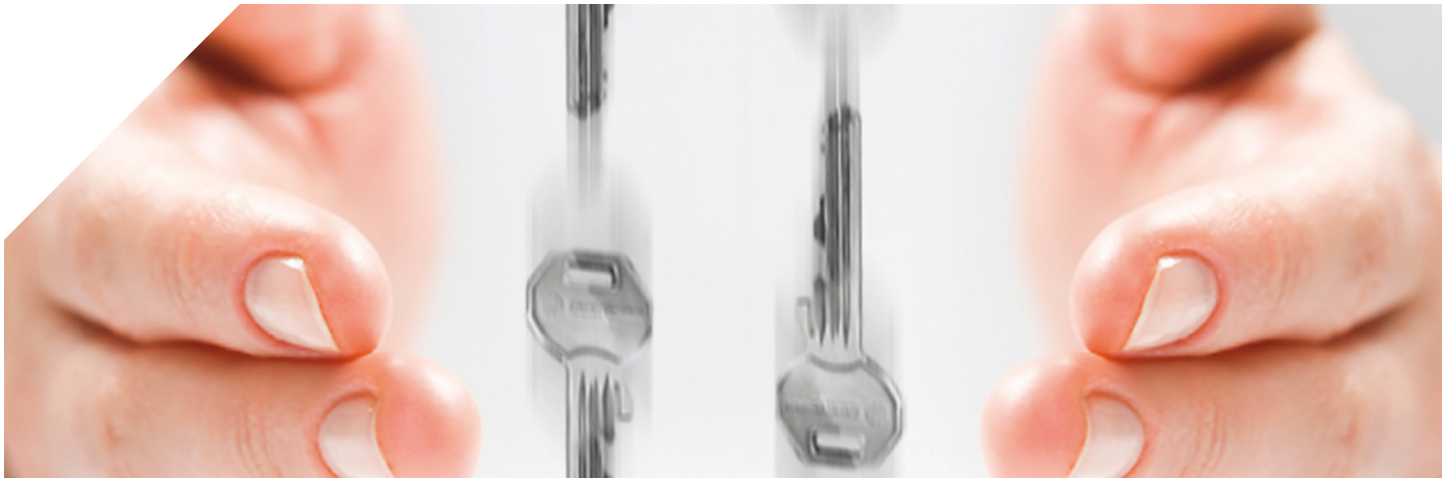
CRYPTOMATHIC

White Paper

Key Management Compliance - Explained



1 Introduction

Cryptographic key management is an umbrella term which refers to the various administration processes that govern the life cycle of keys and the keys' associated crypto material and metadata. Key life cycle stages include, but are not limited to, generation, storage, usage, update and revocation (see Fig. 1), and each of these stages brings with it particular administrative tasks that must be performed securely in an auditable manner.

Most products that use cryptographic keys have some sort of basic key management functionality, which in some cases may be augmented with a hardware security module (HSM) to generate and protect the keys. In these "standalone environments", keys are typically managed by proprietary systems, whose primary purpose is to generate one or more keys and certificates to be used for encryption or authentication, e.g. processing card payments. A proprietary interface works adequately for managing and maintaining a typically limited number of keys in a highly defined and isolated setting that is not expected to change over time.

The situation is different when an organization has large numbers of business applications utilizing a variety of keys and certificates. There are considerable overheads in training staff to operate dozens of different proprietary key management interfaces, which may have subtle incompatibilities, not to mention the cost and inefficiency overheads of operating and maintaining multiple systems. In this scenario, a general-purpose key management system will be more suitable. Cryptomathic's Crypto Key Management System (CKMS) is a perfect example of a versatile solution providing complete and automated life cycle key management.

There are strong business drivers towards achieving key management compliance, but if not carefully approached, it can add significant overheads to business operations - and does not necessarily result in better security.

This document provides an overview of the scope of key management compliance requirements, discusses their impact on the security and architecture of key management solutions, and offers recommendations for achieving compliance while simplifying audits.

