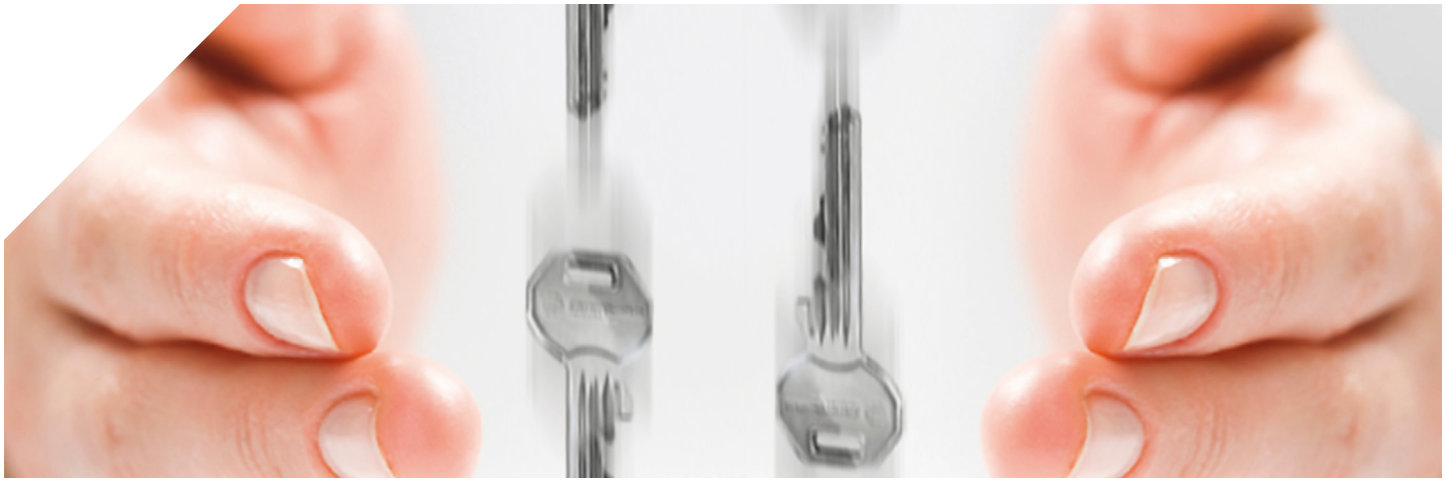
CRYPTOMATHIC

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, certification, distribution and revocation, archival and destruction, and each of these stages brings with it particular administrative tasks that must be performed securely in an auditable manner. The exact processes vary depending upon a number of factors, such as key type (symmetric or asymmetric), environment in which they are used and industry.

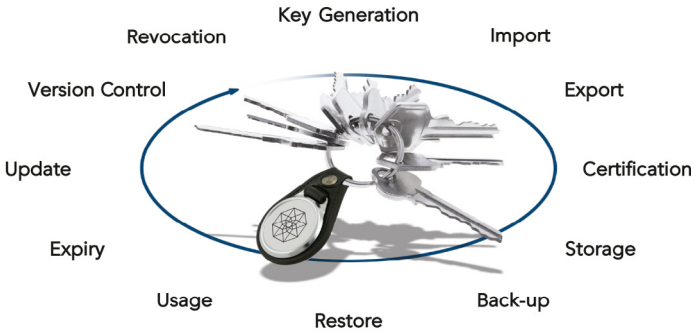


Figure 1: Key Life Cycle

All software products that use cryptographic keys have some sort of basic key management functionality. 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 rather limited number of keys in a highly defined and isolated setting that is not expected to change over time.

The situation is different for large numbers of business applications utilising a variety of keys and certificates. In this setting, there are considerable overheads in training staff to operate dozens of different proprietary key management interfaces, which may have subtle incompatibilities, so a general-purpose key management system will be more suitable. Cryptomathic Key Management System (CKMS) is a perfect example of a versatile solution providing complete and automated life cycle key management.

Regardless of which system or solution is used, the cryptographic keys will always need to be managed using secure processes. However, the internal and external compliance requirements that organisations, such as financial institutions, must adhere to are becoming ever more influential in determining how to manage keys. Achieving compliance is a strong business driver, but if not carefully approached, it can add significant overheads to business operations and does not necessarily result in better security. This document aims to provide an overview of the scope of key management compliance requirements, discuss their impact on the architecture of key management solutions, and offer recommendations for achieving compliance while simplifying audits.

Overseeing, ensuring and being able to demonstrate that keys are managed securely is essentially what key management compliance is all about.

