Post-Quantum Cryptography (PQC) Working Group

Current State (Crypto Agility) Technical Paper

FS-ISAC

PQC Working Group

Current State (Crypto Agility)

CONTENTS

Abstract

The main objective of this paper is to inform and present recommendations to ensure the security, resilience, accuracy of inventory, and accountability of data protection assets (keys, secrets, cryptographic modules and certificates), while mapping some initial and relevant transition steps to inculcate a balanced, cost efficient, and faster implementation. The aim of the research was to serve as a reference point to promote collaboration on crypto agility (via accurate inventory) early in the design phase of Engineering & Technology projects involving cryptography.

We aim to provide:

- *Baseline Component Information* and the metadata relationships are provided to derive low-level, co-relatable data models in any architecture.
- The security patterns and the Questionnaire to enable creation of security policies to govern and retrieve the inventory.
- Suggested mechanisms to enable ongoing review and upliftment of the current state (managed and unmanaged data protection assets) and its oversight.

This research limits the focus on data protection assets limited to keys, secrets, cryptographic Modules, and certificates and their inventory to set the perimeter of the work to be done and serve as a basis of future developments for better metrics and progress towards crypto agility.

In addition, this document may also support discussions at a policy-making level and therefore be of interest to strategic DevSecOps target areas.

Introduction

A strategic cybersecurity asset is a collection of co-relatable metadata as inventory of data protection assets (keys, cryptographic modules, secrets and certificates). It will enable organizations preparing for post-quantum to:

- Establish foundational work to start designing systems that improve metrics.
- Record exact use/purpose.

- Enforce security policies across IT infrastructure.
- Reduce root cause analysis mean time.
- React quickly to security issues.
- Efficiently carry out strategic transformations towards crypto-agility, such as controlled migration of cryptography services to the cloud or deploying post-quantum cryptography.

The Inventory Problem

The lack of central governance structure for cryptography security: There may not always be a central cryptography security team in every organization.

Inadequate central governance controls to protect the confidentiality, integrity, and availability of data protection assets: Even if the cryptography security team exists, sometimes, it might not be fully set up, or has no control to set policies, or might have minimal authority to enforce the policies or might have no control on the Cryptography Lifecycle management and tooling.

Issues with efficiencies in governance: Due to the lack of visibility centrally, it is possible that there is no central Infrastructure or shared services team that ensures all statutory, regulatory and contractual cybersecurity and privacy obligations are addressed to ensure secure configurations are designed, built, and maintained. This is another problem waiting to happen as a surprise to the organization's security operation teams.

Roles, responsibilities & standardization issues w.r.t. configurations: The configuration management function for cryptography may not always be formally assigned with defined roles and associated responsibilities. Implementation business teams might see this as complex additional work due to the lack of understanding of cryptographic issues and compromises. Configurations might not conform to industry-recognized standards for hardening (e.g., NIST, ANSI, DISA STIGs, CIS Benchmarks or OEM security guides) for test, development, staging and production environments, including the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies to protect the confidentiality and integrity of the data.

Possible loss or misrepresentation of metrics due to lack of co-relations & full visibility: Inventory of Data Protection Assets such as keys, certificates, cryptographic libraries, cryptographic modules and secrets related to cryptography are created and updated manually on some, for example, using a certificate manager, key manager, or HSM for some, and manually for other cryptography. Inventory is not centralized or co-related or cross referenced. Sometimes metrics containing metadata of keys, certificates, cryptographic modules, secrets and their issues are generated via different tools. These might be downloaded and matched manually based on the perspectives of the generator of the reports & metrics for seniority teams. There might not always be automated feeds from different tools to present a common area to derive metrics directly from one tool.

We will attempt to solve these issues of inventory and crypto agility by establishing some foundational groundwork to derive data models, corelations between them and conceptual architecture covers not only the assets but also their issues and drafting next steps towards better inventory, metrics and governance.

Software Bill of Materials (SBOM)

What is an SBOM?

An SBOM is a formal, machine-readable inventory of software components and dependencies that contain information about those components and their hierarchical relationships. These inventories should be comprehensive, or should explicitly state where they could not be.

SBOMs should include baseline attributes that can uniquely identify individual components in a standard data format. The most efficient generation of SBOMs is as a byproduct of the Continuous Delivery or DevSECOps process. For older software, less automated methods exist.

Baseline Component Information

The primary purpose of an SBOM is to uniquely and unambiguously identify components and their relationships to one another. To do so, some combination of baseline component information is required.

These baseline components support many use cases, but not all. Additional attributes may be required to support advanced use cases

Baseline component Information
Author Name
Supplier Name
Component Name
Version string
Component Hash
Unique Identifier
Relationship

The following three formats and specification can be used:

Format	Specification	Tools
SPDX	https://spdx.github.io/spdx-spec/	https://tiny.cc/SPDX
CycloneDX	https://cyclonedx.org	https://tiny.cc/CycloneDX

SWID	ISO/IEC 19770-2:2015	https://tiny.cc/SWID

For more resources about SBOM, see www.ntia.gov/sbom.

Proposed *baseline component information* for recording inventory of data protection assets

Baseline Component Information
Author Name/Owner
Supplier Name /Generated inside which module?
Component Name
Version string / Validity dates
Component Hash / Fingerprint [where possible]
Unique Identifier / Human readable Alias
Relationship (example: Primary Key and Foreign key relationships)

Current state Inventory Considerations

Current State – Questionnaire That can Assist in Building an Inventory of Data Protection Assets and Their Security.

