DEUTSCHE BÖRSE GROUP

Encryption and Key Management Guideline

Version: 1.1

Valid From Date: 15.08.2025

Last Review Date: 27.06.2025

Notes: This written rule uses gender-neutral and inclusive language. Whenever possible, the generic masculine is avoided and all employees of any gender identity (m/f/d) are addressed.

Content changes compared to the previous document version are highlighted in color.

Content

1. Purpose, Objectives and Basis

1.1. Purpose and Objectives

The Encryption and Key Management Guideline (hereinafter “Guideline”) establishes control requirements for DBAG and/or adopting Legal Entities within DBG (refers only to Legal Entities that have ratified the Guideline at hand) and provides criteria for fulfilling the control requirements.

The purpose of the Guideline is to effectuate the below listed Minimum Requirements, stipulated in the ICT Risk Management Policy (structured into Core Functions), acting as objectives to the Guideline and the control requirements at hand:

Core Function	Minimum Requirement	ICT Risk Management Policy chapter
Govern	2. Allocate roles and responsibilities as detailed in chapter 5 in the ICT Risk Management Policy.	4.1
Govern	6. Have in place a mechanism to define and document responsibilities for implementing control requirements both within and outside IT and IS (e.g. HR). This can be documented e.g. as part of the Mandatory Control Framework (MCF).	4.1
Protect	1. Design and implement ICT risk management control requirements to achieve the protection goals and integrating them to the ICT risk framework. These control requirements are including but not limited to ICT operations and physical and environmental security, network and infrastructure management, encryption and cryptographic controls, identity management and logical/physical access control, software development, change and project management, threat management, patch and vulnerability management, human resources, and third-party management.	4.3

Table 1: Minimum Requirements

Note: The full list of Core Functions and Minimum Requirements is stipulated in the ICT Risk Management Policy.

1.2. Basis of this Guideline

The basis for this Guideline is the ICT Risk Management Policy.

2. Functional Scope and Target Groups

2.1. Functional Scope of applicability

Entity	DBAG and/or adopting LE within DBG
Area	CIO / COO Division; Chief Risk Officer Area; Chief Compliance Officer Area; or any other area that owns Encryption and Key Management topic

Table 2: Scope

2.2. Target groups

Within the scope of the current Encryption and Key Management Guideline below is addressed the list of applicable target groups and operation areas[1]:

Target group	Key message
ICT Risk Oversight	To oversee the strategic direction and policy enforcement related to encryption and key management.
ICT Operational Management	To implement and maintain technical measures on encryption and key management.
Business Management	To manage the encryption and key management related risks and consequent tracking and reporting.

Table 3: Target groups

[1] For LE Guidelines adoption process the target groups should be adjusted according to organizational structure of the LE.

2.3. Transition period

The grace period for new requirements commences from the “valid from” date stated on the cover page. The compliance dates for control requirements defined in this version of the Guideline are defined as follows:

- For unchanged control requirements and new DORA requirements the compliance date equals the “Valid from” date.
- For new and changed control requirements that are more stringent than before and are not subject to DORA, the compliance date is generally 90 calendar days after the “Valid from” date unless otherwise stated in brackets after the control requirements. These control requirements are marked with ●.
- For Legal Entities that have not previously approved the IT-related requirements and are therefore addressing these requirements for the first time, a grace period of 90 days may be granted at the discretion of the Legal Entity. DORA requirements are exempt from this grace period.

For a **compliance date** exceeding a 180 calendar days implementation timeline, a Board approval is required.

3. Definitions

3.1. Requirements

Control requirement

The control requirements define the organizational, process or technical controls to be implemented by the control owner to achieve compliance with this Guideline.

Criteria

Criteria define the measures that ‘must’ or ‘should’ be taken to fulfill the control requirement.

Level of obligation

With respect to requirements and criteria, the following terms are used to define the level of obligation, provided for the implementation of a particular requirement or criteria:

- **“must”:** Mandatory control requirements / criteria derived directly from law, regulations, or internal specifications that the legal entity must comply with. Incompliance could result in consequences with external regulators and Internal Audit.
- **“should”:** Non-mandatory control requirements / criteria derived from best-practice frameworks or equivalent sources that the legal entity does not have to necessarily comply with. Under specific circumstances there may exist valid reasons to ignore a particular control requirement, but the full implications must be understood and carefully weighed.

