This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise should be edited appropriately. Items highlighted in green are examples and should be removed. After all edits have been made, all highlights should be cleared.

Insert organization logo by clicking on the placeholder to the left.

Key Management Standard Template

Choose Classification

DATE	Click here to add date
VERSION	Click here to add text
REF	Click here to add text

Replace <organization name> with the name of the organization for the entire document. To do so, perform the following:

- Press “Ctrl” + “H” keys simultaneously.
- Enter “<organization name>” in the Find text box.
- Enter your organization’s full name in the “Replace” text box.
- Click “More”, and make sure “Match case” is ticked.
- Click “Replace All”.
- Close the dialog box.

Disclaimer

This template has been developed by the National Cybersecurity Authority (NCA) as an illustrative example that can be used by organizations as a reference and guide. This template must be customized and aligned with the <organization name>'s business and relevant legislative and regulatory requirements. This template must be approved by the head of the organization (Authorizing official) or his/her delegate. The NCA is not responsible for any use of this template as is, and it affirms that this template is solely an illustrative example.

Document Approval

Role	Job Title	Name	Date	Signature
Choose Role	<Insert job title>	<Insert individual's full personnel name>	Click here to add date	<Insert signature>

Version Control

Version	Date	Updated by	Version Details
<Insert version number>	Click here to add date	<Insert individual's full personnel name>	<Insert description of the version>

Review Table

Periodical Review Rate	Last Review Date	Upcoming Review Date
<Once a year>	Click here to add date	Click here to add date

Table of Contents

Purpose

This standard aims to define the detailed cybersecurity requirements related to the Key Management process for <organization name>.

The requirements in this standard are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) including but not limited to (ECC-1:2018) and NCS-1:2020, in addition to other related cybersecurity legal and regulatory requirements.

Scope

This standard covers all information and technology assets in the <organization name> and applies to all personnel (employees and contractors) in the <organization name>.

Standards

1	General requirements
Objective	General requirements for the Key Management process must be defined to ensure appropriate secure management of cryptographic keys used by <organization name> during their lifecycle.
Risk Implication	If cryptographic keys are not used properly and its management process is not conducted in line with general cryptographic standards, this can impact the communication and data exchange process which may result in information theft, unauthorized access, and information disclosure.
Requirements	
1-1	Cryptographic key management must be in line with the 2-8-3 control of the Essential Cybersecurity Controls (ECC-1:2018).
1-2	Keys must be managed through the activities that involve handling keys and related security parameters such as

	initialization vectors during the key cycle, including generation, storage, establishment, insertion, output, use, and destruction.
1-3	Keys must be categorized according to their classification (public, private, shared or symmetric) and use.
1-4	Keys and their association must be protected according to their type and the required protection.
1-5	Using Hardware cryptographic modules must follow the below requirements: ● Private keys should not be valid for more than 5 years (this does not limit CA certificates' lifetime) for MODERATE level of Cryptographic Standards. ● Private keys should not be valid for more than 3 years (this does not limit CA certificates' lifetime) for ADVANCED level of Cryptographic Standards.
1-6	Using Software cryptographic modules must follow the below requirements: ● Private keys must not be valid longer than 2 years for MODERATE level of Cryptographic Standards. ● Not accepted for ADVANCED level of Cryptographic Standards.
2	Key Generation
Objective	Define requirements for the Key Generation process to ensure proper key generation according to security rules.
Risk Implication	If cryptographic keys are not generated properly and in line with the defined process, this may result in the generation of weak keys which can have severe implications that could lead to information theft, unauthorized access, and information disclosure.
Requirements	

2-1	Key generation must be performed based on: ● the generation of a key using the output of a Random Bit Generator (approved RBGs are specified in NIST SP 800-90ar1). ● the derivation of a key from another key. ● the derivation of a key from a password key agreement performed by two parties using an approved key-agreement scheme.
2-2	Certificate Authority key generation must be undertaken in a physically secured environment by personnel (employees and contractors) in trusted roles under, at least, dual control, defined as requiring two or more persons to control the generation process to be parts of the key ceremony.
2-3	The asymmetric key pairs generating methods must be approved, listed and complied with the National Cryptographic Standards document.
2-4	An asymmetric static key pair must be generated by either: ● the party that owns the key pair (i.e., the party that uses the private key in the cryptographic computations). ● a facility that distributes the key pair. ● the owner and facility in a cooperative process.
2-5	Symmetric keys must be either: ● generated by an approved, listed and complied with the National Cryptographic Standards document method, ● derived from a master key/key-derivation key using an approved and complied with the National Cryptographic Standards document key-derivation function.