1. Does the organization have an inventory of all instances of non-console administrative access?

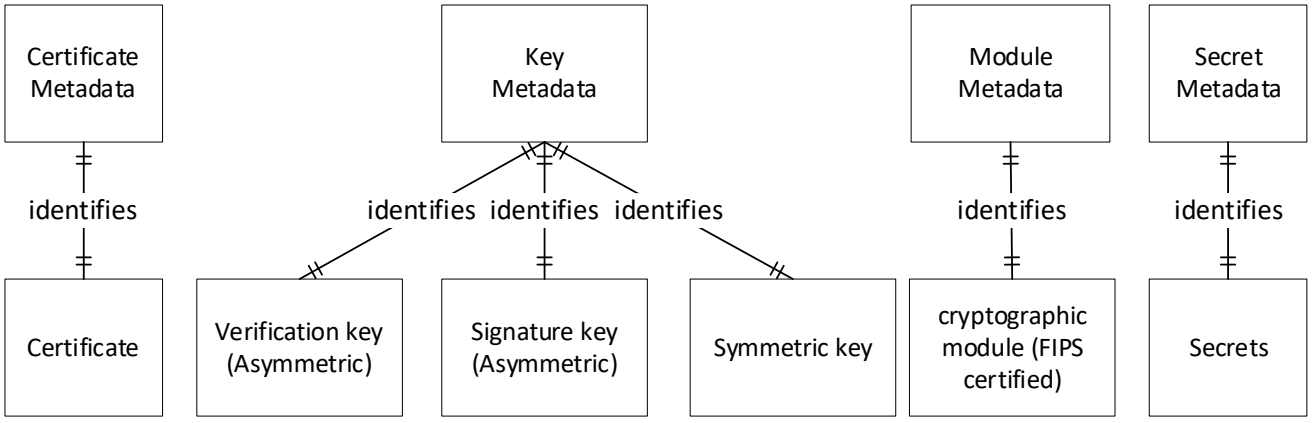
2. Does every instance of non-console administrative access utilize cryptographic mechanisms to protect the confidentiality and integrity of the data being transmitted? What are those cryptographic mechanisms? What data protection assets do they use? Where are they located? Is a related responsibility matrix (RACI) defined per data protection asset?
3. Do all mobile devices containing sensitive data utilize a cryptographic mechanism to prevent the unauthorized disclosure of information at rest and in transit? What are those cryptographic mechanisms? What data protection assets do they use? Where are they located? Is a related responsibility matrix (RACI) defined per data protection asset? Example: full drive encryption.
4. Do all databases containing sensitive data utilize a cryptographic mechanism to prevent the unauthorized disclosure of information in the database? What are those cryptographic mechanisms? What data protection assets do they use? Where are they located? Is a related responsibility matrix (RACI) defined per data protection asset? Example TDE, full disk encryption.
5. Do all network communications containing sensitive data utilize a cryptographic mechanism to prevent the unauthorized disclosure of information while in transit? What are those cryptographic mechanisms? What data protection assets do they use? Where are they located? Is a related responsibility matrix (RACI) defined per data protection asset? Examples: SSH, TLS, VPN, etc.
6. Is all wireless access protected via secure authentication and encryption? What are those cryptographic mechanisms? What data protection assets do they use? Where are they located? Is a related responsibility matrix (RACI) defined per data protection asset?
7. Are all Systems/applications /services that include cryptographic mechanisms controlled to ensure the exporting of cryptographic technologies is in compliance with relevant statutory and regulatory requirements? What are those cryptographic mechanisms? What data protection assets do they use? Where are they located? Is there a related responsibility matrix (RACI) defined per data protection asset?
8. Are all Systems/applications/services that store, process, or transmit sensitive data utilize cryptographic mechanisms to prevent unauthorized disclosure of information as an alternative to physical safeguards? What are those cryptographic mechanisms? What data protection assets do they use? Where are they located? Is a related responsibility matrix (RACI) defined per data protection asset?

9. Does a dedicated PKI infrastructure team, or similar function, implement and maintain an internal Public Key Infrastructure (PKI) infrastructure, or does it obtain PKI services from an industry-reputable PKI service provider?
10. Does the PKI management function facilitate the implementation of cryptographic key management controls to protect the confidentiality, integrity, and availability of keys?
11. Does an IT infrastructure team, or similar function, facilitate the production and management of symmetric cryptographic keys using Federal Information Processing Standards (FIPS) or their Internal organization standards-compliant key management technology?
12. Does an IT infrastructure team, or similar function, facilitate the production and management of asymmetric cryptographic keys using Federal Information Processing Standards (FIPS) or NIST 800-53 or NIST 800-57 or their Internal organization standards compliant key management technology such that private key never leaves a secure boundary?
13. How does the PKI infrastructure ensure or provide assurances of the availability of information in the event of the loss of cryptographic keys by individual users? How frequently are the entitlements and existing architecture reviewed?
14. How does the PKI infrastructure facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry-recognized key management technology and processes? Who would be owner of the shared-secret, keys, endpoints, and users?
15. Is there a 1:1 mapping/binding of All cryptographic keys and secrets to individual identities?
16. How does the SSH infrastructure ensure or provide assurances of the availability of information in the event of the loss of cryptographic keys by individual users? How frequently are the entitlements and existing architecture reviewed?
17. How does the SSH infrastructure facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry-recognized key management technology and processes? Who would be owner of the shared-secret, keys, endpoints, and users?
18. Can all the secrets related use cases be automated and managed via a privileged access control model from a central secretsManager with essential audit and reporting capabilities?

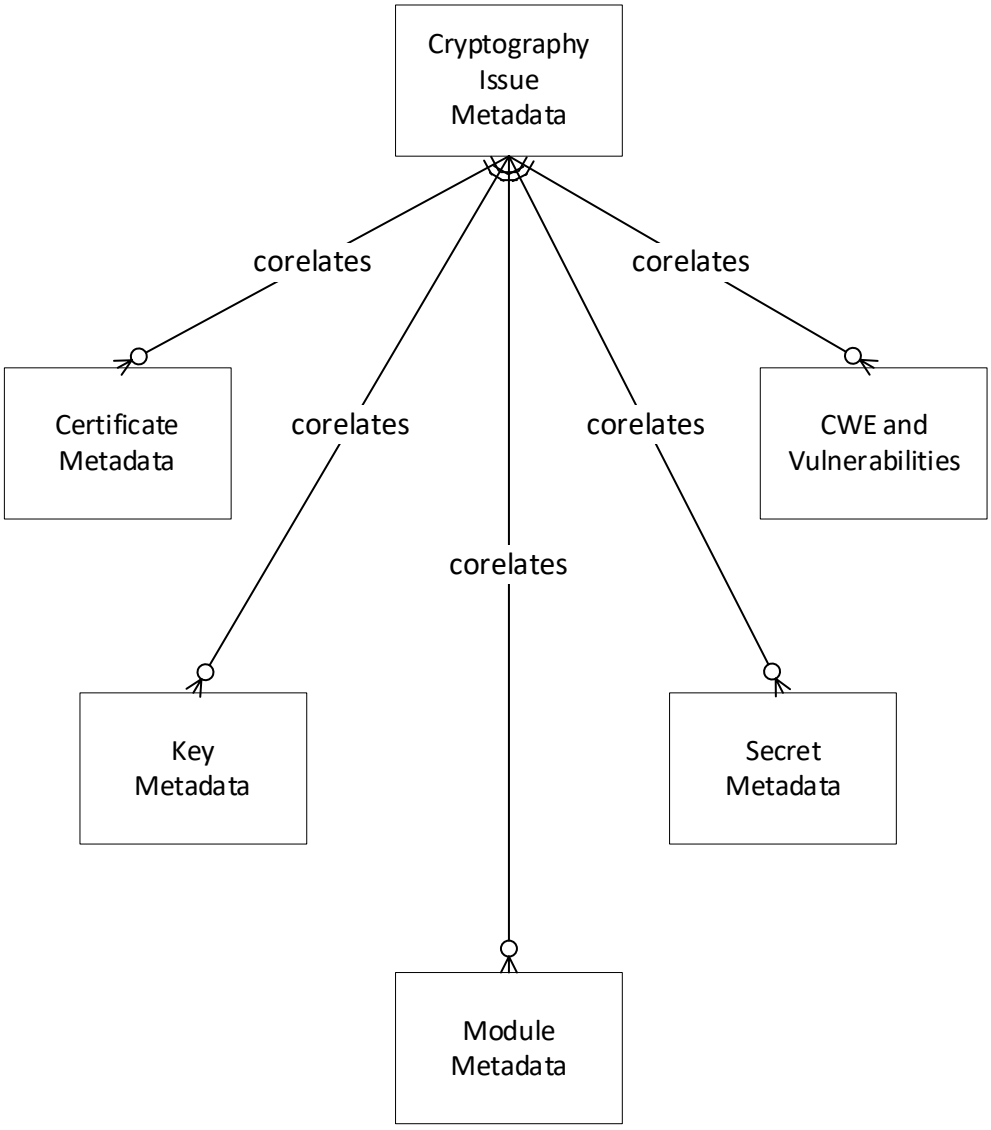
19. Do all cryptography-related issues and tickets include the metadata of keys, secrets, cryptographic modules, cryptographic libraries, and certificates?