2 Compliance Domains

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

- Physical Security
- Logical Security
- Personnel security

2.1 Physical Security

Physical security is about ensuring that valuable company assets cannot be removed from company premises without authorisation, and preventing company employees from performing unauthorised actions by restricting their movement. Physical security is the most visible form of compliance, employees may see locked doors for secure rooms, "man-trap" doors that aim to prevent tail-gating and theft, and over and above the visible elements, physical security requirements may mandate movement detectors, positions of surveillance cameras and so forth. In the context of key management, physical security requirements also act to protect envelopes containing printed copies of key material, and protect the computers and hardware security modules (HSMs), which run key management software.

Physical security works in conjunction with logical security and they correlate on e.g. access control and usage of hardware. Equipment for securing and handling confidential material must essentially be of a protecting nature and subtle distinctions exist between:

- Tamper evident [tampering is detectable]
- Tamper proof/resistant [tampering is physically infeasible]
- Tamper responsive [tampering triggers appropriate countermeasures]

Where physical compliance relates to key management, it is worth mentioning that tamper resistant hardware for managing keys and key components (such as HSMs and safes) often need to be in place and, moreover, stored in rooms with restricted access. Tamper resistant devices should be securely fixed so that they cannot be easily removed, e.g. bolted to a solid unmovable object. Cameras monitoring the devices and individuals accessing them add to the security, along with

mantraps that ensure staff cannot leave with any items of even moderate weight. Additional security measures may also be applicable.

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

2.2 Logical Security

Addressing the logical integrity of processes and procedures, logical security aims to protect an organisation against the theft or abuse of information, rather than physical objects, and to ensure that both framework and execution of business practices are designed and held to a specified security standard in this regard. The topic is broad and involves detailed requirements for cryptographic, infrastructure and software design.

2.2.1 Cryptographic Design

In order to address cryptographic design we will introduce the reader to an important set of terminologies. An encryption algorithm 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 decryption algorithm.

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

The function of a symmetric key is generally to act in a reversible cryptographic operation to ensure confidentiality of sensitive information, such as:

- 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
- Key part: When a key is transported it can be in encrypted form, or it can simply be split into several components or parts, each of which are transported separately and assembled on arrival. The most used method by far is the exclusive-or (X-OR) splitting mechanism and secondly an n-of-m mechanism where any n-size subset of m components are needed to assemble the original key
- Typical symmetric key types/algorithms are DES, triple-DES, 3-key triple-DES and AES

Exchanging encrypted information between two entities defines an encryption zone, wherein entitles exchange keys for encryption/ decryption and communicates encrypted data.

Asymmetric keys are used for encryption of sensitive data where many parties may wish to encrypt but only a few decrypt, or for demonstrating the authenticity of information from a particular source – known as a digital signature. A digital signature shows that through successful encryption of a signature over a document, the decryptor (known as the signer) has access to the authentic decryption 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 part is available in 'the open' and typically embedded in a data structure with additional information about the key. Hence anyone can encrypt using the public key but only the entity with the private key (aka secret key) can decrypt. Reversely, only one entity can encrypt/digitally sign data using the private key and all can decrypt/verify the signed data using the public key. These techniques are often deployed in a two-level structure where the data structure with the public key is encrypted by yet another private part from another key. This way anyone with access to the corresponding public key can decrypt the original key and hence verify that its origin is authentic and the key can be trusted. Such a data structure which is private-key-encrypted [here termed 'signed] in full or partially is denoted a digital certificate.

Cryptographic design sets the encryption zones and key usages. It includes key management (key generation/distribution/life cycles) and all procedures around them including how to securely operate the key management equipment.

It is worth pointing out that encrypting data "at rest" (that is data sitting on your hard drive, doing nothing) is a very different proposition from encrypting "dynamic" data (data that is being used- a good example is an email displayed on your screen). The security assurances that can be given for dynamic data are less than those that can be given for data at rest. The simple reason is that, at some point, data being used must be in the clear (otherwise it's useless- just like a scrambled-text email) whereas static data can be safely scrambled indefinitely. One practical example of how this property is exploited is with encrypted tape drive

2.2.2 Infrastructure Design

Infrastructure design covers the arrangement of network infrastructure

Algorithm	Symmetric/Asymmetric	Usage	Safe Key Length
AES (Advanced Encryption Standard)	Symmetric	Encryption of conveyed/stored data Modern systems	128 bits
Triple DES (Data Encryption Standard)	Symmetric	Encryption of conveyed/stored data, eg banking networks	56 bits (single-length keys) 112 bits (double-length keys) 168 bits (triple-length keys)
RSA (Rivest-Shamir-Adleman)	Asymmetric	Encryption - public key cryptography and digital signatures	1024 bits
DSA (Digital Signature Algorithm)	Asymmetric	Digital signatures, eg on documents	1024/160 bits
ECC (Elliptic Curve Cryptography)	Aysmmetric	Mobile/Chip (small keys and strong cryptography) for encryption and digital signatures	160 bits
MAC (Message Authentication Code)	One-way function	Authentication of cryptographically stamped data	56 bits (single-length keys) 112 bits (double-length keys) 168 bits (triple-length keys)
SHA (Secure Hash Algorithm)	One-way function	No key authentication of algorithmically stamped data	No keys
SSL (protocol) (Secure Sockets Layer)	Asymmetric + Symmetric	Network communication security Asymmetric endpoint auth Symmetric message encryption	2048/112 bits

