cryptographic protection, such as cardholder data under PCI DSS or personally identifiable information (PII) under the General Data Protection Regulation (GDPR).

> “Most IT organizations are not aware of the type of encryption they are using – including which applications are using it, how it is used, or who makes decisions about cryptography.” – Gartner, Preparing for the Quantum World with Crypto-Agility, September 2022.

Process – Attributes & Recommended Actions		
	Description	**Recommendation**
Governance	The corporate Compliance Officer should be aware of the role that cryptography plays in managing risks related to information assets and IT systems security. A Policy Authority (PA) should be established with overall accountability for policy relating to cryptography and PKI standards throughout the organization. The PA should have jurisdiction across lines of business for consistency and to avoid duplication or ambiguity regarding responsibility for cryptographic policy.	Establish an accountable Policy Authority with appropriate terms of reference. This would typically be a cross-business and multiskilled body that already meets regularly, is suitably empowered, and includes a remit for a longer-term roadmap against emerging threats.
Risk Management	Information security and cryptography exist to manage risk. The compliance and risk teams are therefore key stakeholders in the process of managing risk associated with IT systems.	The organization’s Compliance Officer should ensure risks associated with cryptographic protection of corporate information assets are recorded on the appropriate register.
Policies and Processes	Documented Cryptographic Policy	To ensure secure and consistent use of cryptographic systems, clear guidelines are needed. Policies and procedures on the use of cryptography should be documented. This should include cryptographic and key management policies, as well as certificate policy and certificate practice statements for PKI systems. Policies should be clear on the uses of cryptography to deliver confidentiality, integrity, and authentication within digital systems.
Information Assets	It is only possible to determine the adequacy of cryptography if we know the type of data that it protects. It is therefore critical that we understand our data.	Establish and maintain inventory metadata on information assets including: • Sensitivity of data (e.g., PII, intellectual property) • Impact of loss of data (availability impact) • Impact of breach of data (confidentiality impact) • Lifetime of data (map to cryptographic policy for appropriate protection level) • Applicable regulations for protection of data (e.g., GDPR, PCI DSS, etc.)

Technology

This section examines the influence and importance of technology on cryptographic agility. This includes having a documented cryptographic architecture, an inventory of cryptographic artifacts and protected data, cryptographic refresh, and rationalization of cryptographic implementations.

Cryptographic Inventory

While establishing a Policy Authority and publishing guidelines is an essential starting point, compliance should be audited regularly. Cryptography is often introduced into organizations with new IT systems, whether on-premises, hardware or software, or cloudbased. It is important to maintain an inventory of cryptographic assets across the organization, as well as ensure that it meets corporate policies.

Cryptographic agility requires us to be able to update our cryptography with minimal impact on business systems. This is only achievable if we know what cryptographic assets exist in the estate. Ensuring that business applications comply with policies and leverage the organization's PKI and key management systems facilitates cryptographic agility.

It is unlikely that a single tool will be effective at managing all cryptographic assets within an organization. It may be possible to leverage existing tools that manage software inventory or scan for general vulnerabilities to address this requirement, at least in part.

Organizations should ensure they are able to inventory different types of cryptographic artifacts, including:

	Cryptographic Artifact Location	Example of Cryptographic Artifact
	Discoverable remotely	Includes web server digital certificates that can be monitored using network scanners
	Discoverable locally	Includes digital certificate and cryptographic keys stored on servers, which can be monitored using local software to scan local key stores and application binaries
	Cryptographic artifacts monitored manually	Could apply to offline or air-gapped systems, or IoT environments where scanning is not possible

Industry efforts, particularly in the public sector and regulated industries such as financial services, are focusing on acquiring tools to discover cryptographic artifacts and formalizing cryptographic inventory into a Cryptographic Bill of Materials (**see IBM's Cryptography Bill of Materials to speed up quantum-safe assessment | IBM Research Blog**).