Current State - Data Protection Assets Metadata and Their Co-Relations That Needs to be Kept in Mind with Recording Inventory

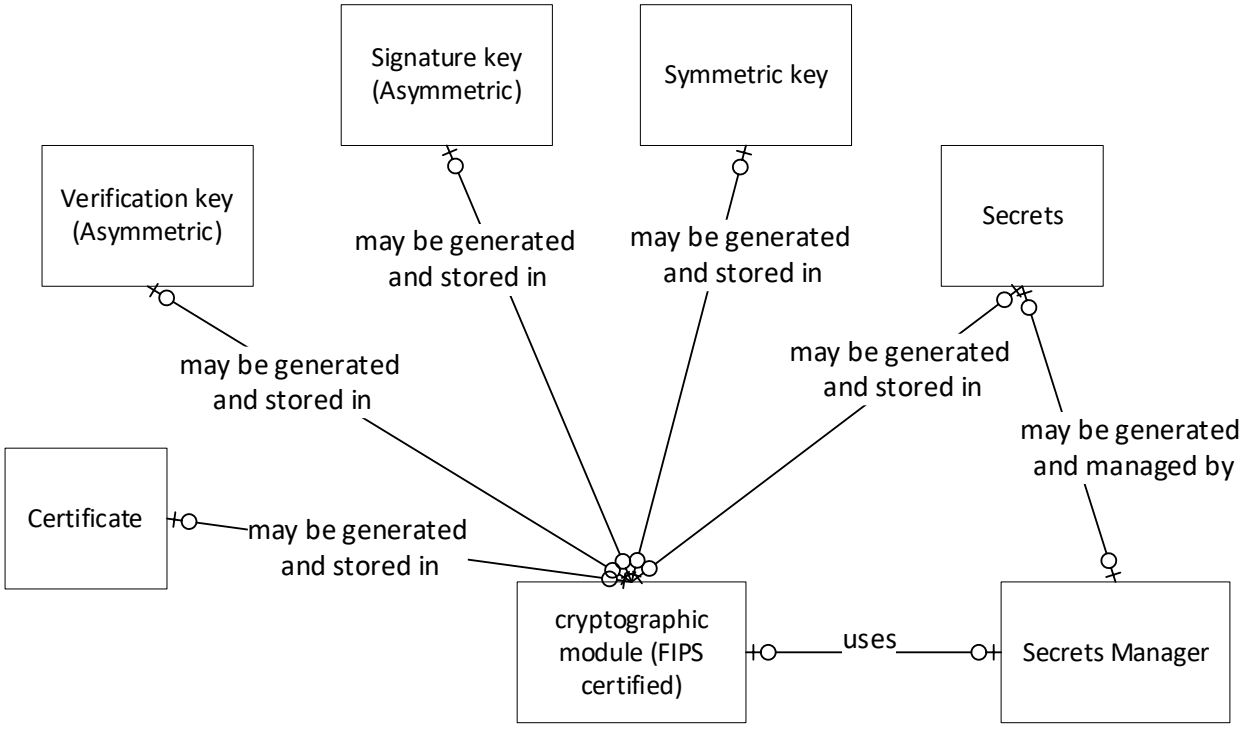
- Metadata vs Actual Data Protection Assets relationship:



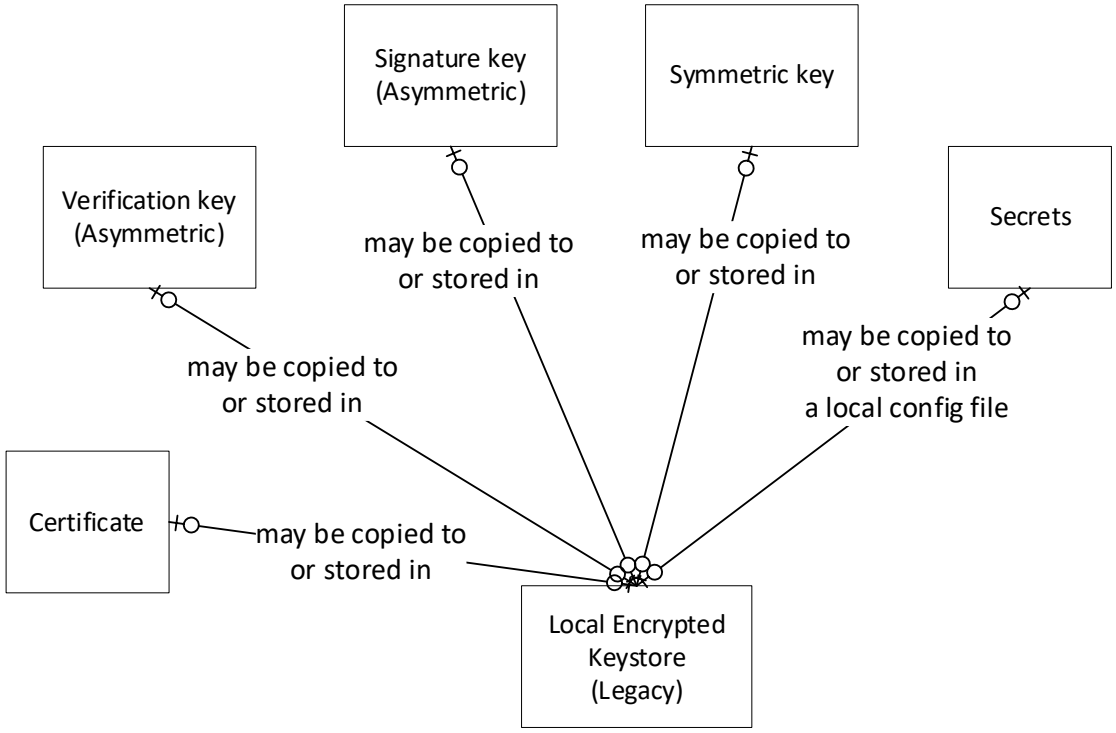
- Issue Metadata vs Data Protection Assets Metadata relationship:



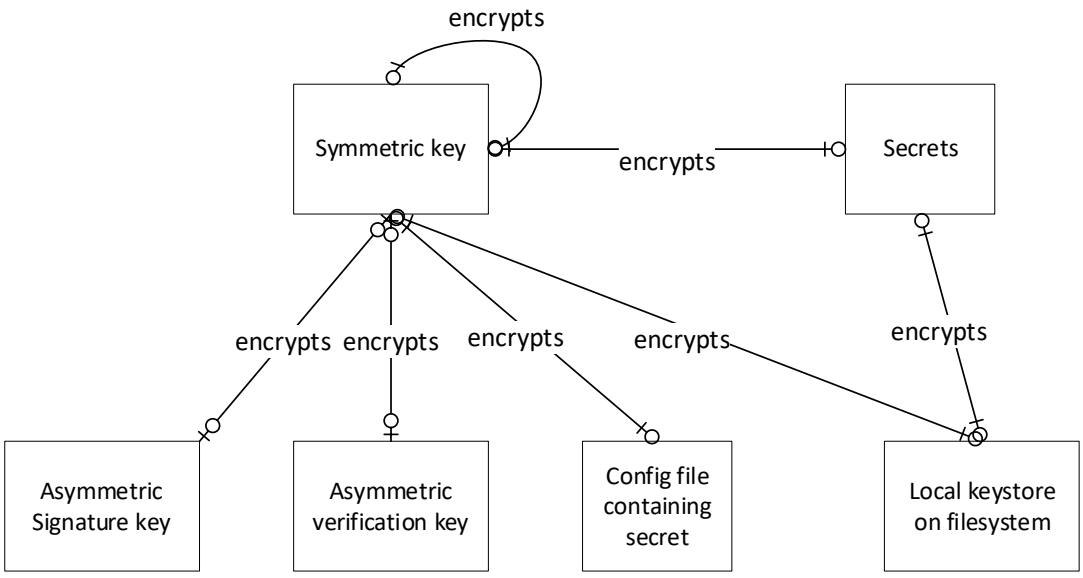
- Cryptographic module vs Keys, Secrets and certificates relationship:



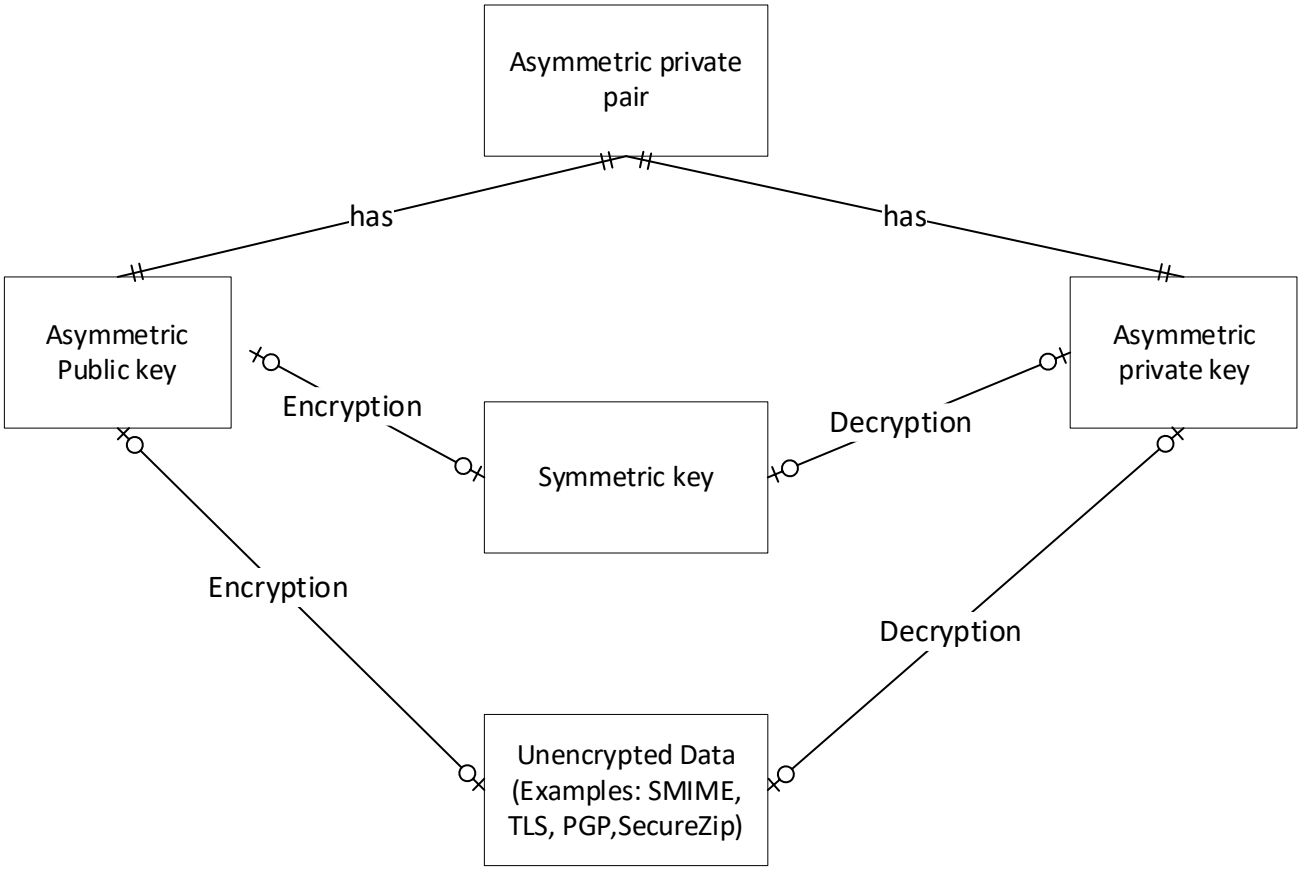
- Local Encrypted Keystore vs Keys, Secrets and certificates relationship:



- Symmetric key relationship with secrets, asymmetric key pair and local store:



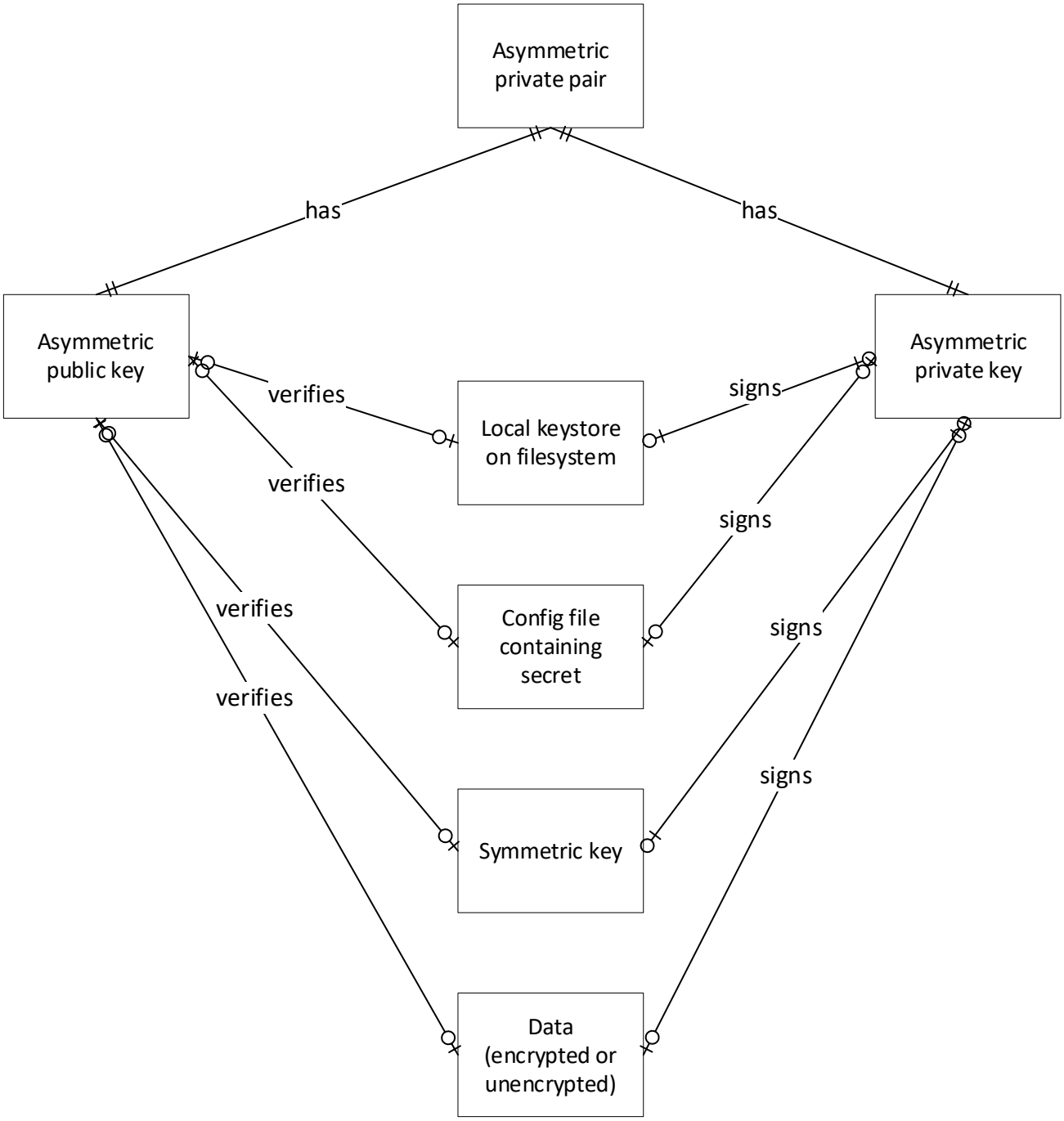
- Asymmetric key relationship with local store, encrypted information and symmetric keys (encryption and decryption):



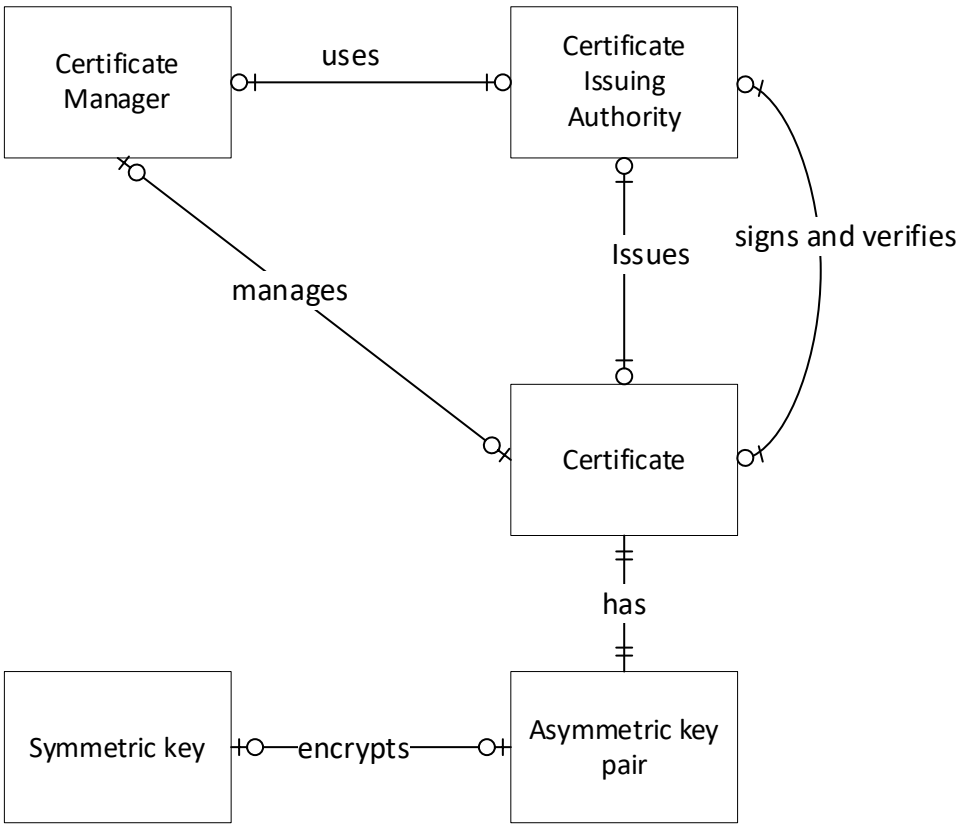
- Asymmetric key relationship with local store, encrypted information and symmetric keys (signing and verification):

PQC Working Group

Current State (Crypto Agility)

