White Paper

Defining a Cryptographic Center of Excellence

Five pillars for establishing a "CryptoCoE" for business continuity, compliance, and security

ENTRUST

SECURING A WORLD IN MOTION

Contents

Executive Summary 3

Pillar 1: Discovery 6

Pillar 2: Analysis 8

Pillar 3: Recommend a Strategy 11

Pillar 4: Best Practices 13

Pillar 5: Maintaining a CryptoCoE 15

Conclusion 16

PRO TIP:

Do you have the appropriate corporate, information security, and cryptographic policies in place to measure against compliance?

The information provided herein does not, and is not intended to, constitute legal advice; instead, all information, content, and materials provided are for general informational purposes only.

Executive Summary

Reliance on cryptography has evolved over the last few decades to become an integrated layer of defense within modern digital transformation initiatives. Complex ecosystems and expanding use cases, such as DevOps, Internet of Things, cloud, and multi-cloud environments, are increasing the organization's crypto footprint. Throughout the digital transformation process, the realm of cryptography has also been dynamic, with changes on various axes. The nature of cryptography requires that as computing devices become more powerful, key lengths and algorithms must evolve to mitigate brute force attacks. The evolution of quantum computing also challenges the mathematical basis of algorithms widely used today, leading to the development of post-quantum algorithms, which will be required in the future. As crypto evolves, organizations must amend governance, best practices, and processes to maintain compliance with security requirements.

Crypto is critical infrastructure because increasingly the security of sensitive data rests on cryptographic solutions. On their own, keys, algorithms, certificates, libraries, and cryptography do not guarantee security. If not managed properly, crypto can expose critical infrastructure to vulnerabilities. Well-managed crypto can be used to secure transactions and communications, safeguard personally identifiable information (PII) and other confidential data, authenticate identity, prevent document tampering, and establish trust between servers. Crypto is one of the most important tools businesses use to secure the systems that hold their most important asset – data. Data is vital information in the form of customer PII, employee PII, intellectual property, business and financial plans, as well as other confidential information. The underlying confidentiality and authentication of all online services rely on the use of digital certificates and implementations of TLS/SSL. GDPR, PCI DSS, and many other regulations around the world require businesses to encrypt the personal and financial information that are kept in their possession in order to provide products and services.

Weak and hidden crypto instances present a challenge for security, risk, and compliance professionals — who already have some of the toughest jobs in the organization. Organizations must heed the guidance of standards bodies, such as NIST and ISO, and browser vendors who control the user interfaces with which online consumers interact. It's important to note that browser vendors also place their own demands on

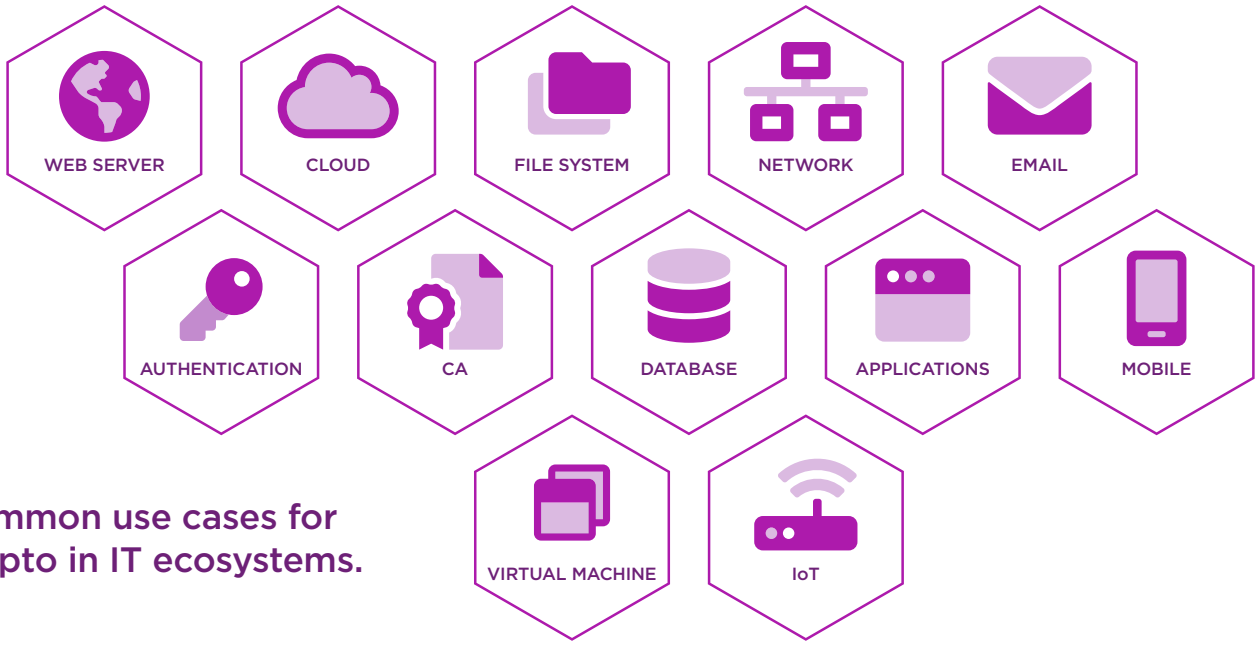
the certification authorities (CAs) who issue digital certificates to secure online transactions.