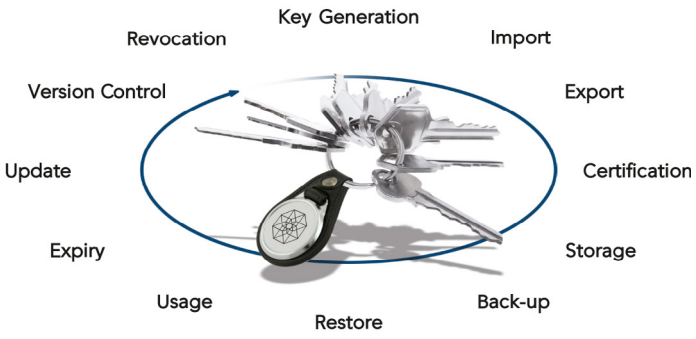


Figure 1: Key Life Cycle

2 Compliance Domains

Compliance regulations can be divided into individual compliance domains with explicit requirements:

- Physical security
- Personnel Security
- Logical Security

2.1 Physical Security

Physical security is about ensuring that valuable company assets cannot be accessed or removed from company premises without authorization, and preventing company employees from performing unauthorized actions by restricting their access to these assets. Physical security is the most visible of the compliance domains; employees may see locked doors for secure rooms or "man-trap" doors that aim to prevent tailgating, surveillance cameras, safes and so forth. In the context of key management, physical security requirements also act to protect hard copies of key material, and the computers and HSMs which store keys and run key management software.

Physical security works in conjunction with logical security, e.g. for managing access to and usage of hardware. Equipment for securing and handling confidential material is typically characterized as being one of three types:

- Tamper evident (tampering is detectable)
- Tamper proof or resistant (tampering is physically infeasible / difficult)
- Tamper responsive (tampering actively triggers appropriate countermeasures)

The most common intersection of physical security and key management is in relation to the specification and use of tamper protected hardware for safeguarding keys, such as HSMs and safes.

Physical security is a costly affair and non-compliances may result in re-construction and re-certification.

2.2 Personnel Security

Personnel must be assigned specific roles/privileges and their access to sensitive information must be on a strict need-to-know basis. Security awareness training should be provided. No single person should be relied upon for critical knowledge or system access, and all contact with security material must be thoroughly recorded.

Even if roles and privileges are well controlled - a 'bad actor' can cause disruption to the operation of a system. In the worst case a conspiracy of multiple operators could compromise processes and data. It is therefore often required that organizations conduct background checks on new employees involved in security related tasks.

2.3 Logical Security

Addressing the integrity of processes and procedures, logical security aims to protect an organization against the theft or abuse of information by non-physical means, and to ensure that both the framework and execution of business practices are designed and held to a specified security standard. The topic is broad and involves detailed requirements for operational processes as well as system architecture, including the design of infrastructure, use of cryptography and development of software. Key management also falls into this domain.

2.3.1 Operational Processes

The operational processes and procedures for any security system must be carefully documented and followed, with records kept and both random checks and regular audits to ensure compliance. Maintenance tasks are also in-scope, such as software patching, moves/adds/changes, monitoring of audit logs and alarms, etc. Where possible, security should be embedded within the systems and software to reduce the risk of accidental or malicious circumvention of security processes. This includes mechanisms such as strong authentication (using a minimum of two factors), following the principle of least-privilege, employing segmentation of duties (to prevent any one individual having too much authority) and enforcing dual-control (for operations that are security-critical and cannot be trusted to any single person).

2.3.2 Infrastructure Design

Infrastructure design covers the arrangement of network infrastructure such as cabling, switches and firewalls into a segmented architecture which creates safe zones for data at rest but also permits data transit between segments/zones within the organization. The secure segments of the network will have special requirements, including access control and intrusion detection.