2-6	A symmetric secret key used to apply cryptographic protection to information and to remove or verify the protection must be generated by: ● One or more of the organizations that will share the key, or ● A trusted party that provides the key to the intended sharing organizations in a secure manner. The trusted party must be trusted by all organizations that will share the key not to disclose the key to unauthorized parties or otherwise misuse the key.
2-7	Key lengths used in symmetric key algorithms must be complied with the National Cryptographic Standards document.
2-8	All symmetric keys and key shares must be generated within a cryptographic module specified in the National Cryptographic Standards document.
2-9	For critical systems, it is mandatory to employ symmetric key lengths that are at least 256 bits, and asymmetric Elliptic Curve Cryptography ECC key lengths that are at least 512 bits.
3	Key Registration/Certification
Objective	Define requirements for the Key Registration/Certification process to ensure proper key registration/certification according to security rules.
Risk Implication	If cryptographic keys are not registered in line with the defined requirements, this may result in e.g., the key registration in untrusted and unauthorized Certification Authority which can have severe implications that could lead to information theft, unauthorized access, and information disclosure.
Requirements	

3-1	Keys must be associated with their owner (user) with a certificate.
3-2	Root certificates must be distributed to relying parties and signatories.
3-3	A trusted Certificate Authority must be used.
3-4	Key registration must result in the binding of keying material to information associated with a particular organization. Keys that would be registered include the public key of an asymmetric key pair and the symmetric key used to bootstrap an organization into a system.
3-5	The binding must be performed by a trusted third party. Examples of a trusted third party include a Kerberos realm server or a PKI Certification Authority.
3-6	If a Kerberos realm server performs the binding, a symmetric key must be stored on that server with the corresponding metadata.
3-7	If a Certificate Authority performs the binding, the public key and associated information must be placed in a public-key certificate that is digitally signed by the Certificate Authority.
3-8	If a Certificate Authority provides a certificate for a public key, the public key must be verified to ensure that it is associated with the private key known by the purported owner of the public key.
4	Key Distribution and Installation
Objective	Define requirements for the Key Distribution and Installation process to ensure proper key distribution and installation according to security rules.
Risk Implication	If cryptographic keys are not distributed and installed in line with the defined requirements, this may result in e.g. a key

	breach and compromise or key distribution to an unauthorized third party which can have severe implications that could lead to information theft, unauthorized access, and information disclosure.
Requirements	
4-1	The integrity and authenticity of the CA signature verification (public key) and any associated parameters must be maintained during its distribution to relying parties.
4-2	Keys must be distributed to their users securely and must be under the users control.
4-3	Keys must be transported securely by protecting their confidentiality and authenticity in a way complied with and defined in the National Cryptographic Standards document.
4-4	Private and secret keys must not be distributed in plain text.
4-5	All copies of keys must be securely installed and stored.
4-6	Public keys must be kept secure to prevent interception and manipulation until they are distributed.
4-7	Public keys must be transported, and authenticity (but not privacy) must be protected by using certificates.
4-8	Private keys must be protected and authorized by the owner/third party or CA.
4-9	The generated keys must be transported (when transportation is necessary) using only secured channels.
4-10	Keys must not be shared or distributed beyond those specific organizations or devices requiring the use of the key for approved purposes.
4-11	Keys that are manually distributed must either:

	• be cryptographically protected in the same manner as those intended for electronic distribution. • receive physical protection and be subject to controlled distribution using approved and secure method between the key processing facility and the end organization.
4-12	Keys used only for the storage of information must not be distributed except for backup or to other authorized organizations that may require access to the stored information protected by the keys.
4-13	The private key of an asymmetric key pair must be kept secret. If the key is transferred, it must be taken out and transferred in a form and manner that provides appropriate assurance of its confidentiality, integrity and authenticity.
4-14	The method used for symmetric key transport or key wrapping must support the desired security strength needed to protect the target data.
4-15	The encrypted data and the key used for it must not be transmitted together unless the encryption key is protected via a secondary encryption, e.g., public key encryption.
5	**Key Use**
Objective	Define requirements for the Key Use process to ensure proper key use according to security rules.
Risk Implication	If cryptographic keys are not used in line with the define requirement, this may result in e.g. the key misuse or its unauthorized usage which can have severe implications that could lead to information theft, unauthorized access, and information disclosure.
Requirements	