Figure 2: Keys and Usage

such as cabling, switches and firewalls into a segmented architecture which creates safe locations for data at rest but also permits data transit between segments within the organisation. The secure segments of the network will have special requirements, including restrictions on information access on networks and systems such as internet control, line-encryption and audit logging.

2.2.3 Software Design

Computer software on a site has to comply with cryptographic standards regarding how cryptography is used, but additionally, the entire software development process must be performed in a compliant manner, which means using best practices such as change control for software and code review of critical components.

Certain requirements must however be met and in many cases HSMs for key management will have to be certified to FIPS 140-2 level 3 or higher, while software must follow prescriptions such as enforcing dual control for functional separation of security activities. Dual control, aka the four-eyes principle ensures that two persons are present to authorise an important activity whereas the similar sounding split-knowledge principle denotes splitting up information to two or more persons so that a single person only knows part of the information and 'not the whole secret'. Secure logging of security relevant actions is typically a compliance requirement to software design, in order to detect security violations if/when they happen.

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

A commercial platform like the Cryptomathic CKMS meets the requirements for securely obtaining keys and transmitting them from a central point to one or more autonomous systems. Additionally, logging of all key activities combined with access to full logs from a single location significantly simplify management processes, proof of compliance and saves time if or when the auditor comes around. For more information please read CKMS case studies, which are available for download on the Cryptomathic web site.

2.3 Personnel Security

There is increased focus on personnel with security clearance. Personnel must be assigned specific roles/privileges and their access to information must be on a strict need-to-know basis. No single person can be relied upon for critical knowledge or system access, and all contact with