Independent of the level of obligation of a given requirement or criteria, it is allowed to deviate from single requirements or criteria in individual cases. However, a control requirement deviation always requires the conduction of a risk assessment and risk management including adequate risk acceptance and/or mitigation.

Any deviation from the Guideline denotes an exemption. The respective Information Owner makes decisions on such exemptions. Information Owners can only decide on risks with impact exclusively in their area of responsibility.

Responsibilities

The responsibility for fulfilling control requirements may be distributed across the organization, e.g., multiple Sections, Units, or Departments. In some cases, one Unit may be responsible for both the design and implementation of measures. In other cases, one Unit may be responsible for the design of measures, and another Unit may be responsible for the implementation of the measures. In addition, multiple Units may be responsible to collectively fulfill one requirement.

The precise responsibilities are to be defined in the underlying Procedure documents (e.g. via RACI matrices).

The ICS, among its various functionalities, registers Process Operators (PO) and Risk Representatives (RRs) mapped to the corresponding processes, controls, and risks which the RRs and/or POs are responsible for managing on behalf of the part of the organization that utilize their services (e.g. Asset Owners). For more information on ICS, please refer to the DBG ICS Guideline.

3.2. Explanation of requirements and key definitions

Control requirements are defined in a standardized format and are structured into the following components:

<Specify ID: xx (version x)>	**<Name of control requirement (e.g. Access to production data)>**
1	**<Description of the control requirement>**
1.1 1.1.1	<Lists the criteria applying to the control requirement> <Lists the sub-criteria applying to the control requirement>
Protection goals <Specifies the protection goal of the control requirement e.g., CIAA (Confidentiality, Integrity, Availability, Authenticity)>	**Key references** <Lists key regulatory references and industry best practice requirements affecting this control requirement (e.g., ISO/IEC 27001:2022 A.5.10, A.8.1)>

The terms in this document are defined in the overall ICT Risk Glossary, which is provided on the Intranet website.

4. Requirements

4.1. Requirements

ID: 1 (version 1.1)	Procedure, Development and Governance
1	**An Encryption and Key Management procedure must be defined, documented, and implemented to ensure company data is protected. The procedure must include controls, rules, and guidance for the implementation.**
1.1	Encryption and Key management controls, rules and guidance must entail rules around preservation of confidentiality, integrity, availability, and authenticity of data.
1.2	In instances where adherence to leading practices, standards, or the utilization of the most reliable techniques, including the updating or changing of cryptographic technology, is not feasible, Encryption and Key management controls, rules and guidance must entail mitigation and monitoring measures, accompanied by a reasoned explanation for the deviation.
1.3	Encryption and Key management procedure must entail activities on review, approval, implementation, and communication of cryptographic, encryption and key management technology changes.
Protection goals Confidentiality, Integrity, Availability, Authenticity	**Key references** – CCM requirement CEK-05 – DORA RTS RMF A.6.1, A.6.4, A.6.5

ID: 2 (version 1.1)	Selection and implementation of cryptographic measures
2	**Cryptographic measures selection, implementation must be aligned with recognized standards, applicable legislation, and legal entities' approval. They must provide sufficient strength and commensurate to applicable data classification.**
2.1	Requirements of cryptographic measures regarding strength and quality to be legal entity approved:
2.1.1	Key lengths, encryption schemes and allowed hash functions must comply with the requirements specified in BSI TR 02102-1, 31.01.2025[2], with the following exemption: the key length for the cryptographic algorithms DLIES, DSA and RSA must be at least 2000 bits and should be ≥ 3000 bits if possible.

[2] Future enhancements for quantum-safe cryptography can be aligned with project-specific timelines and implementation guidance defined in upcoming phases.