Key Management

While cryptographic libraries are built into products and services, it is often possible to abstract key management away from applications. This allows keys to be managed independently of cloud-based infrastructure and applications. Protocols such as Key Management Interoperability Protocol (KMIP), along with cloud providers' Bring Your Own Key (BYOK) and Hold Your Own Key (HYOK) functionalities, give flexibility for how organizations can manage cryptographic keys. Deploying a key management system (KMS) can significantly enhance cryptographic agility, allowing easier key management and automation and enforcing compliance with cryptographic policies.

Additionally, a KMS should allow the most sensitive keys to be managed within hardware security modules (HSMs) for enhanced protection. Referencing Zero Trust principles, if we assume that an attacker has access to our corporate network and IT systems, we should ensure they cannot read our most sensitive keys such as certificate authority signing keys from the memory of our machines.

Reporting compliance against evolving key management policies can prove difficult in complex organizations, given that keys reside within disparate systems. Keys are often distributed across different geographic regions in order to comply with local data sovereignty requirements. Where possible, a high-level compliance capability should be deployed to report on compliance posture across an organization, while allowing keys to be managed within distinct vaults. This ability to audit key usage across an organization, including operational management of metadata associated with keys, will enhance cryptographic agility.

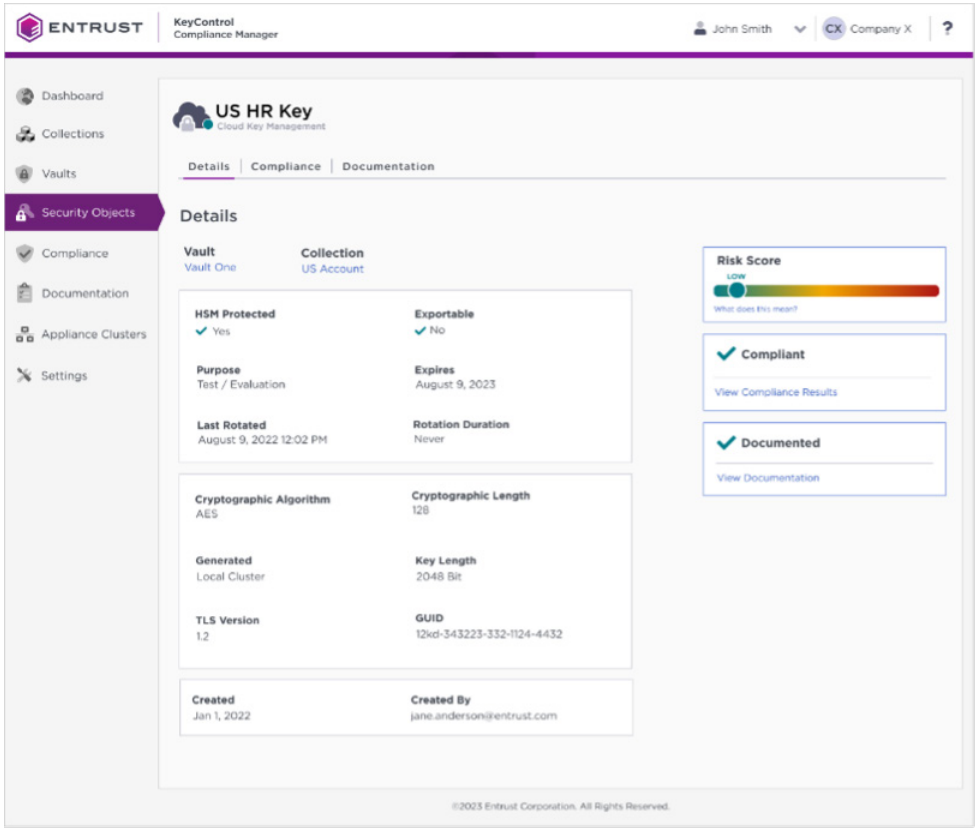


Figure 5: Screenshot of Entrust KeyControl key management solution, which creates a granular inventory of keys, secrets, and certificates

Certificate Management

Since the late 1990s, almost all organizations have deployed certificate authorities (CAs) to issue digital credentials to users, devices, and applications, supporting authentication, integrity, and confidentiality for data in transit and at rest. While we've already discussed the need for a published policy documentation set associated with a PKI in our discussion of process, there is also a significant technology aspect to cryptographic agility.