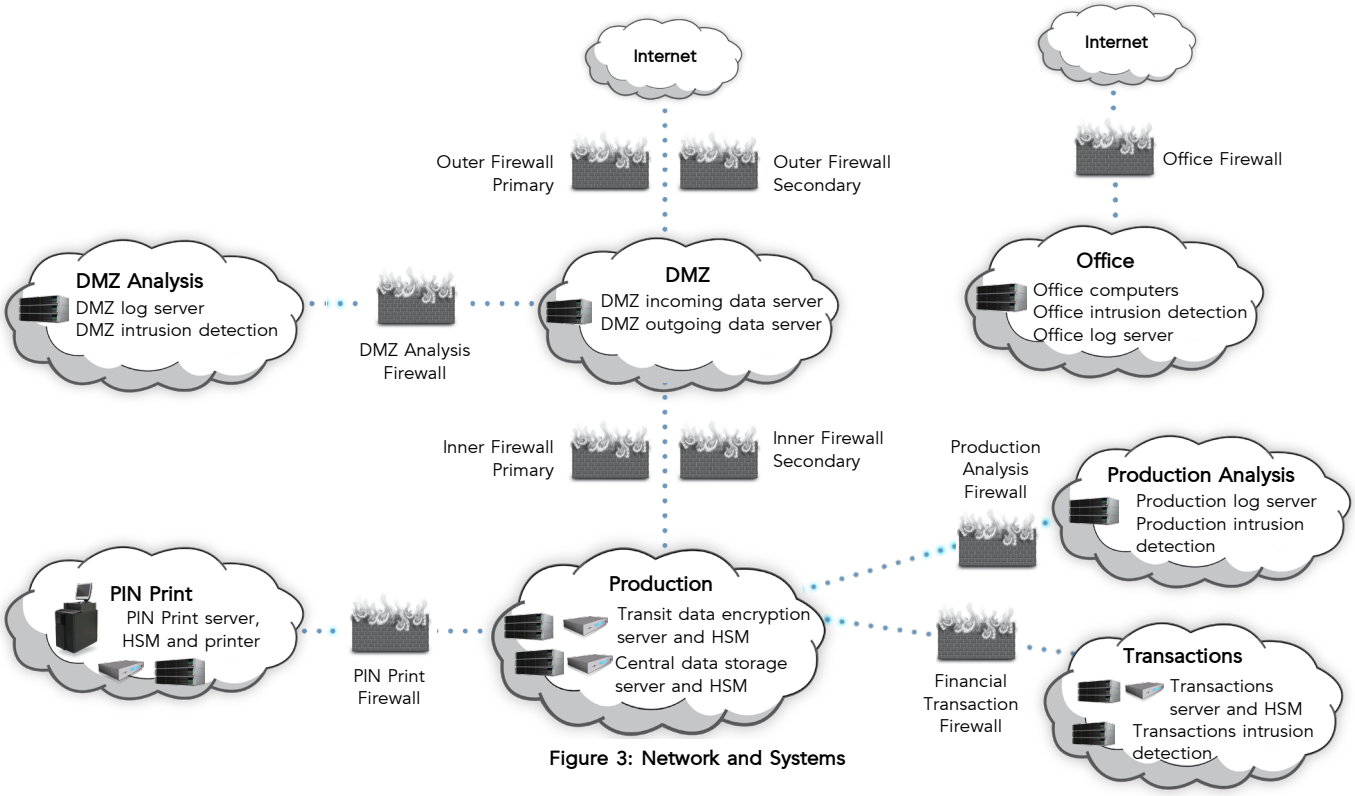


Figure 3: Network and Systems

security material must be thoroughly recorded.

Even though no single person should be relied upon to carry out vital security tasks, an individual with bad intentions can still cause havoc. It is also possible for multiple individuals to conspire for criminal purposes, e.g. to defraud a company. It is therefore vital and often required, that organisations conduct background checks on new employees and security related tasks. Changing roles in organisations also help ensure security, which after all is the key driver of compliance.

3 Applicable Compliance Programs

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

3.1 Certification Compliance

Certification compliance is all about getting the tick in the box from the auditor for correctly following the specific compliance authority standards. The certification can be for a device or a whole operation, and some certifications of a larger operation can involve the use of separately certified devices. A classic example is the use of FIPS certified HSMs for cryptography.

3.2 Standards Compliance

Key management compliance may be subject to various internal and external standards. External standards include commonplace acronyms such as PCI, EMV and NIST. The rules set out in the relevant standards do not necessarily prescribe how to accomplish the goal, but upon inspection, it is clear whether a requirement has been met or not.

3.3 Audit Compliance

A compliance audit normally covers two points. One is to ensure that the 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 shared and systems demonstrated to show how the compliance standards are adhered to. Not everything is investigated, and much is subject to interpretation, hence the audit process and auditors' assessment becomes influential.

3.4 Compliance Dependencies, Including Industry

Even though compliance consists of certification, standards and audits that typically follow a clear set of definitions and specifications, the process is also quite dependent upon other factors such as operating environment, type of data as well as type and function of crypto.

The more an organisation knows about its set-up and is able to demonstrate and document on the fly the more likely it is that an auditor will be convinced.