2.1.2	The cryptographic measures must be selected in compliance with all relevant agreements, legislations, and regulations, based on recognized international, European, harmonized, or national standards, and the classification of IT Assets.
2.1.3	**Protection level**: The required protection level must be commensurate with the criticality of the data to be protected with respect to its impact and visible label. For each protection goal - confidentiality, integrity, authenticity, and availability - it is marked whether the impact is “critical”, “major”, “minor” or “negligible” and whether the visible label of the data is “strictly confidential”, “confidential”, “internal”, “external” or “public”.
2.1.4	**Requirements regarding certificates for payment services**: If certificates are used for the purpose of identification within a payment service, they must rely on qualified certificates for electronic seals or on qualified certificates for website authentication.
2.1.5	**Requirements regarding key storage**: The key storage must be commensurate to the strength and quality of the cryptographic measure used and the use case for which the key is applied.
2.1.6	**Risk Analysis**: Based on the risk analysis, requirements for the strength and quality of the cryptographic measures must be defined, implemented, ensuring that appropriate BSI approved cryptographic measures are applied.
2.2	It must be ensured that only cryptographic measures approved by Legal entity are used (see Control ID 2.1, Selection of cryptographic measures). If these standards cannot be met, mitigation and monitoring measures must be adopted to ensure cyber resiliency.
2.3	Requirements regarding key management: All cryptographic certificates which are used to secure the communication should be issued by a Public Key Infrastructure (PKI) with the exception of SSH keys.
2.4	**Additional for IT Assets subject to MAS TRMG:** Transaction signing must be implemented for authorizing high-risk activities.

Protection goals	**Key references**
Confidentiality, Integrity, Availability, Authenticity	– BSI TR 02102-1, 31.01.2025 – DORA RTS RMF A.6.3 – ISO/IEC 27002:2022 A.8.24 – MAS TRMG 14.2.3

ID: 3 (version 1.1)	Review, assessment and monitoring of cryptographic measures and products
3	**Cryptographic measures and products must undergo regular assessment, monitoring regarding compliance with applicable standards, legislation, and adherence with developments in cryptanalysis to ensure they remain resilient against cyber threats.**
3.1	The cryptographic measures implemented must be reviewed/ reassessed at least every 12 months.
3.2	For cryptographic measures and products which do not meet applicable technical or legal requirements or cannot mitigate applicable threats from cryptanalysis development, the potential risks must be assessed and treated.
Protection goals Confidentiality, Integrity, Availability, Authenticity	**Key references** – DORA RTS RMF A.6.4 – ISO/IEC 27002:2022 A.8.24

ID: 4 (version 1.1)	Documentation of key and cryptographic measures
4	**Documentation of cryptographic measures, PKI architecture, connection paths with corresponding key and certificate register must be established and regularly maintained to ensure proper operation and compliance.**
4.1	The cryptographic measures must be documented to ensure that they are safely operated, and an overview of the implemented measures is provided: Details of all algorithms and protocols used for the protection of classified data and the keys used should be documented. More precisely, for algorithms and protocols at least the aspects bit security, protection level, standard as well as usage and for keys the strength, expiry date and usage must be recorded.
4.2	The PKIs must be documented to ensure their safe operation.
4.2.1	For each PKI a governance model for generation, distribution and management of cryptographic keys must be in place and documented, providing requirements for the complete life cycle of certificates and keys.
4.2.2	For each certificate authority, methods and processes to be implemented must be described to meet the requirements demanded by the governance model.
4.2.3	The documentation of PKIs should ensure that the keys are securely managed, conflicts of interest are strictly avoided and a clear role concept with separation of duties is in place to avoid misuse during the creation and administration of cryptographic keys in accordance with Identity and Access Management Guideline.

4.3	Connection paths and corresponding keys without central validation must be documented in an auditable format to ensure proper compliance of authorizations in addition to providing the ability to remediate any access violations.
4.4	A register for all certificates and certificate-storing devices for at least IT Assets supporting critical or important functions must be in place and up to date.
Protection goals Confidentiality, Integrity, Availability, Authenticity	**Key references** – DORA RTS RMF A.7.4 – ISO/IEC 27002:2022 A.8.24