These dynamics disrupt traditional crypto and PKI planning efforts, as organizations increasingly rely on them to improve their overall security posture. If not managed properly, crypto can expose critical infrastructure to vulnerabilities.

This environment requires organizations to implement and enforce a solid crypto management strategy. System outages resulting from mishandled crypto lead to costly business disruptions and data breaches, which can become public events that damage brand reputations. If data is exposed, a business or its fiduciaries may be subject to financial penalties in accordance with regional laws.

A solid crypto management strategy can help security, compliance, and risk professionals lead the organization in establishing a Cryptographic Center of Excellence (CryptoCoE). The goal of a crypto-centric organization is to augment operational cryptographic processes with tools and expertise — and provide increased insight into the cryptography that organizations rely on to maintain secure operations and comply with applicable regulations. A CryptoCoE comprises five pillars that align expertise with a strategy for bringing hidden crypto to the surface, remediating weak crypto, adhering to best practices, and providing ongoing monitoring to enforce policies that bring crypto under control and into compliance.

CRYPTO IS CRITICAL INFRASTRUCTURE



Common use cases for crypto in IT ecosystems.

PRO TIP:

Do you have a certificate policy in place that defines the processes and roles for certificate enrollment, certificate revocation, and users/devices?

Pillar 1: Discovery

If crypto can't be seen, how can it be managed? Unmanaged crypto is the main cause for crypto-based system outages that disrupt business continuity and negatively impact both revenue generation and brand reputation. Yet, visibility into an organization's growing cryptographic infrastructure remains one of the main challenges facing security, compliance, and risk professionals. According to the Ponemon Institute 2020 Global Encryption Trends Study, "A barrier to a successful encryption strategy is the ability to discover where sensitive data resides in the organization. Sixty-seven percent of respondents say discovering where sensitive data resides in the organization is the number one challenge."

The use of an advanced discovery tool is needed to mitigate the risks associated with unknown crypto and to manage the certificate lifecycle for public and private trust. An advanced discovery tool can scan an IT environment end-to-end and bring hidden crypto to the surface, where it can be tested for compliance and monitored. To find hidden crypto, vulnerability scanning must search beyond the endpoints to detect various certificate types — even those buried inside binaries. A comprehensive scanner will search broadly across the IT ecosystem and bring visibility to unknown crypto instances. The discovery process should:

1. **Uncover number of PKIs in-service**
    a. Assess the status of the existing PKI implementations
    b. Lifetime of the Root CA certificates
    c. In compliance with current PKI governance standards
2. **Inventory (external and internal crypto)**
    a. Certificates (e.g., public, private, signing, SSH, etc.)
    b. Crypto algorithms
    c. Crypto libraries
3. **Search locations**
    a. Network
    b. Host
    c. Applications
    d. Binary files
    e. Java files
    f. Java KeyStores
    g. MS CAPI store certs
    h. Compressed files
    i. PEM, CER, DER, P12 files

Visibility is a key aspect of the research process that's used to create a baseline analysis of an organization's crypto security posture. Once the critical exercise of a prescriptive discovery is completed, a crypto expert can evaluate the findings and make clear determinations on the health of the crypto environment. Results of this process provide an opportunity for in-depth analysis that someone with domain expertise can use to assess and make recommendations for remediation plans.