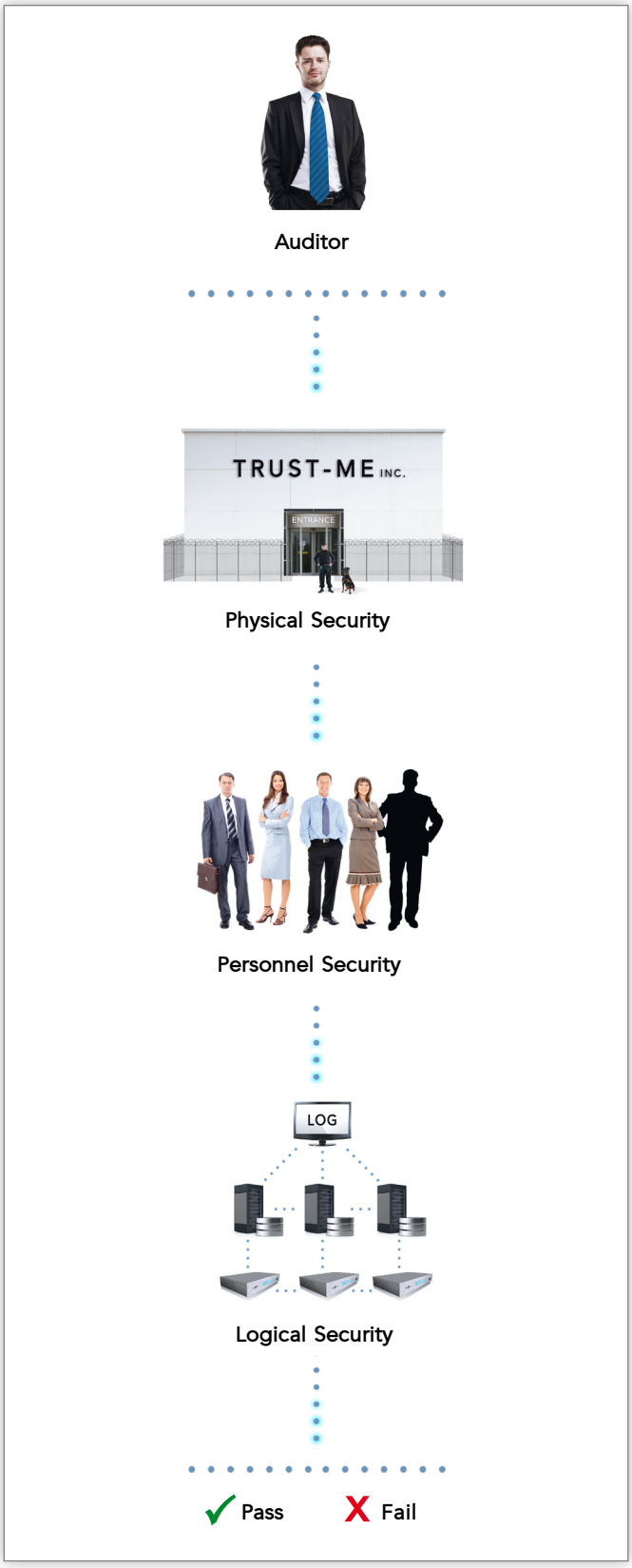


Figure 4: Auditor Checking domains

On the other end of the scale some industries are subject to particularly stringent regulation, primarily government and banking. Regulation

On the other end of the scale some industries are subject to particularly stringent regulation, primarily government and banking. Regulation in banking is often heavy and widespread with tough requirements and enforcement in place by authorities 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, banking standard organisations not to mention national and international legislation.

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

4 Compliance Authorities

It is considered practically impossible and fairly pointless to compile an exhaustive list of compliance authorities that are remotely relevant to key management. This section aims at reducing the level of complexity by highlighting major authorities that play a significant impact on key management compliance, particularly in the financial sector.

4.1 NIST

NIST (National Institute of Standards and Technology) produces the FIPS[1] standard that covers computer systems security and technology. Particular topics are 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[2] 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:

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.

---

[1] Federal Information Processing Standard
[2] American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.

4.2.2 PCI PTS

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

4.3 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 rigorous assessment methodology that covers the process of product specification, the implementation and evaluation of a computer's security against relevant protection profiles.

4.4 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 (see previous section for more information about logical and physical compliance). They consist foremost of the multinational organisations with global brands and reach which are American Express, Discover, JCB, MasterCard and Visa. In additional to the international 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.

4.5 PKI Schemes and Trust Service Providers

The European Directive on 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 signatures 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 and also national levels.

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

4.6 Other External Compliance

There is also a large number of other external compliance authorities. These are highly dependent on industry and offered services and may include other regulators, customers, partners and so forth.

4.7 Process Compliance

Process compliance in the form of ISO (e.g. 27001), Sarbanes Oxley as well as other commonly used de facto or standard processes may apply and although many of these simply require data to be encrypted without providing a great level of detail it is worthwhile checking in most cases.

4.8 Internal Compliance

Internal compliance is a very important aspect for many organisations and it also impacts on key management.

Whereas service providers are often faced with rigorous requirements and audit from external governing bodies it is common for large organisations to have very tight requirements determined by internal audit departments. 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.

4.9 Which Compliance Authorities Apply?

In order to ensure compliance an important first step is to discover which compliance authorities are relevant to the business. At one end of the spectrum it could be none and at the other end it could be countless authorities and it all depends on business and industry (as mentioned in Section 3) along with a variety of other factors, e.g. location, reputation, solution design, contractual requirements and so forth.

The best way to find out what applies to a specific organisation is to do the research, which includes contacting industry experts as well as leading solutions providers, such as Cryptomathic. Regardless of which compliance authorities and type of compliance that may be applicable to the business it is always worth to keep in mind that compliance offers a means to controlling risk by highlighting and subsequently minimising it significantly, even if compliance is not a legal requirement of direct business obligation (which is not always the case for key management). See Figure 5 for a list of influential standards and authorities.

In the light of severity of compliance failure not all compliance authorities are equal. Some attract more serious consequences upon failure to comply, some mean you don't get to play in the security game at all. Sarbanes Oxley is Federal Law, PCI attracts significant fines (6 figures and upwards), ISO and FIPS are qualifications for entering into the hardware security market. So 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 that is a big consideration.