All too often, CAs are deployed tactically within business units and are managed manually by an individual or small group, without formal documentation or procedures. Certificate issuance may be manual, and tracking certificate expiry is performed using spreadsheets. Publicly trusted certificates for internetfacing web services are procured from a variety of CAs, with no consolidation of suppliers.

Many "core" PKI use cases leverage mainstream commercial software or cloud services. In these cases, organizations should engage with suppliers regarding roadmaps with a view to implementing updates and benefit from cryptographic refresh cycles. Note that vendors typically support a selection of cryptographic algorithms to maintain backward compatibility, but it will be the responsibility of each organization to configure their systems to use secure algorithms and keys appropriately.

There are also "specialized" PKI use cases for which organizations will need to take greater responsibility for cryptographic agility. These may relate to legacy systems or to bespoke applications. The figure below illustrates the concept of "core" versus "specialized" use cases and presents examples of each. Organizations will need to categorize their various use cases of PKI to determine the appropriate approach to cryptographic agility.

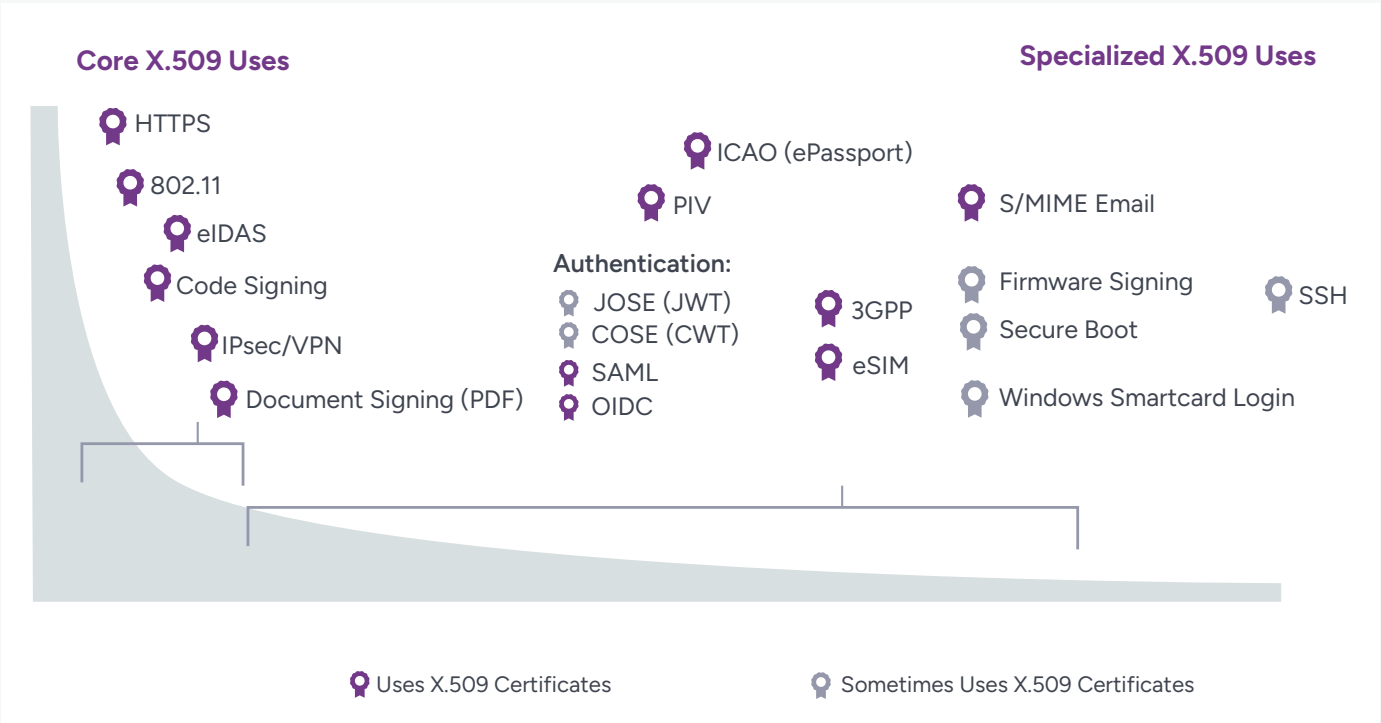


Figure 6: The long tail of X.509 Digital Certificate Usage

Cryptographic Libraries

As mentioned earlier, cryptographic implementations are embedded into the devices, platforms, and applications that support digital business. Such cryptographic libraries may be difficult to inventory, and even more difficult to replace. In-house developed applications should leverage centrally administered key management systems to decouple applications from cryptography to the greatest extent possible. It is important to consider cryptographic agility of thirdparty applications to assess ease of crypto replacement – whether it requires a new version from the vendor, a patch, or a full product replacement.

Automation

Digital certificate lifetimes are shortening due to policy changes within the CA/Browser Forum, and the quantum threat to cryptography will also drive this trend. Automation of certificate issuance and update is therefore required not only for agility but also for efficiency and cost management purposes.

In the realm of security operations, automation plays a pivotal role. Security teams can leverage tools and scripts to automate repetitive tasks such as log analysis, incident response, and vulnerability scanning. This trend toward automation should extend to key and certificate lifecycle management, using solutions that support key and certificate management protocols compatible with commercial off-the-shelf applications, such as KMIP, WSTEP, and CMPv2. To support integration with CI/CD processes, RESTful APIs can be consumed with Ansible playbooks or PowerShell scripts to automate certificate issuance.

Technology – Attributes & Recommended Actions

	Description	Recommendation