5-1	Keys must be protected against unauthorized use during their lifetimes.
5-2	Keys must implement authorization check mechanisms to protect against misuse from the owners.
5-3	A single key must be used for only one purpose (e.g., encryption, integrity authentication, key wrapping, random bit generation, or digital signatures).
5-4	The keys and their intended usage must be connected in a reliable way (key wrapping). Key usage information tells the system what the key can (and cannot) be used for.
5-5	For asymmetric key pairs, each key of the pair must have its own crypto period defined.
5-6	The key change may be done when: ● The key may have been compromised. ● The key's cryptoperiod may be nearing expiration. ● It may be desirable to limit the amount of data protected with any given key (re-keying – defined as a process of changing the session key of an ongoing communication in order to limit the amount of data encrypted with the same key).
6	Key Storage
Objective	Define requirements for the Key Storage process to ensure proper key storage according to security rules.
Risk Implication	If cryptographic keys are not stored in line with the defined requirements, this may result in e.g. the key leak and its compromise and as result data leak which can have severe implications that could lead to information theft, unauthorized access, and information disclosure.

Requirements	
6-1	Organizations must require secure backups of keys (for internal or law enforcement use) when encryption is supported.
6-2	Storage rules and retention time for key information must be defined by <organization name>.
6-3	Keys used for non-repudiation must be under the sole control of the user.
6-4	Key identifiers or distinguished naming must be used for proper key identification.
6-5	<organization name> must address how the cryptographic device or application stores and protects key information including how long it is to be stored.
6-6	<organization name> must indicate how the key information (key identifier, distinguished name, ownership, key users, generation date, expiration date, associated CA) is identified during its storage life (e.g., using a Distinguished Name or key identifier). The storage capacity requirements for storing the key information must be included.
6-7	Asymmetric private keys must be stored in one of the following ways: ● Inside one piece of Hardware Security Modules in plaintext (or even encrypted under a Master key). ● Outside HSMs but encrypted with a key wrap function in accordance with the NCS-1:2020. ● Inside many HSMs pieces of hardware but in plaintext fragments (or even encrypted under a Master key).
6-8	Symmetric keys must be stored inside the Hardware Security Modules. In case of exception, where a key is stored outside a

	cryptographic module, the method of protection must depend on the impact level associated with the data protected by a key.
6-9	The database that is used to store the keys must be encrypted using validated and complied with the National Security Standards document module.
7	Key Revocation/Validation
Objective	Define requirements for the Key Revocation/Validation process to ensure proper key destruction according to security rules.
Risk Implication	If cryptographic keys are not revoked and validated in line with the defined requirements, this may result in e.g. data encrypted by the compromised key decryption and leak or expired key usage which can have severe implications that could lead to information theft, unauthorized access, and information disclosure.
Requirements	
7-1	A key must be revoked in case where: ● the authorized use of a key needs to be terminated prior to the end of the established cryptoperiod of that key. ● a key whose usage period has expired. ● a key has been compromised.
7-2	A key may be revoked for administrative reasons (e.g., the key's owner has left <organization name>, or a device containing the key has been removed from service).
7-3	A key must be revoked on an emergency basis if there is reason to believe that it may have been disclosed to or otherwise accessed by an unauthorized organization.

7-4	A key must be revoked as soon as feasible after the need for revocation has been determined.
7-5	The Certificate Revocation List (CRL) and the Online Certificate Status Protocol (OCSP) must be implemented to avoid relying on keys that have expired.
7-6	Relying parties must be notified about key revocation using, for example, Certificate Revocation Lists (CRLs) or the Online Certificate Status Protocol (OCSP).
7-7	When a key is compromised, all organizations sharing the key need to be notified (e.g., using a Compromised Key List (CKL)).
7-8	<organization name> must validate used keys by checking the CRL or OCSP lists/servers.
7-9	An assurance of public-key validity must be obtained to ensure that the key is arithmetically correct, through one of the following methods: ● Assurance from the key owner, key verifier, or trusted third party. ● Explicit public key validation by encrypting a message using one key and decrypting using the other one.
8	Key Archive
Objective	Define requirements for the Key Archive process to ensure proper key archive according to security rules.
Risk Implication	If cryptographic keys are not archived in line with the defined requirements, this may result in e.g., the key leak and its compromise and as a result data leak which can have severe implications that could lead to information theft, unauthorized access, and information disclosure.
Requirements	