"Sixty-seven percent of respondents say discovering where sensitive data resides in the organization is the number one challenge."
– Ponemon Institute 2020 Global Encryption Trends Study

Pillar 2: Analysis

Vulnerabilities are tied to algorithmic values and key strength — as well as the ability to meet minimum requirements for compliance to regulations, standards, and policies. There are a growing number of regulations that enforce data encryption practices on organizations, as indicated below. Heightened regulations, which are meant to enforce data encryption practices on organizations, particularly in the United States and the European Union, are primarily meant to do two things: 1) Protect user privacy requiring organizations to obtain explicit permission from users to collect data; and 2) Protect data in transit. Additional cryptographic standards and internal policies are put in place to protect data at rest.

After conducting an enterprise-wide search for implemented cryptographic solutions, a baseline assessment can be established by comparing the identified solutions against applicable standards and recommendations. A crypto expert can mine the data compiled during the discovery phase and present the organization with a threat-to-risk analysis. The current-state outcome will quantify the impact each vulnerability poses, identify high-risk areas, and prioritize crypto concerns. Organizations can use these findings as a benchmark to measure security improvements moving forward.

Here is a comprehensive list of IT systems and examples of various regulations, standards, and policies that the organization can use the baseline assessment to test against requisite industry and business requirements:

1. **Infrastructure assessment**

   Assess various systems including applications, servers, and network devices.

   a. Certificates

      1. Weak key algorithms
      2. Weak signing algorithms
      3. Improper validity periods
      4. Improper trust anchors
      5. Certificate expiration
      6. Unauthorized or rogue certificate authorities

   b. Cryptographic keys

      1. Improper key sizes
      2. Improper key algorithms

   c. Algorithms

      1. Improper TLS algorithms
      2. Old/outdated cryptographic libraries

   d. Protocols

      1. Weak TLS/SSL protocol versions

e. Policies

   1. Correlation between corporate policies against findings

2. Compliance verification

Test compliance with a growing number of protocols, requirements, and regulations instituted by various governing bodies. Consider the following examples of relevant legislation to help guide the process.

Regulations by region

a. CCPA — California Consumer Privacy Act, United States, State of California
b. GDPR — General Data Protection Regulation, European Union
c. PSD2 – Revised Payment Services Directive, European Union

Regulations by industry

d. PCI-DSS — Payment Card Industry Data Security Standard
e. PCI-CP — Payment Card Industry Card Protection
f. The Gramm-Leach-Bliley Act – Financial Service Institutions, United States
g. HIPAA — Healthcare Insurance Portability and Accountability Act (Healthcare Institutions, United States)

Industry standards groups

h. NIST – National Institute of Standards and Technology

   - NIST 800-53
   - Quantum Algorithms (currently under review)

i. FIPS — US Government Federal Information Processing Standard

   - FIPS 140

j. C/A Browser Forum
k. ISACA
l. CSA

International Organization for Standardization

m. ISO 27001

PRO TIP:

Are the cryptographic libraries in your environment that are embedded in critical systems updated with the latest patches, and with the latest cryptographic implementations?

3. **Quantify the impact**

   A quantitative crypto assessment reveals the vulnerabilities that exist on all tested systems and evaluates high-risk areas where weak or unmanaged crypto requires remediation to avoid data breaches, system outages, or penalties for putting sensitive data at risk.

4. **Prioritize focus areas**

   Many organizations deploy systems to support specific use cases — with some being more critical than others. A typical enterprise might classify its in-use servers into three categories: business critical, core business, and limited business, for example. It's important to identify where crypto vulnerabilities exist, so the organization can protect the infrastructure that supports the most critical data and establish a plan of action that prioritizes remediation for the most critical assets.

5. **Generate a findings report**

   A comprehensive report of the findings provides both an overview and a detailed analysis of crypto instances and host systems. The goal is to provide the security, compliance, and risk teams a detailed assessment of the current threat level and present the overarching findings in a way that can be easily communicated to non-technical stakeholders.

   The report should cover technical details for the target systems that were scanned and provide insights on the specific issue(s), including where they reside and recommendations on how to remediate them.

   Obtaining buy-in from board of directors (BOD) members to support a security project that exceeds their core areas of expertise can be difficult. It's a challenge many CISOs face. Having a board-ready report to explain urgent issues and outline a remediation plan can be a great tool for convincing a skeptical BOD to understand what is at stake and the importance of a CryptoCoE.