Cryptographic Inventory	There should be a clear and documented association between organizational data and the keys and cryptography protecting that data. It is strongly recommended that tools be deployed to automatically discover and inventory cryptographic assets where possible.	Consider deploying systems/tools to discover and manage an inventory of cryptographic assets, mapping them to the sensitivity and lifetime of protected data assets. This could entail leveraging currently deployed asset management tools, such as Tanium or ServiceNow, or procuring new products, such as Entrust KeyControl, to manage keys, secrets, and certificates. It may not be practical to automate discovery of all keys, and manual processes may also need to be supported.
Key Management	Key management systems should support centralized compliance dashboards across geographies and business units, even when keys are distributed. Key management systems should manage metadata bound to cryptographic keys, including details of the owners of keys, and the types of data protected by the key. For example, it is important to know if a key protects Test or Live data, as this could determine the key rotation policy or key length.	Consider deploying a key management platform that supports centralized visibility and auditing across the organization. It should also maintain compliance with data sovereignty regulations, which dictate where cryptographic assets are stored.
Certificate Management	Cryptographic agility is enhanced if we can easily report on and update certificates.	Recommend deploying a certificate lifecycle management (CLM) capability. This typically includes a certificate discovery and reporting engine to present a single pane of glass through which to view details of issued digital certificates. A CLM solution should meet the needs of operational and audit stakeholders.
Cryptographic Libraries	The existence of out-of-date IT inhibits the update of cryptographic algorithms. For example, if an old desktop operating system is still in use, it could prevent an organization from moving away from a weak algorithm to maintain compatibility.	Follow best practices and maintain up-to-date software versions to eliminate security vulnerabilities. This is also essential for maintaining up-to-date cryptographic standards. Where legacy systems have no upgrade path to maintain security, plan for mitigation or migration.
Automation	Automating the issuance and update of keys and certificates allows key material to be updated quickly and at low cost, supporting cryptographic agility.	Manual operations inhibit cryptographic agility. Many use cases of cryptography support automation of issuance and update of keys and certificates. These should be leveraged to reduce operational cost and enhance agility.
Hardware Protection	Cryptographic keys protect organizations' data. But when stored in software, they are vulnerable to malware, which could compromise data confidentiality and access to IT systems.	Ensure your organization's most sensitive keys are managed within accredited hardware security modules (HSMs) for enhanced protection.Ensure your organization's most sensitive keys are managed within accredited hardware security modules (HSMs) for enhanced protection.

People

This section considers the role people play in an organization's cryptographic agility, including executive sponsorship, defined roles and responsibilities, training, vetting, and audit functions.