ID: 5 (version 1.1)	**Protection of data in transit**
5	**Data in transit must be protected in accordance with its classification and risk analysis and exchanged through secure network only.**
5.1	Data in transit must be protected depending on its classification based on the results of the approved data classification and risk analysis.
5.1.1	If data communicated within internal network is classified as “critical” or “major” with respect to confidentiality and/or integrity and/or authenticity or when the visible label of the data is “strictly confidential” or “confidential”, it should be protected by cryptographic measures.
5.1.2	The approach to the data in transit cryptographic protection should consider the Control requirement and criteria in ID 2 and a technical risk analysis for at least the following scenarios: connection from a compromised or malicious software client, connection to a compromised or malicious server, “man-in-the middle” attack, data theft by traffic sniffing.
5.1.3	WLAN: Only access solutions for WLAN must be applied using legal entity approved cryptographic measures to ensure authenticity. Furthermore, the communication must be encrypted (see below, communication within internal network) to provide confidentiality.
5.1.4	Communication within internal network: Communication within internal network should be protected regarding confidentiality, integrity, and authenticity by using a standardized transport layer protocol. The protocol prevents man-in-the-middle attacks when using legal entity approved cryptographic measures and a secure configuration.
5.1.5	Port Security: Secure cryptographic measures should be used to ensured that only legal entity owned assets are connected to internal network (excl. legal entity guests) ensuring that confidentiality, integrity, and authenticity are preserved.
5.1.6	Internet of Things and Operational Technology: Data communication should be protected regarding their confidentiality, integrity, and authenticity either by using the cryptographic measures applied for the communication within internal network, by establishing a Virtual Private Network (VPN) based connection or other equivalent technologies.

5.1.7	Emails (to internal communication partners): Emails should be protected regarding confidentiality, integrity and authenticity using legal entity approved cryptographic measures and keys generated and managed by a PKI.
Protection goals Confidentiality, Integrity, Availability, Authenticity	**Key references** – DORA RTS RMF A.6.2a), A.6.2c) – ISO/IEC 27002:2022 A.8.24

ID: 6 (version 1.1)	**Protection of data at rest**
6	**Protection of data at rest and rules for encryption of data must be in place and aligned with data classification and risk analysis.**
6.1	Data stored inside of internal infrastructure or legal entity approved data centers must be protected with respect to confidentiality, integrity and authenticity depending on its classification and risk analysis.
6.1.1	Independent of the classification the following data must be protected by cryptographic measures to preserve confidentiality: personalized security credentials.
6.1.2	Data stored within internal infrastructure classified as “critical” or “major” with respect to confidentiality and/or integrity and/or authenticity or where the visible label of the data is “strictly confidential” or “confidential”, should be protected by cryptographic measures.
6.1.3	The approach to the data at rest cryptographic protection should consider the requirement and criteria in Control requirement ID 2 and a technical risk assessment for at least the following scenarios: equipment theft, malicious actions of underlying platform administrator.
6.1.4	The storage of mobile devices and storage media must be fully encrypted using legal entity approved cryptographic measures to preserve their confidentiality.
6.1.5	**Backups:** Backups must be protected from loss of confidentiality, integrity, and authenticity. Depending on the information classification, cryptographic measures must be used.
6.1.6	**Archives:** Archives must be protected from loss of confidentiality, integrity, and authenticity. Depending on the information classification, cryptographic measures must be used. Furthermore, long-term security must be ensured, data is protected and can be accessed during its entire legally obligated archival period.
6.1.7	**Stationary Devices:** The storage of all Stationary Devices containing critical data should be protected regarding confidentiality using legal entity approved cryptographic measures.
6.1.8	**Internal Servers:** File-, database-, mail-, application- and web servers, internal data centers, on-premises clouds as well as collaboration platforms should be protected regarding confidentiality using legal entity approved cryptographic measures providing full disk or partitions encryption.