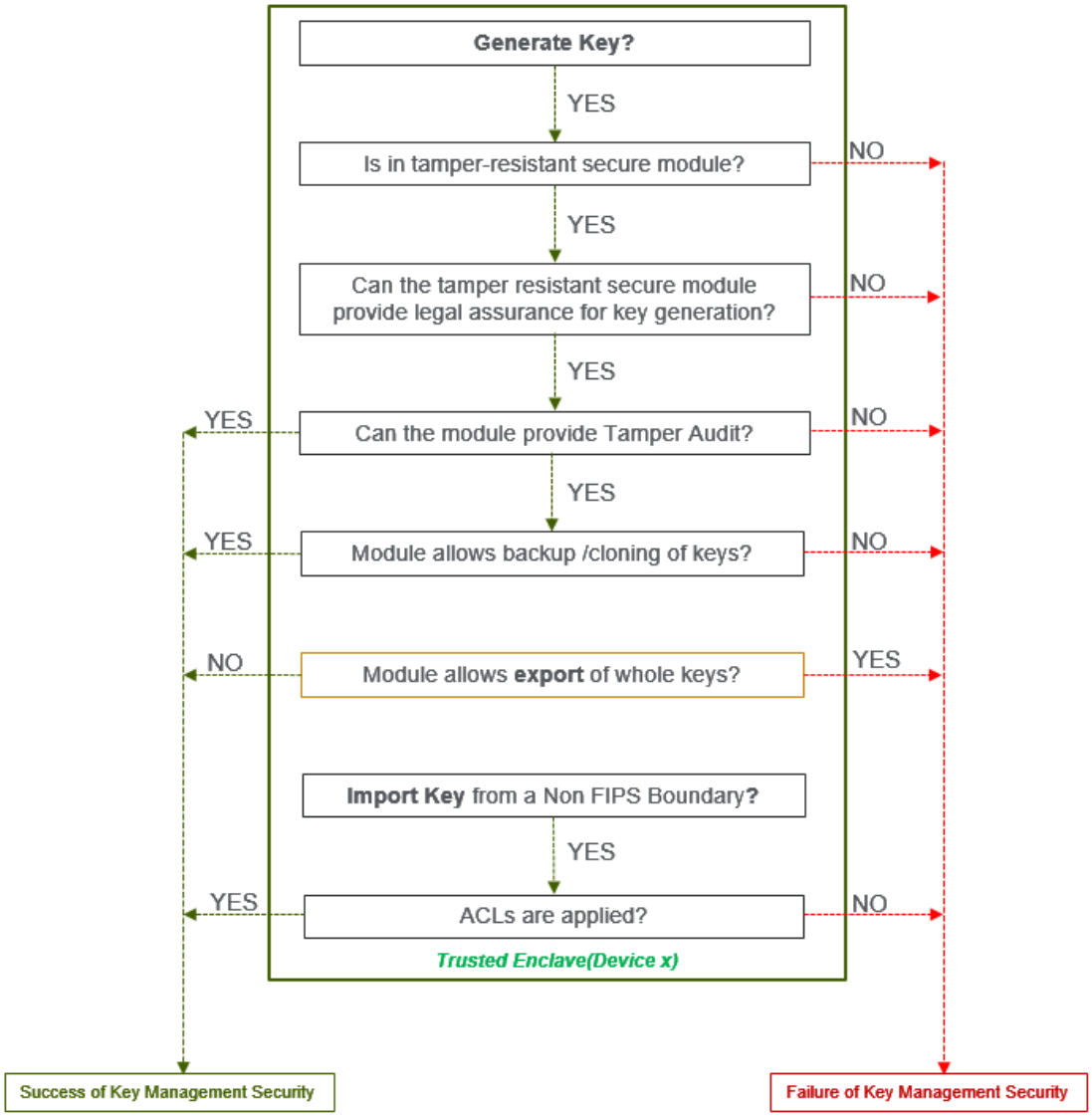


- Relationship of certificates, issuing CA, certificate manager and keys:



Current State - Security Policies can be Created by the Referring of the Following Security Patterns

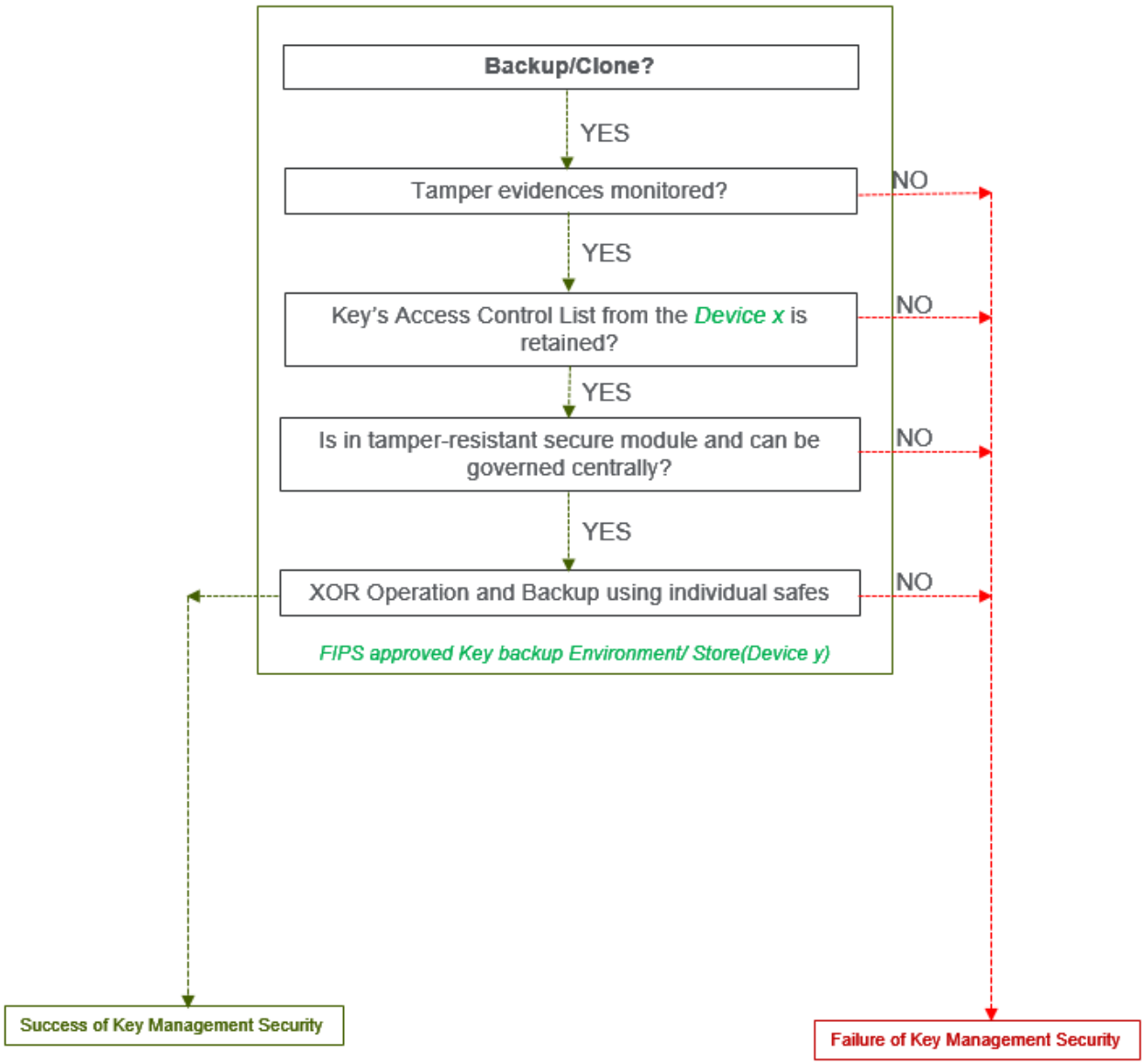
Trusted Enclave Security pattern for secure key generation, Import and export operation within the organization approved *Trusted Enclave*