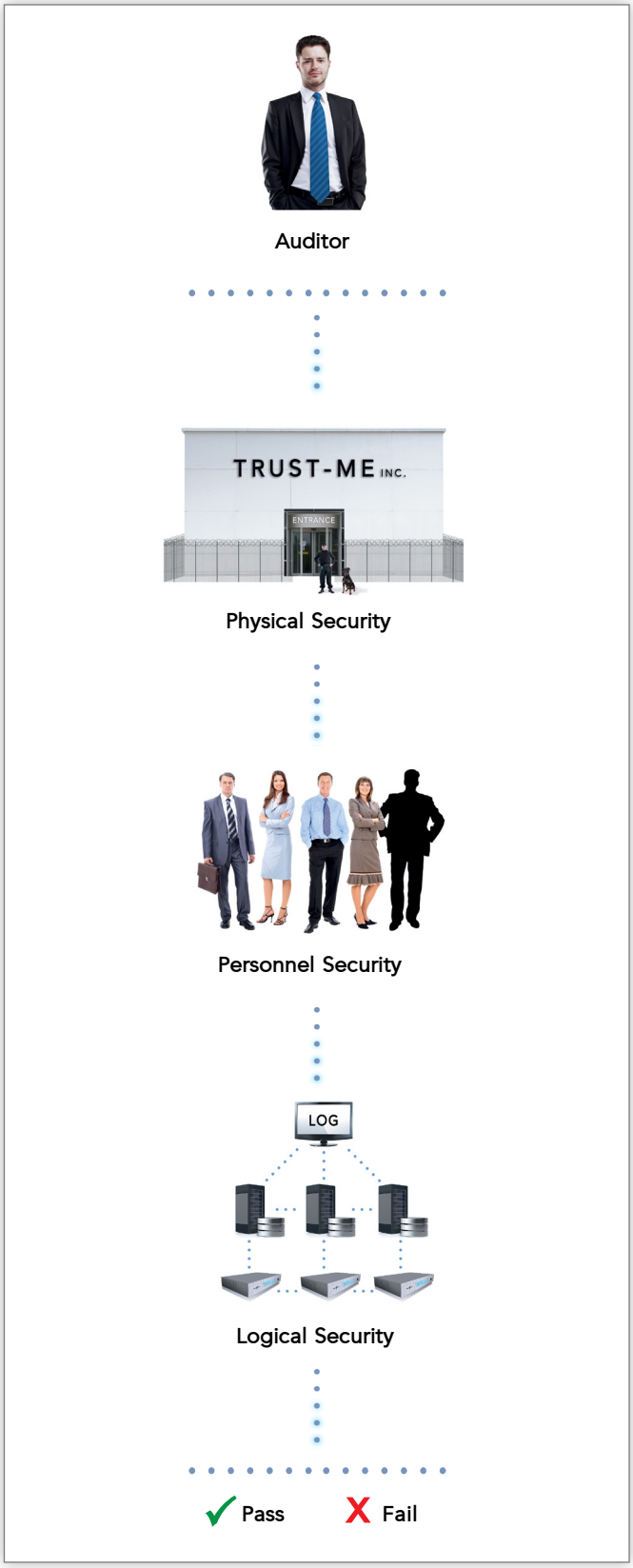


Figure 2: Auditor checking domains

Algorithm	Symmetric/Asymmetric	Typical Usage	Minimum Safe Key Length*
AES (Advanced Encryption Standard)	Symmetric	Encryption of conveyed/stored data in modern systems	128 bits
Triple DES (Data Encryption Standard)	Symmetric	Encryption of PINS and other banking related functions	168 bits (triple-length keys)
RSA (Rivest-Shamir-Adleman)	Asymmetric	Encryption - public key cryptography and digital signatures	2048 bits
DSA (Digital Signature Algorithm)	Asymmetric	Digital signatures, e.g. on documents	2048 bits
ECDSA (Elliptic Curve Digital Signature Algorithm	Aysmmetric	Small keys and strong cryptog-raphy for encryption and digital signatures	224 bits

Figure 3: Keys and Usage

2.3.3 Use of Cryptography

One of cryptography's most basic functions relates to employing an encryption algorithm that uses a key to encode confidential information, producing a scrambled result which is meaningless to others who do not possess the right key. To reverse the process, simply input the key and the unintelligible data to the algorithm.

Keys exist as different types, have different functions, and are used by different algorithms. Type and algorithm may be either symmetric, where the encryption key matches the decryption key, or asymmetric with different keys for encryption and decryption. (see Fig. 3)

Symmetric encryption

The function of a symmetric key is generally to act in a reversible cryptographic operation to ensure confidentiality of sensitive information. Examples of such keys are:

- *Application key:* A key used by a specific application for directly protecting application data
- *Master key:* A key used for protecting other keys, e.g. HSM master keys or (as in EMV) a key used to derive another key such as an application key. Derivation typically consists of encrypting specific data with a master key and the result is termed a derived key
- *KEK (Key Encryption Key):* One key encrypts another key, such as an application key, to secure it during transport/ storage
- *PIN Transport Key:* One key encrypts a PIN code to secure it during transport
- *ZMK (Zone Master Key):* A two-level scenario where one key encrypts transport keys that encrypt data/PINs

Typical symmetric key types/algorithms are 3DES and AES.