6.2	Data at rest stored outside of internal infrastructure or legal entity approved data centers must be protected depending on its classification and risk analysis.
6.2.1	If data is classified as “minor”, “major” or “critical” with respect to confidentiality or when the visible label of the data is “internal”, “external”, “confidential” or “strictly confidential”, it must be encrypted by the legal entity using its approved cryptographic measures, such that only the legal entity can decrypt the data to preserve its confidentiality (the data is stored in encrypted form in external servers).
6.2.2	The approach to the data at rest cryptographic protection should consider the requirement and criteria in Control requirement ID 2 and a technical risk analysis for at least the following scenarios: equipment theft, malicious actions of underlying platform administrator, cyberattack on the external infrastructure provider.
6.2.3	Legal entity approved cryptographic measures must be used to ensure that only authorized persons access the ICT Systems to preserve integrity and authenticity.
Protection goals Confidentiality, Integrity, Availability, Authenticity	**Key references** – DORA RTS RMF A.6.2a), A.6.2b) – ISO/IEC 27002:2022 A.8.24

ID: 7 (version 1.1)	**Protection of data in use**
7	**Protection of data in use must be in place and aligned with data classification and risk analysis.**
7.1	Rules for the encryption of data in use must be defined, documented based on the results of the approved data classification and risk analysis, for example, rules for confidential computing.
7.2	In case encryption of data in use is not possible, the data should be processed in a separated and protected environment or take other equivalent measures that ensure confidentiality, integrity, authenticity, and availability of data.
Protection goals Confidentiality, Integrity, Availability, Authenticity	**Key references** – DORA RTS RMF A.6.2b)

ID: 8 (version 1.1)	Key Management and Governance
8	**It must be ensured that requirements and guidance for cryptographic key management are in place.**
8.1	Requirements for cryptographic key management must cover the entire lifecycle of cryptographic keys.
8.2	Requirements must specify how cryptographic keys are correctly used and protected.
8.3	The cryptographic keys should be dedicated to a single purpose.
8.3.1	The key should be either used for encryption or for digital signatures.
8.3.2	**Additional PKI-specific and certificate-related requirements:** Certificates used for authentication of users or entities should not be used for digital signatures or non-repudiation.
8.3.3	Where an IT Application uses certificates for user authentication and digital signatures, two separate keys and certificates should be issued to each user.
8.3.4	If a digital certificate to a key pair is generated it should clearly indicate the intended usage using X509 key usage and extended key usage attributes.
8.4	Customer keys or other master keys must be generated and stored under legal entity control whether on-premises or in the cloud.
Protection goals Confidentiality, Integrity, Availability, Authenticity	**Key references** – DORA RTS RMF A.6.2d), A.7.1) – ISO/IEC 27002:2022 A.8.24

ID: 9 (version 1.1)	Key generation
9	**It must be ensured that key generation is performed appropriately with sufficient security measures and that generated keys meet applicable strength and quality requirements.**
9.1	The key generation and utilized random number generators must comply with the requirements specified in BSI standards or by using hardware coming with a NIST FIPS 140-2 validation. For detailed requirements on key generation and random number generator, please refer to BSI TR 02102-1, 31.01.2025 and NIST SP 800-90A, 06.2015.
9.2	The security parameters of the keys must be chosen such that they provide the strength and quality demanded by the legal entity.
9.3	When keys used in the Red Segregation Area are generated, at least two persons should be present and provide a formal documentation of the steps performed.

9.4	If users generate their own keys, they should be guided in generating key material, especially when they decide for parameters or add randomness.
9.5	Keys should only be created with the intent of establishing an approved trust relationship and must be deleted if approval of the request has been denied or revoked.
9.6	**Additional PKI-specific and certificate-related requirements:**
9.6.1	The key generation must be carried out using a secure cryptographic key generator.
9.6.2	The hardware used to generate the keys must be protected against unauthorized access, theft, or damage by appropriate physical and organizational measures.
9.6.3	Key-encrypting keys (keys used to protect multiple keys) must be at least as strong as the data-encrypting keys they protect.
9.6.4	After key generation, all data used during this process should be destroyed.
9.6.5	For long-living keys or sensitive keys, it should be ensured that no single individual knows the key in its entirety or has access to all the components generating the keys.
9.7	**Additional SSH-key-related requirements:**
9.7.1	SSH-keys generation must be carried out using a secure cryptographic key generator, which ensures enough randomness and prevents manipulation.
9.7.2	SSH-key pairs should be created on the source system where the private key remains.
9.7.3	Least privilege principle and measures to reduce risks related to misuse should be technically enforced for generated SSH-keys.