PRO TIP:

How well prepared is your organization to protect against and mitigate certificate security issues and expirations?

Pillar 3: Recommend a Strategy

The research collected throughout the discovery and analysis phases will help security, risk, and compliance leaders create a strategic security roadmap for risk mitigation and remediation. The security assurance level targeted by the organization will shape security policies. This plan must include assembling a team to monitor crypto assets for compliance and best practices on a regular basis.

A risk mitigation and vulnerability remediation plan is based on the organization's security policy and its level of compliance. The steps toward remediation include:

1. **Risk and compliance assessment**

   This assessment is based on the level of compliance, as well as the specific security objectives, established by an organization. It should include these activities:

   - Assess risk
   - Check compliance to industry requirements
   - Check compliance to standards requirements
   - Check alignment with internal security policies
   - Quantify the impact weak crypto levels present
     - Review the threat-to-risk analysis
     - Review the level of effort-to-benefit for remediation
   - Prioritize focus to areas that pose the highest security risk

2. **Remediation strategy**

   An effective approach is to build a strategy in phases that mirror the established prioritization plan.

   Define the security strategies

   - Identify the essentials
     - Data confidentiality
     - Crypto integrity
     - System availability

   Establish and apply an operational security process based on best practices

   - Develop policies
     - Approved certificate authorities
     - Minimum key lengths and permitted crypto algorithms
     - Crypto refresh policy/certificate lifetimes
     - Formally document and define procedures and roles

- Enforce policies
  - Train key personnel on your policies and procedures
  - Maintain control through defined roles
- Meet the auditing requirements
  - Establish periodic review of policies and audit compliance
- Control deployed and managed security technology
  - Scale with some level of automation for efficiency
  - Ensure your PKI and HSM technology is up-to-date

PRO TIP:

Are web servers for internal and external facing applications configured with appropriate cryptographic algorithms to maintain appropriate levels of confidentiality?

Pillar 4: Best Practices

Once visibility into a crypto environment is established and the IT ecosystem is stabilized against vulnerabilities, standardizing the way cryptographic instances are managed is the next essential step for maintaining compliance. As methodologies and standards change, remaining in compliance through transitional periods becomes even more challenging. Building a clear model for crypto management based on best practices is the logical next step.

PROCESS

Is there an appropriate governance structure in your organization to oversee the use of cryptography as part of an information security portfolio?

Implementing cryptographic functions, such as encryption, authentication, and key management, is considered a drag on CI/CD workstreams. DevOps, however, shares a common objective with InfoSec in the desire for secure, scalable, and automated workflows.

Finding ways to integrate security features required by InfoSec into DevOps methodologies — and doing it in a way that doesn't overly tax InfoSec resources or undermine the DevOps culture — is key. This starts with standardizing processes that mandate compliance throughout the organization.

InfoSec sets the policies and requires DevOps to script those policies into their code-as-infrastructure methodologies. A certificate authority (CA) like Entrust can play a critical role in overcoming that friction by enabling seamless TLS/SSL security for a true DevSecOps experience.

EXPERTISE

Are you applying governance appropriately for your critical crypto and/or PKI systems?

People with crypto domain expertise navigate this world of cryptography every day, working closely with the major industry standards groups and regulatory bodies. They anticipate how to be compliant today and tomorrow through the application of established and emerging security standards. Ongoing monitoring and analysis are required to keep pace with a rapidly changing regulatory environment. It's important to continually test systems against changing algorithmic requirements and the more stringent anticipated quantum algorithms.

All companies have a need for security expertise to ensure compliance with both internal and external policies; however, an even more important consideration is the protection of their networks and data. Most organizations lack the necessary cryptographic expertise to ensure both compliance and data protection. That's why it's important to have a

trusted partner with strong domain expertise.

DELIVERY

Does your organization have the necessary tools to scan your end-to-end security posture for rogue crypto? Do you have the skills and tools to evaluate and score it against current requirements and post-quantum algorithms?

A proper evaluation ensures organizations are up-to-date and in compliance with evolving business needs and regulations.