Asymmetric encryption

Asymmetric keys are used for encryption of sensitive data, or for demonstrating the authenticity and integrity of information – known as a digital signature. A digital signature shows that, through successful encryption of a signature over a document, the signatory (person singing the document) has access to the authentic signing key which corresponds to their identity.

The two different keys in an asymmetric key-pair are often termed the public key and the private key. The public key is available in 'the open' and typically embedded in a data structure (certificate) with additional information about the key. One of the use cases of asymmetric cryptography is securing online services, where anyone can encrypt using the public key but only the entity with the corresponding private key can decrypt.

2.3.4 Software Development

Computer software should follow standards regarding how cryptography is used. Where appropriate, any software development processes must be performed in a secure manner, which means using best practices such as change control for software and code review of critical components.

* Minimum safe key length is based on NIST SP 800-57 Part 1 recommendations

2.3.5 Key Management

Key management systems must be designed and implemented in accordance with the physical and logical security principles above in order to prevent keys from being compromised. In many cases, HSMs used for key management will have to be certified to FIPS 140-2 level 3 or higher, while software must follow practices such as enforcing dual control and functional separation of security activities. Dual control, AKA the four-eyes principle, ensures that two persons are present to authorize an important activity, whereas the similar sounding split-knowledge principle denotes splitting up sensitive information (such as a cryptographic key) between two or more persons so that a single person only knows part of the information and 'not the whole secret'. The secure logging of security-relevant actions is typically a compliance requirement on key management tools to both provide evidence of good behaviour and catch deliberate or accidental misconfigurations.

A commercial platform like Cryptomathic's CKMS meets the requirements for securely obtaining keys and transmitting them from a central point to one or more autonomous systems. It also enforces security policies, including dual control and split-knowledge, that may be required by an organization. Additionally, logging of all critical activities, combined with access to full audit logs from a single location, significantly simplifies management processes, proof of compliance and saves time when an audit occurs.

3 Applicable Compliance Programs

Compliance has three aspects worth noting here, namely standards, audit and certification.

3.1 Standards

Compliance may be subject to various internal and external standards. External key management standards include commonplace acronyms such as PCI, EMV, ISO and NIST, which are managed by industry bodies or governments and thus typically pertain to specific industries and/or geographies - see section 4. The rules set out in such standards do not necessarily prescribe exactly how to accomplish the goal, but upon inspection (during an audit), it should be clearly demonstrated how a requirement has been met (or not).

3.2 Audit

A compliance audit normally covers two points. One is to ensure that the business' processes and procedures meet the compliance objectives and the other is to check that the company *actually* follows these procedures. Documented policies and procedures will be provided and systems demonstrated to show how the relevant standards are adhered to. Not everything is investigated, and much is subject to interpretation, hence the audit process and auditors' assessment becomes influential.

Even with a rich understanding of compliance requirements, it is not possible in advance of an audit to single out any system guaranteed to pass the audit, because compliance is dependent both on the design and on the actual usage of the system.

3.3 Certification

Certification (sometimes called accreditation or validation) refers to achieving compliance with a particular standard through an independent evaluation process. The certification can be for a device or a whole system, and some certifications of a system can involve the use of separately certified devices. A classic example is the use of 'FIPS certified' HSMs for cryptography.

3.4 Compliance Dependencies

As described above, compliance typically consists of certification, audits and standards that follow a clear set of specifications. However, the process is also dependent upon other factors, such as the operating environment, type of data as well as type and function of cryptography.

Compliance is highly dependent on industry so it is important to determine which compliance authorities are relevant to key management for each individual business.

Some industries are subject to particularly stringent regulation, primarily government bodies and banking / finance. Regulation in banking is widespread with tough requirements and enforcement in place for most functions, such as accounting, currencies, data protection, investment, payments and trade. Key management compliance in banking is no exception, where a strict set of rules are defined by internal auditing authorities, international card payment schemes and industry bodies, not to mention national and international legislation.