Protection goals	**Key references**
Confidentiality, Integrity, Availability, Authenticity	– BSI TR 02102-1, 31.01.2025 – ISO/IEC 27002:2022 A.8.24 – NIST SP 800-90A, 06.2015 – NIST FIPS 140-2

ID: 10 (version 1.1)	Key distribution
10	**Keys must be protected when distributed.**
10.1	It must be ensured that only authorized key holders receive secret keys.
10.2	The key holder should formally acknowledge that they understand and accept their key-custodian responsibilities.
10.3	**Additional PKI-specific and certificate-related requirements:**
10.3.1	During key distribution, the same protection level as required for key storage must be met.
10.4	**Additional SSH-key-related requirements:**
10.4.1	Private key distribution process must be done in encrypted form, and it must be ensured that the private key is kept confidential during the process.
10.4.2	Private key distribution must be prevented to avoid exposure, if applicable.
10.4.3	Public keys must only be distributed by authorized users for the establishment of approved trust-relationships.
10.4.4	Established trust-relationships must be documented to ensure audit and remediation activities.
Protection goals Confidentiality, Integrity, Availability, Authenticity	**Key references** – ISO/IEC 27002:2022 A.8.24

ID: 11 (version 1.1)	Key installation
11	**Keys must be checked prior to installation and deployment.**
11.1	Before key installation, the key holder receiving the key must verify its integrity and authenticity, following a risk-based approach.
11.2	**Additional SSH-key-related requirements:** When the SSH target Account Owner receives a key deployment request the following attributes must be checked: It must be verified whether the SSH-key pair expiration date has not been met yet and no deletion date is documented for the SSH-key pair.
Protection goals Confidentiality, Integrity, Availability, Authenticity	**Key references** – ISO/IEC 27002:2022 A.8.24

ID: 12 (version 1.1)	Key storage
12	**Cryptographic keys must be physically and/or logically protected against modification, theft, loss, and deletion, in accordance with the classification level of the data they protect and aligned with risk-based approach.**
12.1	The keys must be stored such that the strength and quality demanded by the legal entity is provided.
12.2	Key-encrypting keys must be stored separately from data-encrypting keys.
12.3	Private keys should remain non-exportable or vaulted.
12.4	In case cryptographic keys are managed by the Asset Owners themselves, all operations must be recorded in a log and forwarded to central storage.
12.5	**Additional PKI-specific and certificate-related requirements:**
12.5.1	Hardware storing key material must be protected from loss, theft, or damage by appropriate organizational and physical measures.
12.5.2	Hardware storing keys must be certified to be sufficiently tamper-proof.
12.5.3	Access to key-encrypting keys must be protected using the multiple-eyes principle.
12.5.4	Access to systems storing key material must be limited to the need-to-know principle for authorized people.
12.5.5	Private keys must only be stored in encrypted form.
12.5.6	Cryptographic keys that are used for long periods of time or pose a high risk in case of key leakage, must be stored outside of the used ICT Systems.
12.5.7	If long-living keys are stored, they should be protected by the multiple-eyes principle.
12.5.8	If the key is used to protect data classified as “critical” with respect to confidentiality or the visible label of the data is “strictly confidential”, it should be stored on a hardware security module.
12.6	**Additional SSH-key-related requirements:** Access to private SSH-keys must be restricted to authorized users and should be limited to read access, if applicable.
Protection goals Confidentiality, Integrity, Availability, Authenticity	**Key references** – ISO/IEC 27002:2022 A.8.24 – DORA RTS RMF A.7.2

ID: 13 (version 1.1)	Key renewal/rotation
13	**Key renewal and session key change should be performed regularly to avoid compromise over time.**
13.1	To address potential compromise of key material over time, a periodic key renewal should be performed.
13.1.1	For each use of cryptographic measures, the validity period of keys should be determined by consideration of the cryptographic algorithms and parameters, the threat vectors and landscape, the sensitivity and protection requirements of the data, the frequency, volume and use case of key usage, the level of security of the key storage and the operational criticality.
13.1.2	The process to renew keys should be initiated early enough to ensure that a new key is in place before the old key expires.
13.1.3	The new keys should be generated independently from the previous key.
13.1.4	**Additional SSH-key-related requirements:** SSH-key pairs held by a group of individuals should be changed whenever an individual is removed from the group.
13.2	Session keys should be changed after a specific time or number of encrypted packets, considering risk analysis.
13.3	**PKI-specific and certificate-related requirements:** Certificates must be renewed in an appropriate time before they expire.
Protection goals Confidentiality, Integrity, Availability, Authenticity	**Key references** – DORA RTS RMF A.7.5 – ISO/IEC 27002:2022 A.8.24