In any sphere, agility requires coordination, and cryptography is no different. From governance to audit, and implementation to operations, it is essential to consider the role of people.

Accountability

While there may be ownership of centralized services such as PKI and key management, cryptographic assets – including libraries and keys – are typically distributed across IT systems and lines of business. This distribution can inhibit cryptographic agility through lack of accountability in implementing required steps.

Therefore, the first action organizations should take is to assign clear ownership and accountability for initial activities relating to cryptographic agility. This was the first step taken by the U.S. federal government in memorandum M-23-02, which required departments to assign a lead for cryptographic inventory and migration.

The need to implement cryptographic agility to maintain effectiveness of information security risks should be visible at the CxO level within an organization. The individual or body responsible for driving improvements in cryptographic agility should be supported and empowered with the appropriate level of authority and funding.

Audit

To maintain the effectiveness of cryptography, it is important to audit compliance with organizational policies and procedures over time. It is all too easy to "drift away" from best practices to gain efficiencies, which can undermine security posture. Many cryptographic operations should be formally audited as required by policy.

Establishing regular audits of cryptographic policies and procedures is essential for maintaining effective security controls. The audit team may require training on the role of cryptography in protecting corporate information assets, including understanding policies and procedures. The audit team should also be a stakeholder in enterprise key management systems to evaluate compliance with these policies. Below is an example of a key management compliance dashboard that would be appropriate for an audit role.

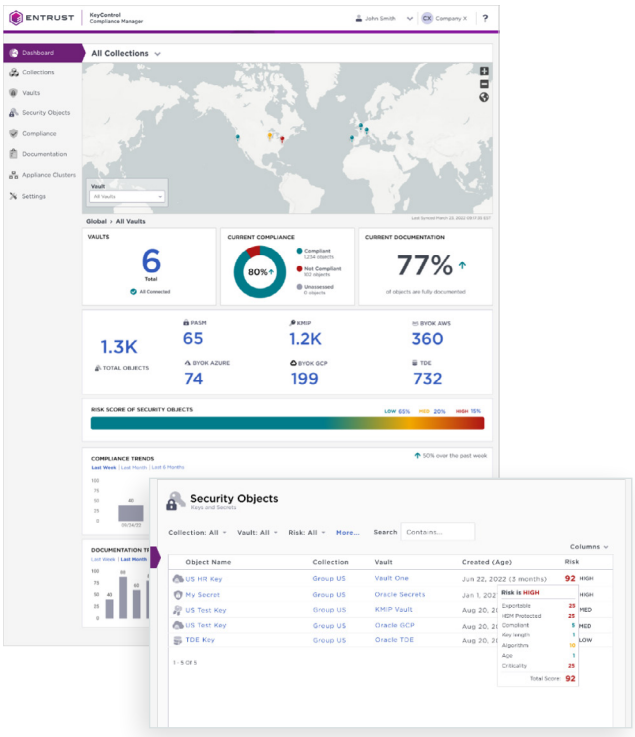


Figure 7: Screenshots of the Entrust KeyControl compliance dashboard show how compliance officers/auditors can gain complete visibility into an organization's cryptographic inventory. This tool allows them to view granular details of specific cryptographic assets per vault and determine the overall level of risk and compliance.

Implementation

In-house developers should be trained on cryptographic standards to ensure proper adoption. This training should include education on the correct implementation of cryptography within applications. Integration with enterprise key management and PKI systems, as well as the automation of certificate and key lifecycle management, should be mandatory requirements.

Additionally, development teams should be educated on organizational policies related to cryptography, including designing with cryptographic agility in mind.

Operations

Cryptography is not static. Operations teams should be enabled with up-to-date information on standards and best practices. While it should be a design goal to automate cryptographic refresh – such as through automated key and certificate lifecycle management – we can fully expect that vendor patches and updated versions will be required over time to benefit from cryptographic updates.