5 How To Ensure Compliance

So how do we ensure compliance? Although the question is obvious, the answer is less so. Like most aspects of IT security, key management can easily meet even the toughest of compliance

Compliance: Influential Standards and Authorities
ISO/IEC 11770-1 – Standardises a general model for the key lifecycle, key management services (Generate, Activate, Deactivate, Reactivate, Destruction) and key state transitions (Pending Active, Active, Post Active)
ISO/IEC 11770-2 – Key Management, Part 2: Mechanisms Using Symmetric Key Management Techniques
ISO/IEC 11770-2 – Key Management, Part 3: Mechanisms Using Asymmetric Techniques (RSA)
ISO/IEC 11568 – Banking – Key Management (Retail)
ISO/IEC 27001 – Information Security Management Systems (ISMS)
ANSI X9.17 – Financial Institution Key Management (Wholesale)
ANSI X9.24 – Retail Financial Services Symmetric Key Management
ANSI TR-31 – Interoperable Secure Key Exchange Key Block Specification
EMV – Book 2: Security and Key Management
FIPS: DSS (Digital Signature Standard) 140-2 (Security Requirements for Cryptographic Modules)
RSA: PKCS 1-15
Payment Schemes: • International Schemes: AmEx, Discover, JCB, MasterCard, Visa • National Schemes: Cartes Bancaires, CUP, Interac, Rupay, SAMA and SIA
Interoperability Standards: GlobalPlatform, KMIP (OASIS), Trusted Computing Group
Government Bodies: CESG, Common Criteria, EPC, ETSI, EU, NIST, etc

Figure 5: Compliance - influential Standards and Authorities

requirements but it probably consumes excessive resources, so the real question is how to ensure compliance while managing costs. The two most important factors to ensure compliance are to:

• Understand what is needed to meet the minimum requirements
• Implement techniques that effectively enforce these rules for all environments and processes within scope

Most organisations aim to meet the minimum given set of compliance requirements, but since compliance is already a focus it is worthwhile to also explore other practical measures above and beyond the minimum set of requirements for multiple purposes, such as minimising overall systemic risk, save cost through automating crypto key management processes and so on.

It is important for compliance that the organisation's operational processes and environment is up to date. It should go without saying that if key management procedures are not followed and keys are managed outside of the securely designed environments it is impossible to ensure compliance. Even more alarming, this will create a high and unmanageable business risk waiting for the worst-case scenario to become reality.

It should also be pointed out that key management compliance relies heavily on secure design, which will not work properly, and as intended, if it can be misused or incorrectly implemented.

Another often overlooked factor that plays its part is the human element. Streamlining and automating processes help to eliminate human error, which is a real threat since humans are prone to making mistakes.

Human error can be minimised if the management of an organisation

takes time and effort to ensure that rules and procedures are actually followed and more importantly understood by all relevant team members.

An example could be an employee that is tasked with ensuring that a cryptographic key is securely managed but where the employee does not possess the adequate level of knowledge to understand exactly how that is done (see the diagram below for details on secure key management).

Finally maintaining a sensible level of knowledge about all systems and processes will minimise risk, help make audit inspections less painful and better consider security when applying changes.