ID: 14 (version 1.1)	Key backup and archiving
14	**Cryptographic keys must be securely protected in backup, archive and their availability must be ensured when needed.**
14.1	Cryptographic keys must be protected when backed up and/or archived.
14.1.1	The same level of protection as for key storage must be provided for the backed up and archived data as well.
14.1.2	Keys must be deposited (respectively backed up and/or archived) when they are used for encryption or, in case of a key loss, access to the encrypted data is still required.
14.2	It must be ensured that keys can be restored and clarified from whom the data can be accessed.
14.2.1	Based on the backup, in case of a disaster or media failure the keys must be recoverable to quickly re-establish products and to access encrypted information.
14.2.2	Processes should be provided on how to react in case of a key loss or failure, malfunction, or breakdown of cryptographic products.
Protection goals Confidentiality, Integrity, Availability, Authenticity	**Key references** – ISO/IEC 27002:2022 A.8.24

ID: 15 (version 1.1)	ICT-related Incidents involving cryptographic keys
15	**It must be ensured that ICT-related Incidents involving cryptographic keys are understood, identified and that countermeasures are available for overall ICT-related Incident response.**
15.1	Possible ICT-related Incidents involving cases such as loss or failure of cryptographic keys must be identified in advance.
15.2	Processes and countermeasures must be defined on how to react in case of a key loss or failure, malfunction, or breakdown of cryptographic products.
15.2.1	**Additional PKI-specific and certificate-related requirements:** Possible countermeasures for these ICT-related Incidents include the following: revocation of the key and adding it to the Certificate Revocation List (CRL), deletion of data encrypted with forged keys, prolonging the security by re-encryption and building of signature chains.
15.3	Parties that are affected by key compromise, such as Information Owners, must be informed.

Protection goals Confidentiality, Integrity, Availability, Authenticity	**Key references** – DORA RTS RMF A.7.3 – ISO/IEC 27002:2022 A.8.24

ID: 16 (version 1.1)	**Key deletion**
16	**Key deletion must be performed securely to ensure non-recoverability.**
16.1 16.2	If keys are no longer required, they must be deleted in a secure way. **PKI-specific and certificate-related requirements:** It should be prevented that deleted keys can be recovered by any party in case keys are stored in a Hardware Secure Module (HSM).
Protection goals Confidentiality, Integrity, Availability, Authenticity	**Key references** – ISO/IEC 27002:2022 A.8.24

ID: 17 (version 1.1)	**Cloud-specific encryption requirements**
17	**It must be ensured that appropriate cryptographic measures and cryptographic key management are in place for cloud.**
17.1	Rules for secure cloud cryptographic key management including key generation, storage and sharing of keys, must be defined and implemented.
17.1.1	For IT Assets classified as major and critical, the key generation should be done inside hardware security modules (HSM) that complies with FIPS 140-2 Level 3.
17.1.2	The default key storage of the CSP may be used for negligible and minor classified IT Assets for the key generation.
17.1.3	Keys must be shared as cryptograms, e.g., encrypted with the addressee's public key via secure e-mail or secure file transfer or via HSM native envelope encryption. Other mechanisms for key distribution are not acceptable.
17.1.4	It must be contractually ensured that cloud service providers provide the ability for the covered legal entity to manage own data encryption keys.
17.1.5	The legal entity must ensure that API keys are secure.