8-1	The archival process must be secured and confidentiality must be ensured to preserve the secrecy of information encrypted with archived keys.
8-2	Expired keys must be archived to keep old data accessible as long as the original encryption is supported.
8-3	Archival systems must follow the retention periods as per relevant regulations and internal <organization name>'s policies and standards.
8-4	A key archive must contain keys and their associated information (i.e., key information like key identifier, distinguished name, ownership, key users, generation date, expiration date, associated CA) for recovery beyond the cryptoperiod of the keys.
8-5	The key archive must continue to provide the appropriate protections in line with requirements included in the National Cryptographic Standards document for each key and any other related information in the archive. The archive must require a strong access-control mechanism to limit access to only authorized organizations.
8-6	The archive must be maintained by <organization name> or trusted third party.
9	**Key Destruction**
Objective	Define requirements for the Key Destruction process to ensure proper key destruction according to security rules.
Risk Implication	If cryptographic keys are not destructed in line with the defined requirements, this may result in e.g., the possibility to decrypt data by compromised key and data leak which can have severe implications that could lead to information theft, unauthorized access, and information disclosure.

Requirements	
9-1	Keys must be removed when key lifetime expires and there is no need for it to be archived or stored via a secure deletion process complied with the National Security Standards document in order to minimize the risk of a compromise. The key must be completely removed with all its instances and make the recovery of that key impossible.
9-2	All copies of secret (symmetric), public and private (asymmetric) keys must be destroyed as soon as they are no longer required (e.g., for archival or reconstruction activity) in order to minimize the risk of a compromise.
9-3	Secret (symmetric), public and private (asymmetric) keys must be destroyed in a manner that removes all traces and records of the keys so that they cannot be recovered by either physical or electronic means.
9-4	A compromised key must be revoked as soon as possible.
9-5	Public keys must be retained or destroyed depending on their future needs associated with archiving, restoring or accountability.
9-6	Media storage systems storing keys must be sanitized before disposal using a process compliant with NIST SP 800-88r1 or NSA/CSS Storage Device Sanitization Manual.
10	Key Accounting
Objective	Define requirements for the Key Accounting process to ensure proper key accounting according to security rules.
Risk Implication	If cryptographic keys are not accounted in line with the defined requirements, this may result in e.g. the impossibility of calling to account the person responsible for key misuse or key compromise which can have severe implications that could

	lead to information theft, unauthorized access, and information disclosure.
Requirements	
10-1	Use of asymmetric keys must be monitored by <organization name>'s <cybersecurity function> or nominated by <cybersecurity function> key owners/administrator through dedicated tools.
10-2	Key usage must be accounted for. Accountability process must involve the identification of those that have access to, or control of, cryptographic keys throughout their lifecycles.
10-3	Each <organization name>'s personal involved with key management must be clearly informed about their responsibilities and held accountable for fulfilling them.
11	Other Standards
Objective	The key management process must be securely configured and performed and meet other associated standards.
Risk Implication	If <organization name> is not compliant with all applicable and mandatory standards and requirements, it could be exposed to severe threat rise specific for areas covers by below mentioned standards.
Requirements	
11-1	The following standards must be implemented in relevance to key management process: ● The National Cryptographic Standards. ● Cryptography standard.

Roles and Responsibilities

1- **Standard Owner:** <head of the cybersecurity function>

2- **Standard Review and Update:** <cybersecurity function>

3- **Standard Implementation and Execution:** <information technology function>

4- **Standard Compliance Measurement**: <cybersecurity function>

Update and Review

<cybersecurity function> must review the standard at least once a year or in case any changes happen to the policy or the regulatory procedures in <organization name> or the relevant regulatory requirements.

Compliance

1- The <head of the cybersecurity function> will ensure compliance of <organization name> with this standard on a regular basis.

2- All personnel at <organization name> must comply with this standard.

3- Any violation of this standard may be subject to disciplinary action according to <organization name>'s procedures.