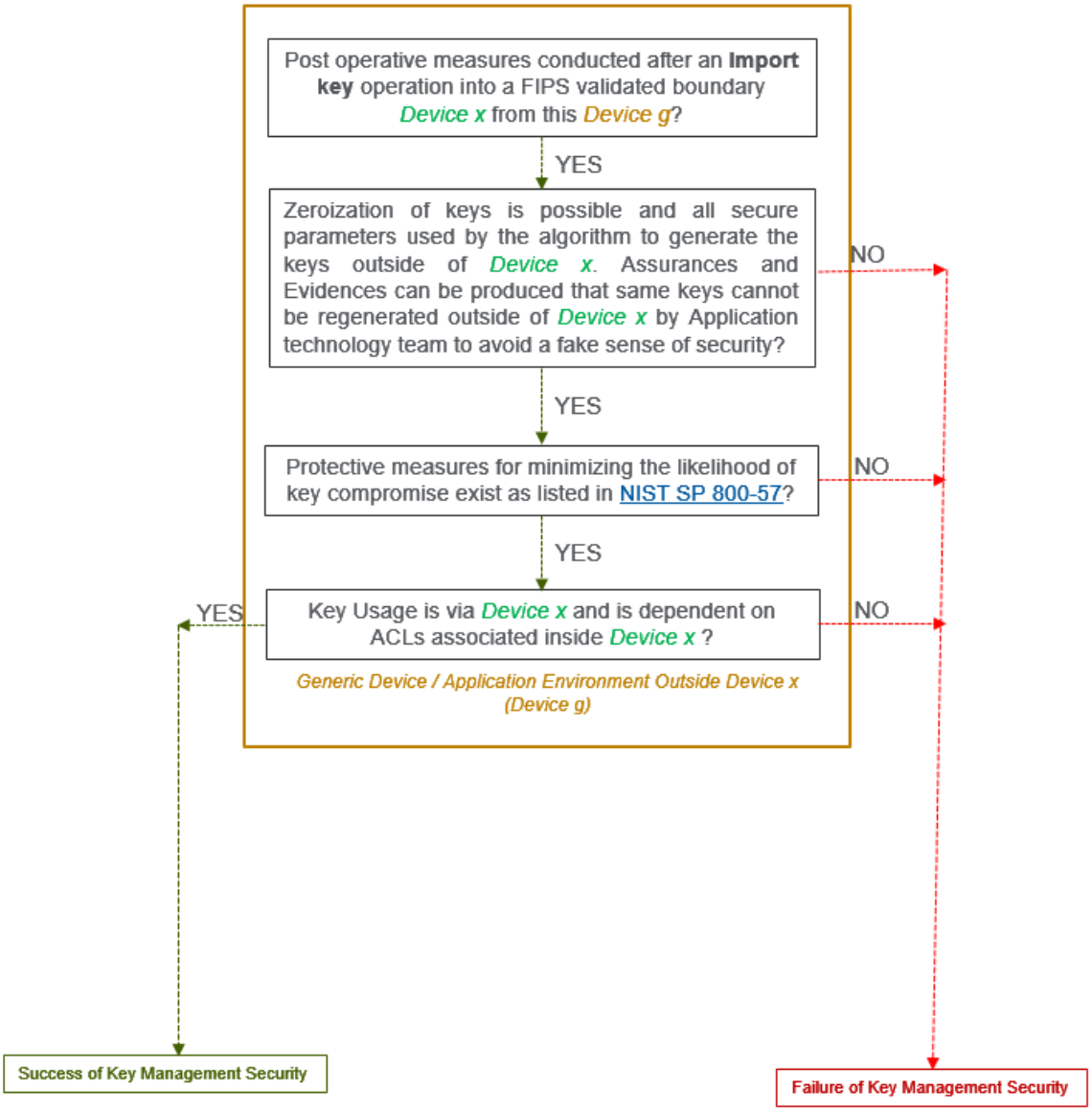
Letters in **bold** depict key lifecycle operations. The box with orange border depicts features and operations highest prone to Key management compliance failures even if a tamper resistant cryptographic module is used.

The Key Export problem: Once keys are exported outside the *Device x*, The operation will be equivalent to an OpenSSL generated key on any application environment and thus, can no longer be governed or be compliant. All Access Control List (ACL) associations with the keys for security from within the *Device x* will be broken after the export.

Trusted Enclave security pattern for secure Backup and cloning of keys Within a *Trusted Enclave only accessible backup*



Trusted Enclave security pattern for secure zeroization of keys after import from any non-trusted environment into a trusted one *(Device x)*



The box with orange border depicts features and operations highest prone to Key management compliance failures even if a tamper resistant cryptographic module is used in the architecture.
If keys were imported into secure Device x then all copies outside of the Device x must be destroyed via zeroization.