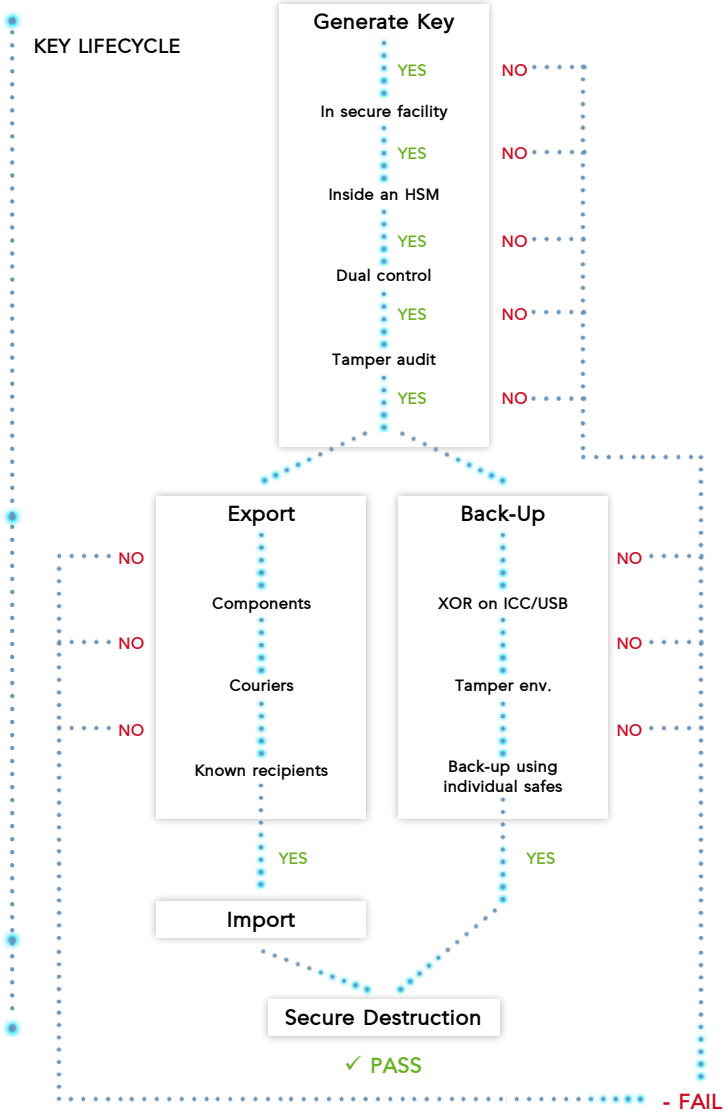


Figure 6: Guide to Key Compliance

5.1 Best Practice

The purpose of best practices for key management is twofold, consisting of actual security requirements and security compliance requirements.

There are real security concerns such as per default always placing sensitive equipment and networks inside a dedicated High Security Area. By this a number of security issues are already covered with controlled personnel access, controlled data access, activity logging requirements etc. On a smaller scale important defaults include storing sensitive material such as USB sticks containing keys or backup data, or key transfer paper with key components written on them, into industry standard tamper evident envelopes inside a safe. Dual control on all potentially dangerous actions and written change requests before changing parameters and settings in electronic systems are also wise. Such practices enhance actual security and are a likely part of the *security compliance requirements* against which you will be audited.

The *security compliance requirements* aims at increasing security and they are written based on both theoretical speculations on how to counter unintended activities but also on practical experiences. A well proven experience is that people tend to choose the easiest way. It is easier for the IT system administrator to have sole free access to the server room and keep the physical keys for the cabinets in there where the HSMs are located. But then one person can in principle get unlogged access to data and systems he alone should not have access to, and one foresees a non-compliance.

So assume that compliance rules and auditors will demand that it will not be up to one single person to evaluate or decide whether security or confidentiality shall be compromised.

Which best practises should you then adopt? Well, start by logging all activities. Electronically tamper evident logs for electronic systems and manual paper logs for the rest. For anything even remotely sensitive the manual logs should be signed off by a second identifiable person. Grant access only on a need-to basis. Prevent any single person from changing anything unless having in approved writing requested to do so. Let no single person have access to information or systems that are security sensitive. Split secrets between multiple persons i.e. what is commonly termed split knowledge. Put dual control on all security sensitive activities including physical access i.e. don't allow anyone to be alone near sensitive equipment, even if it is locked inside a steel cabinet - maybe they have an unregistered key for it.

These considerations may sound a bit drastic, but as the compliance authorities rightfully speculate, anyone could be a criminal - if employees were all trusted there would be no need for security. In any case, most compliance regulations demand security at the level indicated above, so we suggest to deploy this line of thinking into the best practises.

6 Compliance Audits

Audits are reviews, either self-assessments or inspections. 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)
- Report findings and non-compliance
- Verdict: approved, partially approved, or not approved

The auditor will acquire an overview, identify compliance domains and examine them. Audits may involve personnel interviews and review of procedures and documentation. Some authorities mandate employee

QUESTIONNAIRE ITEM	Y/N	COMMENTS
Do you ensure that HSMs are kept under physical dual control at all times?	Y	
Do you ensure that a generated key is not at any time observable or otherwise accessible in plain text to any person during the generation process?	Y	
Are any cryptographic keys hard-coded into software?	Y	The key to authenticate the transaction server to the HSM hs hard-coded
Is the identity of individual key custodians restricted on a need-to-know basis and not made available in generally available documentation?	Y	
Is an inventory of the contents of key storage safes maintained and audited quarterly?	Y	
Are transport keys used to encrypt other keys for conveyance unique per key zone?)	N	The same PIN transport key is used for encrypting PINs to the PIN printer and to the PIN verification server
Do key management logs contain for each entry: • The date and time of when the activity took place? • The action taken (e.g., key generation, key destruction)? • Name and signature of the person(s) performing the action? • Countersignature of the security manager?	Y	
Do you implement daily, automated analysis reports to monitor firewall activity?	Y	
Are all removable media (e.g., USB devices, tapes, discs) within the high security area labelled with unique identifier and data classification?	Y	
Are account numbers masked when displayed or printed unless there is a written issuer authorization?	N	Account numbers are shown in full on the fraud analysis monitor
Do you receive data only from pre-authorized sources?	Y	
Does manually deleted data include sign-off by a second authorized person?	Y	
Do you conduct quarterly audits to ensure that all data beyond the data retention period has been deleted?	N	Bi-annual audits are conducted
In case of a key compromise, is an investigation conducted that includes a documented analysis of how and why the event occurred, impacted systems and the damages suffered?	Y	

Figure 7: Audit Template Example

solidity i.e. clean criminal records and reasonable financial situation.