4 Compliance Authorities

It is impractical to compile an exhaustive list of compliance authorities that are concerned with key management. This section aims at reducing the level of complexity by highlighting major authorities that have a significant impact on key management compliance, particularly in the financial sector.

4.1 NIST

The National Institute of Standards and Technology (NIST) produces the Federal Information Processing Standards (FIPS), which covers computer system security and technology. Whilst intended primarily for the US federal market, NIST standards and guidance have been widely adopted around the world, especially within the financial industry. Particularly relevant to key management is the FIPS 140 standard, where topics refer to approved cryptographic algorithms such as AES and dedicated electronics for cryptographic calculations – Hardware Security Modules (HSMs).

4.2 PCI

The Payment Card Industry (PCI) was founded by the major payment schemes. PCI controls the data security aspects for the entire life cycle of payment cards, from pre-production to end-of-life. All processes and businesses involving payment cards fall under the PCI requirements. PCI maintains two primary programs, PCI DSS and PCI PTS.

4.2.1 PCI DSS

PCI DSS: Data Security Standard. Requirements to secure cardholder data (name, account number, security data) in storage and transmission. It includes key management procedures for the cryptographic keys. Read the white paper on how Cryptomathic CKMS helps businesses solve PCI DSS key management compliance requirements. Read Cryptomathic's White Paper on PCI-DSS & Key Management

4.2.2 PCI PTS

PCI PTS: PIN Transaction Security. Requirements to secure cardholder PINs. Includes PIN management, ATM/POS, HSMs, and key management involved (key generation, key loading, key distribution, and key life cycle management).

4.3 ISO

The International Organization for Standardization maintains the ISO 11568-X family of standards concerning key management within the retail banking and financial services industry. It also maintains ISO/IEC 27001, which defines requirements for developing and operating an information security management system against which organizations may be audited and receive accreditation.

4.4 Common Criteria

Common Criteria offers security certificates for IT solutions. To receive a certificate, hardware or software products need to pass an evaluation which follows a rigorous assessment methodology that covers the implementation and evaluation of a product against relevant protection profiles.

4.5 Payment Schemes

The major players in payment card key management compliance are the actual payment schemes, requiring both logical and physical compliance for third party service providers. They consist foremost of the multinational organizations with global brands and reach, chiefly American Express, Discover, JCB, Mastercard and Visa. In additional to the global players there are a number of regional and national payment schemes such as China UnionPay, Cartes Bancaires (Moneo), Interac (Interac), SAMA (SPAN2) and SIA (Bancomat), which may have their own set of compliance requirements.

4.6 PKI Schemes and Trust Service Providers

The EU eIDAS regulation on trust services and electronic signatures mandates that a supervisory body is established in different member states (typically a state body); this authority supervises the local qualified trust service providers and ensures compliance against EU ETSI/CEN standards and also national electronic signature law for the generation of (qualified) electronic signatures, certificates, time stamps etc.

In practice, the actual assessment/accreditation is performed by an assessor which undertakes onsite conformity assessments (aka audit) to evaluate the compliance of trust service providers against security requirements defined on a European level.

Relevant technical standards include those of ETSI (European Telecommunications Standards Institute) and CEN (Comité Européen de Normalisation).

4.7 Other External Compliance

There is a large number of other external compliance authorities that are beyond the scope of this document. These are highly dependent on industry and offered services and may include other regulators, customers, partners and so forth. Increasingly, cyber insurance policies are influencing corporate security strategy as companies seek to cover their cyber risk while minimizing their insurance premiums.

4.8 Regulatory Compliance

Regulations such as GDPR, HIPAA, Sarbanes Oxley and others may apply in certain geographies, having implications for the protection of sensitive and private data (and consequently the use of encryption and key management).

4.9 Internal Compliance

Internal compliance is a very important aspect for many organizations and it also impacts on key management. Whereas service providers are often faced with rigorous requirements and audits from external governing bodies it is common for

large organizations to have very tight requirements determined by internal audit departments to reduce the risk and impact of cyber attacks and data breaches. Internal auditing is in many cases more strict and rigid than that of external authorities, and financial institutions dealing with internal fraud amongst other issues are particularly tight on internal compliance.