Cryptographic updates will need to be applied to both centrally managed infrastructure, such as a PKI, and to lines of business applications that perform cryptographic operations, including encryption and digital signatures. It is essential to assign responsibility for managing these updates to ensure compliance with policy and to address vulnerabilities. Budgets should reflect the effort required across business units, and roadmaps should be coordinated. Since many cryptographic use cases involve multiple systems that must support common protocols and algorithms, multiple systems may need to be updated before a new cryptographic algorithm can be leveraged.

Legal

Contracts administration functions must ensure that cryptographic requirements are built into agreements with subcontractors and suppliers. Lawyers should be provided with cryptographic standards and requirements to reference in these agreements. Supplier SLAs should be reviewed with a focus on cryptographic agility. For example, vendors should commit to updating cryptographic implementations as required to maintain security in light of emerging threats presented by quantum computing.

People – Attributes & Recommended Actions

	Description	Recommendation
Defining and Establishing Roles Within an Organization	Cryptographic agility requires coordination of various functions within an organization. It is important to define roles and ensure stakeholders are aligned.	Clarity should be established regarding the roles of each internal function (IT, R&D, and compliance/audit) across lines of business to maintain compliance with corporate cryptographic policies. Procedures for management of cryptographic assets should be documented.
Accountability	People will drive implementation of cryptographic agility only when assigned accountability to do so. All appropriate stakeholders should understand their role in protecting the organization's digital assets.	The first action organizations should take is to assign ownership and accountability for initial activities related to cryptographic agility.
Audit	As with all systems, the only way to be confident that security controls remain effective is to audit current state against policies.	Regular auditing of cryptographic policy and procedures, as well as compliance posture, should be established to maintain effective security controls. Consider implementation of dashboards that provide metadata of deployed cryptography in order to facilitate audit activities.
Implementation	Most new applications and IT systems embed cryptography, which must be implemented and configured correctly to avoid introducing vulnerabilities.	Train implementation teams on corporate cryptographic and key management policies and standards, and provide tooling to help them deliver secure applications by default.
Operations	It is common for cryptographic systems to be deployed and managed by different teams, and for systems to be live for many years. Audit of cryptography in use against current standards is a critical step to maintain security over time.	Assign responsibility for managing cryptographic updates to maintain compliance with policy and to remediate vulnerabilities.
Legal	Organizations are increasingly reliant on suppliers of products and services to support their digital business. Compromise of any of these systems can impact the organization.	Legal teams should be educated on the requirement for cryptographic agility to ensure that appropriate terms are included in agreements with suppliers of products and cloud services.

Next steps

As explained within this paper, the best place to start improving cryptographic agility is to assign accountability. Designate an individual or body to define the initial steps for improving cryptographic agility. This could include baselining current policies and processes against best practices to identify and prioritize key areas for improvement. Establish a new or existing body to fulfill the role of Policy Authority. Implement cryptographic governance to inform policy and drive adoption.

Assign responsibility for monitoring current threats and relevant government and industry best practices. Additionally, educate various stakeholder functions within your organization on the use of cryptography relevant to their roles.

The figure below illustrates the high-level steps an organization should take to improve cryptographic agility.