Audits are resource demanding activities. Companies typically undergo several audits yearly from different compliance authorities. With an inhomogeneous assembly of different systems the particularities of each will be investigated and the full documentation set examined. An example of an audit report template is shown in Figure 7.

7 Centralised and Automated Key Management

Data security is all too often reduced to the question of compliance. If a system complies with relevant auditory regulations then all is well. There may still be relevant security vulnerabilities that were not covered by the compliance exercises, but are relevant to this particular section.

Compliance can be a major hassle and is therefore an issue which organisations must deal with in the most practical way possible.

As previously alluded to it is easier to pass and / or demonstrate compliance if procedures are followed, documented and adequately updated. Another means of easing and possibly ensuring compliance is to centralise crypto operations. Centralising means that fewer systems and processes will need to be analysed.

If a system also features automated key management, then the time-demanding manual key management procedures should disappear. Automation can be made for key import/export where systems can exchange keys electronically via a push/pull protocol or automation can be in the form of a secure paper-printout of key components to attach to now simplified key ceremony forms.

Centralised and automated key management has multiple advantages from a compliance point of view, such as:

- **One system to audit**
  - As opposed to application specific key management
- **Only one audit log**
  - Complete history of each key, regardless of the end application
- **Uniform documentation set for key management procedures**
- **Automatic key management:**
  - Application level (an xml push/pull protocol)
  - HSM level (push keys directly into the HSM)
  - Key components are not lost
- **Manual key management:**
  - Secure method of built-in paper-printout of key components to attach to key ceremony forms
- **Operators only need to understand one system**

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

CKMS (Cryptomathic Key Management System) has a global client base that include some of the world's largest payment financial institutions, card payment schemes, data processors, governments 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 aids to ensure compliance, improve security, shorten time to market and save security costs (direct and indirect).

8 Conclusion

The use of IT brings obvious advantages in way of efficiency, time and convenience but it yields a number of new threats and vulnerabilities. Protecting sensitive (or even all) data is the major problem, which has been highlighted time and time again by data breaches leaving vulnerable information, e.g. government or hundreds of thousands of individuals exposed by a click of a button.

Securing data is actually not that complicated but given the data loss scenarios that is constant headline news the main focus of data protection becomes compliance. Since the early 2000s there has been a massive rise to the number of schemes that require compliance and/or conformance.

As described in this white paper, compliance is rarely difficult to achieve, it is typically a question of implementing a certain set of standards and procedures.

However, documenting and proving compliance is a completely different matter, and costly at a bare minimum.

Proving compliance in the world of IT security becomes particularly problematic because crypto is:

- The foundation for online trust – encryption and authentication
- A specialist area requiring the right specific technical background AND experience

The main issues in case of non-compliances clearly depends on the severity of the non-compliances, but can often be so severe that it has serious long-term effects, such as losing your job, damage to company reputation and revenue, losing certification/keys/valuable data and customers, or worst case scenario – the company goes bankrupt. In turn compliance needs to be managed in order to minimise risk.

So compliance is a must and it can be expensive if your organisation is not properly prepared (e.g. leading to a costly re-audit). Having the right

systems, processes and knowhow in place is 'key' to obtaining compliance and a well-structured organisation is much more likely to pass than a disorganised one.

A couple of other essential ingredients include to be responsible, vigilant, as well as avoiding weak points and single points of failure. It is also important to choose partners and collaborators who know what they are talking about – partners with experience (like.... Cryptomathic).

Finally using third party systems that have already been proven compliant in a variety of customer environments, like the CKMS, can save a lot of time, cost, sweat and even tears.

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/
http://www.cryptomathic.com
http://www.cryptomathic.com/products/key-management
http://www.cryptomathic.com/products/key-management/crypto-key-management-system
http://www.cryptomathic.com/hubfs/docs/cryptomathic_white_paper-emv_key_management.pdf?t=1439368020813
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

ABOUT CRYPTOMATHIC

Cryptomathic is one of the world's leading providers of security solutions to businesses across a wide range of industry sectors, including finance, smart card, digital rights management and government. With nearly 30 years' experience, Cryptomathic provides customers with systems for e-banking, PKI initiatives, mobile, cloud cryptography, ePassport, card issuing and advanced key management utilizing best-of-breed security software and services. Cryptomathic prides itself on its strong technical expertise and unique market knowledge. Together with an established network of partners, Cryptomathic assists companies around the world with building security from requirement specification to implementation and delivery.