4.10 Which Compliance Authorities Apply?

In order to ensure compliance, an important first step is to discover which compliance authorities are relevant to the business. The best way to find out what applies to a specific organization is to do the research, which includes contacting industry experts as well as leading solutions providers.

Considering the severity of compliance failure, not all compliance authorities are equal. Some attract more serious consequences upon failure to comply, some mean you cannot operate in the market at all. Sarbanes Oxley is US Federal Law, PCI attracts significant fines and FIPS is a qualification for entering into the hardware security market. Hence, it's not just the number of compliance regimes that must be addressed - it's their nature and the type of expert you might need to consult with, which are the important considerations.

5 How to Ensure Compliance

Like most aspects of IT security, key management processes could be created to meet even the toughest of compliance requirements, but at capital and labor cost that would be prohibitive (except perhaps in the defense market). Moreover, it might become a significant impediment to the organization's essential business operations. So the real question is how to ensure compliance while managing costs, supporting business operations and efficiently scaling as a business grows? The most important factors to ensure compliance are to:

- Understand which standards and regulations your business must comply with (both internal and external)
- Understand what is needed to meet their mandatory requirements
- Implement techniques that effectively enforce these rules for all environments and processes within scope

Many organizations aim to meet the minimum given set of compliance requirements, but when considering solutions there may be opportunities to also reduce systemic risk and save ongoing costs. e.g. through automating crypto key management processes.

5.1 Best Practice

Best practices for key management cover both improving actual security and helping security compliance requirements. The following are general suggestions that are not informed by compliance with any particular standard.

- Place sensitive equipment inside a dedicated High Security Area. By this, a number of physical, logical and personnel security issues are covered.
- Store sensitive material, including keys, using industry-standard tamper evident / resistant measures (e.g. HSMs).
- Use integrity-protected audit logs for electronic systems and paper audit logs for the rest. For anything particularly sensitive, paper logs should be signed off by a second identifiable person.
- Use the well-established principles of dual control, split knowledge and segregation of duties to counter the lone insider threat.
- Use two-factor authentication to prevent unauthorized access.
- Sensitive data should be encrypted whenever possible, whether in transit or at rest.

6 Compliance Audits

The actual audit criteria and process depend on the compliance authority, but generally the following elements are included:

- Audit initiation: scheduled or unannounced
- The audit: see above for relevant compliance domain(s); the scope may include documented processes and procedures, evidence and artefacts (both physical and logical - e.g. network diagrams, tamper-evident labels, paper records, computer logs, meeting minutes, etc.), ad-hoc or systematic inspection/testing of security mitigations, personnel interviews, and so forth
- Report findings and non-compliances
- Verdict: approved, partially approved (e.g. subject to a list of actions), or not approved

Audits are resource-intensive activities. Companies typically undergo several audits yearly from different compliance

authorities. With a heterogeneous assembly of different systems, the particularities of each will be investigated and the full documentation set examined.