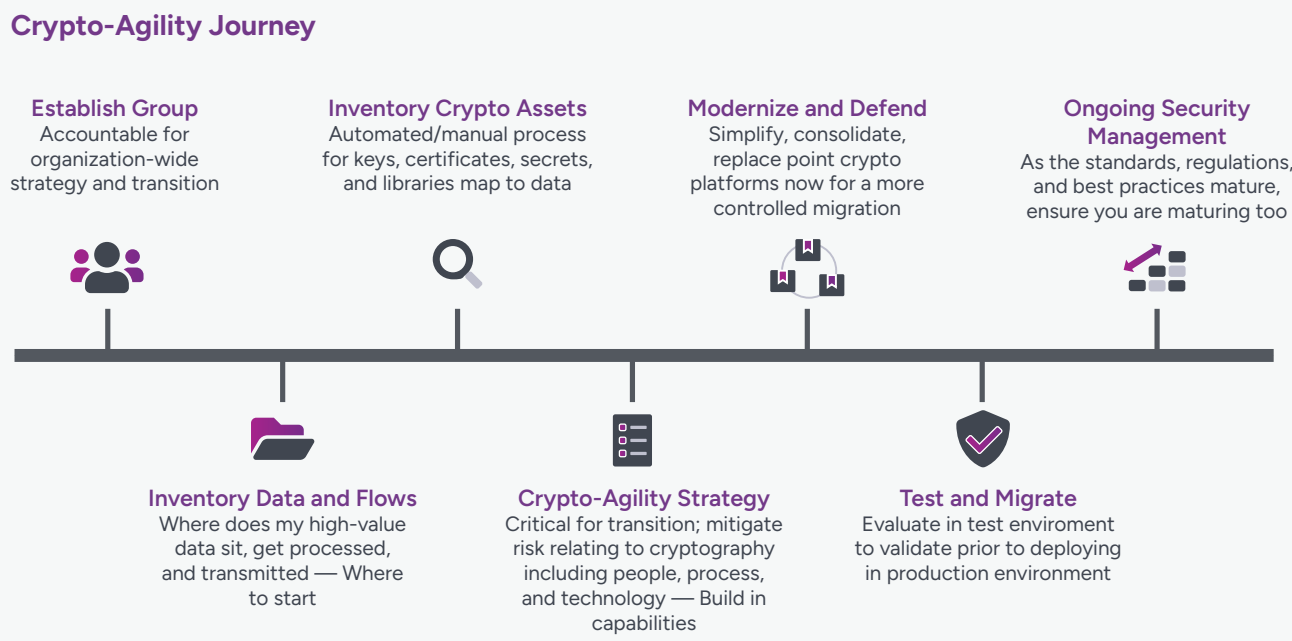


Figure 8: Cryptographic agility journey

Initiate a project to capture and maintain an inventory of cryptographic assets (certificates, keys, and libraries) within your organization. Map cryptographic assets to business information assets. Identify high-priority actions to enhance cryptographic agility, and regularly review and refresh this list to establish a process of continuous improvement.

Engage trusted partner organizations with relevant skills and experience to support your internal team by defining a roadmap for improving cryptographic agility and assisting with identified remediation actions as required.

How Entrust Can Help

Entrust offers a full suite of services designed to help customers secure data and transactions. This is based on decades of experience in the areas of cryptography, PKI, and key management. This section outlines how Entrust can help organizations improve their cryptographic agility through our consulting services, key management, and PKI solutions.

Cryptographic Center of Excellence

The Entrust Cryptographic Center of Excellence (CryptoCoE), a function of the Entrust Professional Services team, helps organizations balance the risks associated with expanding cryptographic use cases by accelerating their crypto strategy for enhanced digital security. It's designed to augment operational cryptographic and PKI processes with specialized expertise, providing increased insight into the cryptography organizations rely on to maintain secure operations and comply with relevant regulations. The Entrust CryptoCoE includes consulting services designed to address specific gaps in your cryptographic and/or PKI environments:

Service	Description	Recommendation
CryptographicAgility/ PQCMaturityAssessment	A subscription service to assist in developing a roadmap for customers to improve PQC readiness across people, process, and technology.	Organizations requiring actionable recommendations and expert advice to develop their roadmap for becoming PQ ready.
PKI Discovery	Analysis of the current PKI state and future requirements, with recommendations for implementing a modern PKI that provides appropriate assurance.	Organizations anticipating new demands on their PKI or requiring help with documenting requirements for new use cases.
Crypto Health Check	Analysis of the current cryptographic state and future requirements, with actionable recommendations to reduce risk and improve key management.	A great starting point for organizations to assess their current cryptographic and key management state, identify issues, and prioritize remediation actions.
PKI Governance Health Check	Review PKI governance documentation (CP, CPS, etc.), security controls, skills/training, and best practices. Provide a report on findings and recommendations.	Organizations requiring an audit of PKI policies, people, and processes to maintain target assurance.
PKI Governance Consulting	Develop a new PKI governance documentation set (CP, CPS, etc).	Organizations building a high assurance PKI.
PKI System Health Check	Analyze PKI software and hardware configurations and operations to deliver a report on findings and recommendations.	Organizations requiring an audit of PKI products and technical deployments to reduce risk and prevent outages.