Tuning an organization's unique IT environment into a CryptoCoE depends upon:

- Advanced tools that capture the widening range of crypto instances
- Solutions that are certified against globally recognized criteria
- Access to deep technical expertise in cryptography and key management

Tuning PKI environments to meet auditing requirements assesses:

- Governance, including policy, procedures, process, and people
- Deployment infrastructure
- Certificate lifecycle management
- Compliance with industry and standards-driven best practices

Delivery of a CryptoCoE relies on having the precise resources and expertise to watch over the business-critical systems that are secured by cryptography.

GOVERNANCE

Are the digital certificates deployed across your organization in line with corporate policies, industry best practices, and standards?

It is essential for an organization to maintain compliance while both internal and external factors remain in motion. Certificates are crucial for validating identity and creating trust. By defining and enforcing their governance, organizations can be confident in their trust environments. Whether new standards are imposed or an organization's own dynamics (i.e., virtualization, expanding use cases, adding networks or new software applications) are at play, it's important to have the right tools, expertise, and policies in place. This enables visibility and governance, provides awareness of the moving parts, and helps prevent threats across an ever-increasing attack surface.

PRO TIP:

How prepared would you be to identify and replace weak or unsupported cryptographic algorithms if you had to do so today?

Pillar 5: Maintaining a CryptoCoE

Dynamic IT environments are subject to frequent modifications to accommodate changes throughout connected ecosystems and to comply with new requirements as they are enacted. Establishing a CryptoCoE is a meticulous process, but a worthwhile investment for security-minded organizations. Once established, it needs to be maintained in order to be effective. Keeping the organization tuned and optimized for crypto compliance requires ongoing monitoring, risk mitigation, and updating.

Ongoing monitoring of the crypto landscape and policies is an essential maintenance practice for a successful CryptoCoE. Doing so requires:

- Managing public and private certificate lifetimes to stay apprised of expiring certificates, duplicate certificates, server compliance testing, and discovery of rogue certificates. This helps avoid unexpected system outages and the introduction of new vulnerabilities.
- Scanning the IT environment routinely for rogue crypto.
- Following industry trends to keep a pulse on emerging industry requirements.
- Maintaining awareness of Standards Groups activity and transitioning to new standards as they are sanctioned.
- Scheduling regular policy reviews to ensure they are relevant and continue to meet evolving security needs.
- Enforcing the policies and procedures that bring security.

Maintaining an environment where cryptographic instances are tuned and optimized for maximum security is not a set-it-and-forget-it project. It requires hands-on expertise and continuous monitoring.

PRO TIP:

Can your organization maintain compliance through transitions as new requirements from standards bodies, regulatory agencies, and quantum policies take effect?

Conclusion

When a CryptoCoE is implemented according to best practices, it greatly improves operational cryptographic processes and ensures an organization can be confident in its trust environment. It requires the use of advanced tools and expertise to gain increased insight into the cryptography that's used to maintain secure operations and comply with applicable regulations. Crypto is critical infrastructure requiring expertise and dedicated resources to bring it under control and into compliance. It calls for a set of organizational standards and practices to rein in rogue crypto wherever it exists. As enterprises adopt new IT practices that expand crypto footprints, which consequently broadens attack surfaces, the need to establish a CryptoCoE becomes mission-critical.

About the Entrust Cryptographic Center of Excellence

Entrust, a leader in cryptographic security solutions, is the first CA to offer a Cryptographic Center of Excellence. It's designed to help organizations balance the risk associated with IT practices that expand crypto use cases by accelerating a crypto strategy for enhanced digital security. We work alongside security, risk, and compliance teams as a trusted partner, sharing our specialized expertise in encryption technology, best practices, and an advanced discovery tool to help bring crypto under control. The Entrust CryptoCoE comprises cryptography experts who offer significant industry experience and provide our customers with a pool of accessible subject matter experts. The CryptoCoE is structured to remain at the forefront of this dynamic domain and offer our customers access to continually updated best practices.

For more information

888.690.2424
+1 952 933 1223
info@entrust.com

entrust.com

ABOUT ENTRUST CORPORATION

Entrust secures a rapidly changing world by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

Entrust and the Hexagon Logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. Because we are continuously improving our products and services, Entrust Corporation reserves the right to change specifications without prior notice. Entrust is an equal opportunity employer.
© 2020 Entrust Corporation. All rights reserved. SL21Q2-ccoe-white-paper-wp

ENTRUST

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com