Current State - Cryptographic KMS (Primary Competitors) Currently Available in the Market and Their Features – Publicly Available Information:

Requirements	Thales		Cryptomathic	Fortanix	QuintessenceLabs
	Cipher	Vormetric Data Security Manager	Crypto-Key-Management-System	Self Defending KMS	qCrypt 300H
	Trust Manager				
Functional Feature:					
Key Life Cycle	YES	YES	YES	YES	YES
Key:					
Grouping	YES	YES	YES	YES	YES
Segregation	YES	YES	YES	YES	YES

Splitting	NO	NO	YES	YES	–
Cryptography:					
RSA	YES	YES	YES	YES	YES
AES	YES	YES	YES	YES	YES
Key Types:					
Private Signature Key	NO	YES	YES	YES	NO
Public Signature Key	NO	YES	YES	YES	NO
Symmetric Data Encryption/Decryption Key	YES	YES	YES	YES	YES
Symmetric Key Wrapping Key	YES	YES	YES	YES	YES
APIs:					
REST	YES	YES	YES	YES	YES
PCKS#11	YES	YES	YES	YES	YES
KMIP	YES (1.1 only)	YES (1.1 only)	n/a	YES (up to version 1.4)	YES (up to version 1.4)
Integration with existing PKI	NO	YES	YES	YES	NO
Access Control:					
Separation of Duties	YES	YES	YES	YES	YES

MFA	YES	NO (optional)	YES	YES	NO
Dual control	NO	NO	YES	NO	NO
Backup & Restore	YES	YES	YES	YES	YES
On-premises	YES	YES	YES	YES	YES
Policy configuration	YES	YES	YES	YES	YES
Accountability	YES	YES	YES	YES	YES
Auditing	YES	YES	YES	YES	YES
Reporting	YES	YES	YES	YES	YES
HW Features:					
Hot swappable RAID	YES	NO	YES	NO	YES
Dual redundant power supply	YES	YES	YES	YES	YES
Independent network interfaces	YES	YES	YES	YES	YES
N+2 redundancy	YES	YES	YES	YES	YES
Business continuity	YES	YES	YES	YES	YES
Security Goals:					
Confidentiality	YES	YES	YES	YES	YES
Integrity	YES	YES	YES	YES	YES

GUI	YES	YES	YES	YES	YES
Input validation	n/a	n/a	YES	n/a	n/a
User assistance	n/a	n/a	YES	n/a	n/a
Non-Functional Requirement Feature/Support					
Design specification	YES	YES	YES	YES	YES
HA	YES	YES	YES	YES	YES
FIPS level 3	YES	YES	YES	YES	YES
Vendor-agnostic	NO	NO	HSM agnostic	NO	NO
Application-agnostic	NO (additional connectors for each application)	NO (additional connectors for each application)	NO (additional key listener)	YES	YES
Strategic nature of the product	YES	NO (the vendor does not support this product in the long term)	YES	YES	YES
Vendor credibility	YES	YES	YES	YES	YES
Vendor support	YES	YES	YES	YES	YES

Current State – Oversight View

The following excel can be used by various organizations to capture their current state inventory of data protection assets

Cryptoagility%20Inventory-%20Capture

Affected Assets, Policies, and Standards with PQC (Managing Changes)

Review for a change can be triggered from any of the Tiers

Change to be triggered from left to right Tier [1] to Tier [3]

Every change to Tier [1] will be informed for appropriate updates to all other Tiers.

Assets Affected ß\ Tiers Affected Þ	**Key Lifecycle Operations Tier [1]**	**Consumption Operations Tier [2]**	**Governance & Compliance Tier [3]**
Company reputation	Cryptography, Key, Certificate, Cryptographic Libraries, Cryptographic Modules related policies and standards in the org	Process Control Management documents. Continuous Monitoring Operational Process related documents.	Data protection policy and standards. Data/media sanitization policies and standards. Company architecture standards. Third-Party cybersecurity specific policies and standards. External hosting standards.
Company's customer reputation			
Company's partner/client reputation			
Intellectual property			
Personal sensitive data (example: confidential PII data)			

Critical data (ex. shared service infrastructure supporting data like web hosting/API gateways)			Company's cloud specific policies and standards. Security incident response related policies and standards. Cybersecurity risk related policies and standards. Remote access related policies and standards. Network security related policies and standards. Virtual asset service related policies and standards. Regional and LOB policies and standards. Company's SDLC policies and standards. Company risk appetite and associated policies and standards. Company information/ cybersecurity policies. Third-Party management policy and standards. AML policy and standard
Personal data (ex HR-requests for travel/ promotion etc)			
Company user data (anything related to a user representing company)			
Client/customer data (agreements, transactional data, digital assets belonging to client/customer)			
Management data (reports etc)			
Operational data (workflows/process specific to the business operation …)			
Functional data (BAU/ business logic related)			
Metadata			
Service delivery - real time			
Service delivery			

Access control (authentication/ authorization) (user/functional identity)			sanctions policy and standard confidentiality policy and standards. Data privacy policy and standards. Records management policy and standards. Conflict of interest policy and standards. Anti-bribery and corruption policy and standards. Continuity of business policy and standards. Disaster recovery policy and standards. Due diligence of subcontractors policy and standards. Insurance in context of tech providers policy and standards. Employee due diligence policies.
Privileged access control (authentication/ authorization) (superuser/admin/ superuser functional identity<high privileges)			
Credentials (secrets/ tokens… etc)			
Directory and folders (with/without data) + entitlements			
Service management interface (at data center)			
Service management interface (on cloud)			
Management interface APIs (dashboards and related admin APIs)			
SDKs and other functional APIs (business logic related)			
Interoperability and connections (company internal)			

Interoperability and connections (extranet/ internet)			
Endpoints and hosts			
Physical hardware & infrastructure			
Virtual infrastructure			
Cloud infrastructure			
Choice of hosting locations, jurisdictions and physical building/locations/postal address and services- legal administrative			
Hosting locations, jurisdictions, and physical building/locations/postal addresses & services - implementation specific (PCM)			
Application source code (company internal)			
Application source code (SaaS/cloud/opensource)			
Operational logs			

Security logs			
Backup or archival			

Currently Available Crypto Inventory Automation Tools

Venafi TPP + Scanafi and SSH Protect: Coverage - Infrastructure.

CryptoSense : Coverage - infrastructure and application + devSecOps

InfoSecGlobal : Coverage - Infrastructure and libraries

Conclusion

This paper has informed and presented a fundamental baseline and recommended tools and guidance to create policies to ensure resilience, and accuracy of inventory of data protection assets (keys, secrets, cryptographic modules and certificates), while mapping some initial and relevant transition steps to inculcate a balanced, cost efficient, and faster implementation.

Our recommendations:

Use the SBOM-based *Baseline Component Information* and the metadata relationships provided to derive low-level co-relatable data models.

Use the security patterns and the questionnaire to create security policies to govern and retrieve the inventory.

Use the oversight view excel to constantly review and uplift current state (managed and unmanaged data protection assets) oversight.

Take any approach that makes it easier to adopt cryptography related security standards and covers benefits as listed below:

- Receive metadata feeds centrally in standard format from different scanning tools if incorporated.
- Simplify Standardization and compliant implementation of cryptography.
- Accelerate percolation and implementation of security policies via automation/ Policy as a code.
- Design toward central control of data and data protection assets governance.
- Automate to accumulate inventory of data protection assets (cryptography SBOMs) in the enterprise.
- Include crypto agility aspects and relationships between metadata for a future proof design.
- Accurately correlate information to provide better control and accurate metrics.

If you are an FS-ISAC member and would like to join the PQC Working Group, please email us.