Key Management

Entrust KeyControl redefines cryptographic key management by combining traditional key lifecycle management with a decentralized vaultbased architecture and a comprehensive central policy and compliance management dashboard. The platform offers decentralized security while providing centralized visibility across your enterprise's cryptographic ecosystem. The compliance manager dashboard allows fine-grained control and a detailed inventory of your organization's keys and secrets. As your inventory grows, you seamlessly build cryptoagility, with each cryptographic asset recorded in detail. This ensures full visibility, compliance tracking, and risk reporting. When migrating a specific algorithm, you can quickly search and rotate them across your organization, saving valuable time for IT security teams and compliance officers. Learn more about **Entrust KeyControl**.

PKI

Since Entrust launched the first commercially available PKI solution in the early 1990s, we have continued to innovate, delivering high assurance PKI solutions either on customer premises or through as-a-service delivery models. Entrust offers a full suite of PKI capabilities, including certificate lifecycle management and support for a wide range of enrollment protocols to integrate with enterprise applications. The ability to automate certificate delivery is available to reduce ongoing operational costs and support cryptographic agility. Furthermore, Entrust already supports advanced postquantum algorithms, helping customers secure their systems against the threat of CRQCs. Read more about our PKI solutions **here**.

Glossary of Terms

For clarity and for those general-interest readers unfamiliar with the subject, here is a high-level definition of some of the terms used within this paper:

Bring Your Own Key (BYOK): Typically for a cloudhosted application, the ability for an organization to generate a cryptographic key externally to the cloud platform and import it into the cloud for use.

Certificate Authority (CA): A component of a PKI that digitally signs subscriber certificates.

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

Classic Cryptography: Cryptographic algorithms in use today (including symmetric, public key, and hashing algorithms). Often used to distinguish from algorithms developed for use in post-quantum cryptography.

Cryptanalysis: The study of cryptographic algorithms with the aim of understanding their performance and security characteristics, as well as identifying potential attack vectors or inherent weaknesses.

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

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.

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 certificate authority and typically comply with the X.509 standard defined by the International Telecommunication Union (ITU).

Digital Transformation: The integration of digital technology into all areas of a business, fundamentally changing how it operates and delivers value to customers.

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.

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.

Hashing Algorithm: 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.

Hold Your Own Key (HYOK): Similar to BYOK, but with the organization's key remaining outside of the cloud platform.

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 post-quantum cryptography standardization process.

Glossary of Terms (continued)

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.

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.

Public Key Infrastructure (PKI): A collection of processes and technologies used to manage digital certificates and keys, allowing relying parties to trust digital transactions.

Registration Authority (RA): The role within a PKI responsible for the issuance of digital certificates according to the appropriate policy.

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.

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.

Bibliography

Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms

UK National Cyber Security Centre (NCSC) , Next Steps in Preparing for Post-Quantum Cryptography

PM Infotech Blog on LinkedIn, Risk Register

Canadian Centre for Cyber Security, Guidance on Becoming Cryptographically Agile - ITSAP.40.018, May 2022

Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography, NIST SP 1800-38B & NIST SP 1800-38C draft

Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography, NIST SP 1800-38c & NIST SP 1800-38C draft

Executive Office Of The President, White House Publication, Migrating to Post-Quantum Cryptography, November 18, 2022

NIST publication SP 800-221, Enterprise Impact of Information and Communications Technology Risk

IBM's Cryptography Bill of Materials to Speed Up Quantum-Safe Assessment | IBM Research Blog

Do You Have Cryptographic Agility? Ian Wills, Entrust, March 14, 2023

ABOUT ENTRUST

Entrust fights fraud and cyber threats with comprehensive identity-centric security that protects people, devices, and data. Our solutions help enterprises and governments safeguard critical systems from every angle, enabling secure onboarding and issuance, providing everyday identity protection, and empowering them with 360-degree visibility and orchestration across keys, secrets, and certificates so they can transact and grow with confidence. Building on our decades as a pioneer and innovator in establishing trust, Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit entrust.com.

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

ENTRUST
SECURING A WORLD IN MOTION