17.2	It must be ensured that connections are established using industry standard protocols including but not limited to HTTPS, IPSec, SSH. Connection in public networks must always be encrypted.
17.3	It must be ensured that backups performed using cloud native services are encrypted.
Protection goals Confidentiality, Integrity, Availability, Authenticity	**Key references** – CCM requirement CEK-08 – ISO/IEC 27002:2022 A.8.24 – NIST FIPS 140-2

ID: 18 (version 1.1)	**Certificate validation requirements**
18	**When encrypting or verifying messages, it must be ensured that the certificate meets security requirements by checking the key holder's data, the validity of the certificate chain, expiration dates, and the Certificate Revocation List (CRL); report any non-compliant certificates as ICT-related Incidents.**
18.1	**<u>PKI-specific and certificate-related requirements:</u>** When a user encrypts the message sent to a receiver or verifies a received signed message, it must be checked whether the certificate fulfills the necessary security requirements. Certificates which do not meet the requirements listed below must be reported as an ICT-related Incident.
18.1.1	It must be verified whether the data of the key holder matches the subject or subject alternative name contained in the certificate.
18.1.2	It must be verified whether the whole certificate chain (up until the root-CA) is valid.
18.1.3	It must be verified whether the validity of the certificates has not yet expired.
18.1.4	It must be verified whether the certificates are not listed on the Certificate Revocation List (CRL) containing a list of all revoked certificates.
Protection goals Confidentiality, Integrity, Availability, Authenticity	**Key references** – ISO/IEC 27002:2022 A.8.24

ID: 19 (version 1.1)	Electronic messaging controls
19	**It must be ensured that all business information transfers use cryptographic measures to meet confidentiality, integrity, authenticity, and non-repudiation requirements, with encryption mandatory for "strictly confidential" data.**
19.1	Solutions for electronic business information transfer must provide adequate protection capabilities by using cryptographic measures to comply with the confidentiality, authenticity, integrity, and non-repudiation requirements of the transferred business information.
19.2	A concept to identify and consider the integrity requirements of the data must be defined and implemented.
19.3	For information which is labelled as “strictly confidential”, all communication should be encrypted.
Protection goals Confidentiality, Integrity, Availability, Authenticity	**Key references** – ISO/IEC 27002:2022 A.5.14

5. Roles and Responsibilities

5.1. Creator

The creator of the Encryption and Key Management Guideline is the ICT Risk Framework Unit (Specialist).

The creator of Encryption and Key Management Guideline has the responsibility to issue clear, precise, and appropriate written rules to give guidance for implementation to the target group. It is important to ensure that all required information is accurate, up to date and complete.

5.2. Guideline Owner

The owner of the Encryption and Key Management Guideline is Head of ICT Risk Framework Unit and LE CISOs (in case of adaption).

The most important tasks (not an exhaustive list) within the scope of responsibility are:

- Ensure completeness of the Guideline within functional area of responsibility
- Ensure correctness of content and the Guideline is up to date
- Define and conduct adherence oversight measures for Guidelines on a regular basis
- Assess impact on the Guideline with major focus on requirements as well as roles and responsibilities in the event of organizational changes, new products etc.

The Guideline Owner has at least an Expert or Head of Unit level (or LE pendant in case of adoption).

The Guideline Owner is responsible for publishing and updating the Encryption and Key Management Guideline according to established procedures within the organization.

6. Appendix

6.1. Contact Information

Please contact ICT Risk Framework in case of any questions related to this Guideline.

6.2. Document History

Document History

Version	Date	Changes & Background
1.0	17.01.2025	Initial set-up of this Guideline
1.1	15.08.2025	Yearly Review Guideline

Coordination before publication

Version	Date	Task	Name
1.1	23.05.2025	**Creator**	ICT Risk Framework Unit (Specialist)
	27.06.2025	**Content Review**	LE CISOs TISOs IT Ameli project
	27.06.2025	**Content Confirmation** Guideline Owner	Head of ICT Risk Framework Unit and LE CISOs

Approvals

Version	Date	Task	Name
1.0	13.12.2024	**Approval**	DBAG Chief Risk Officer (or LE pendant in case of adoption).
1.1	15.07.2025	**Approval**	DBAG Chief Risk Officer (or LE pendant in case of adoption).

6.3. Related Written Rules

Superordinated Written Rules	• ICT Risk Policy
Subordinated Written Rules	• n/a

6.4. Abbreviations

The abbreviations in this document are defined in the overall ICT Risk Glossary, which is provided on the Intranet website.

***** END OF DOCUMENT *****