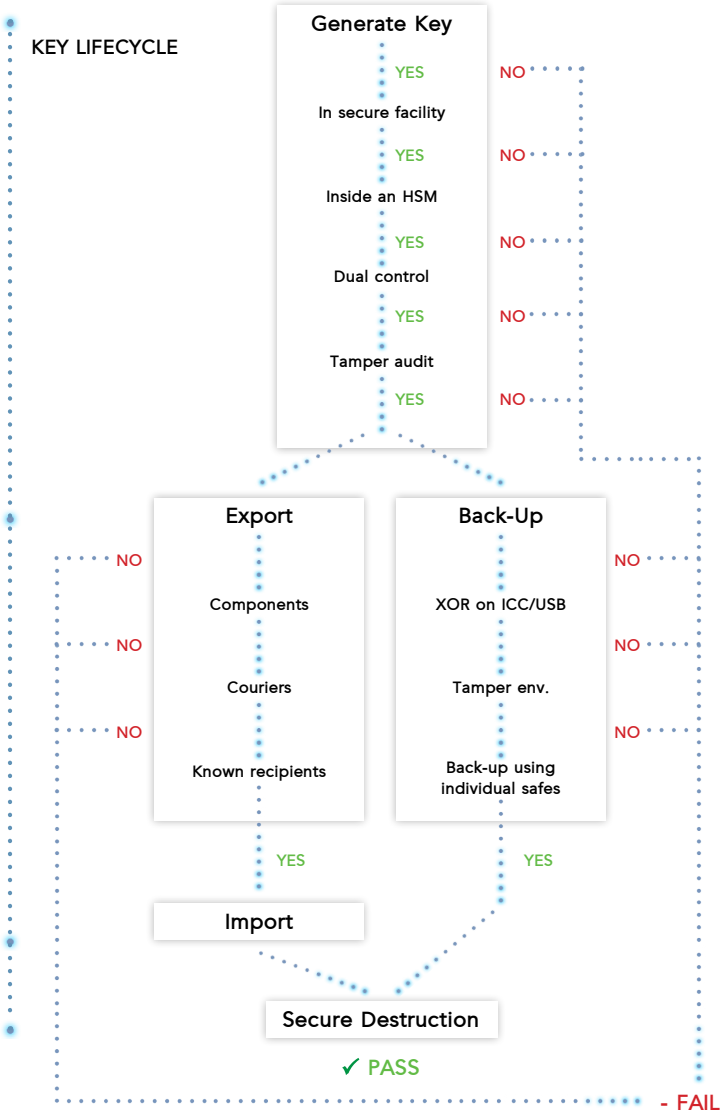


Figure 5: Brief Guide to Key Management Compliance

7 Centralized and Automated Key Management

Data security is sometimes reduced to the goal of compliance where, if a system complies with relevant standards and regulations, then all is well.

While compliance is often necessary, and may inform good behaviour, it does not guarantee 'good security'. Key management processes are an area where a well-chosen solution can both ease compliance AND quantifiably improve security. Automation can both increase efficiency and improve security, by reducing the risk of human error.

A centralized and automated key management can offer the following advantages:

- **One system to audit:** as opposed to application-specific key management
- **A single audit log:** complete history of each key, regardless of the end application
- **One documentation set for key management procedures**
- **Only one set of operators, who only need to understand one system**
- **Automatic key management:**
    1. Ensures keys are rotated when they should be
    2. Ensures keys are delivered when they should be
    3. Reduces the risk of human error

7.1 Cyptomathic CKMS

Cryptomathic is a leading expert in designing and implementing state-of-the-art automated life cycle key management systems.

Cryptomathic's CKMS (Crypto Key Management System) is a centralized solution for securely managing the entire lifecycle of application keys at large scale. CKMS has a global client base including some of the world's largest financial institutions, card payment schemes, data processors and technology manufacturers. The first version of CKMS was released in the late 90s and has consistently been the first to support the most recent industry standards ever since. CKMS helps ensure compliance, improve security and efficiency, shorten time to market and save security costs (direct and indirect).

The first version of CKMS was released in the late 90s and has consistently been the first to support the most recent industry standards ever since. CKMS helps ensure compliance, improve security and efficiency, shorten time to market and save security costs (direct and indirect).

See more information about Cryptomathic's solutions for key & cryptography management on:
https://www.cryptomathic.com/products/key-management

8 Conclusion

As described in this white paper, compliance is not necessarily difficult to achieve, it is typically a question of implementing a certain set of standards and procedures. However, documenting and demonstrating compliance is a completely different matter, and costly at a bare minimum. Some of the main takeways of this paper are summarized below:

- Recommendations and instructions related to key management vary a lot by industry sectors - be clear about what you have to comply with
- There are distinct considerations for the security of the Physical, Logical and Personnel (HR) domains - each must be fully examined in its own right to ensure a holistic approach to security
- No product or service can magically guarantee compliance with any particular standard - good configuration and operation is essential as is the trustworthiness of the people managing it
- Compliance may be non-negotiable for many businesses, but don't consider compliance as the only goal - be aware of the improvements that can be made to 'real' security along the road to compliance
- A well chosen and flexible automated key management system can allow confident compliance together with with reduced operational costs and a stronger security posture.

Useful links:

http://www.ansi.org/
http://csrc.nist.gov/
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2014.htm
https://www.commoncriteriaportal.org/
https://www.cryptomathic.com/EMV_Key_Management_Explained
http://www.emvco.com/specifications.aspx
http://www.etsi.org/
http://www.iso.org/
https://www.pcisecuritystandards.org
https://www.pcisecuritystandards.org/security_standards/documents.php