LIBRARY, ICT SERVICES & ARCHIVE

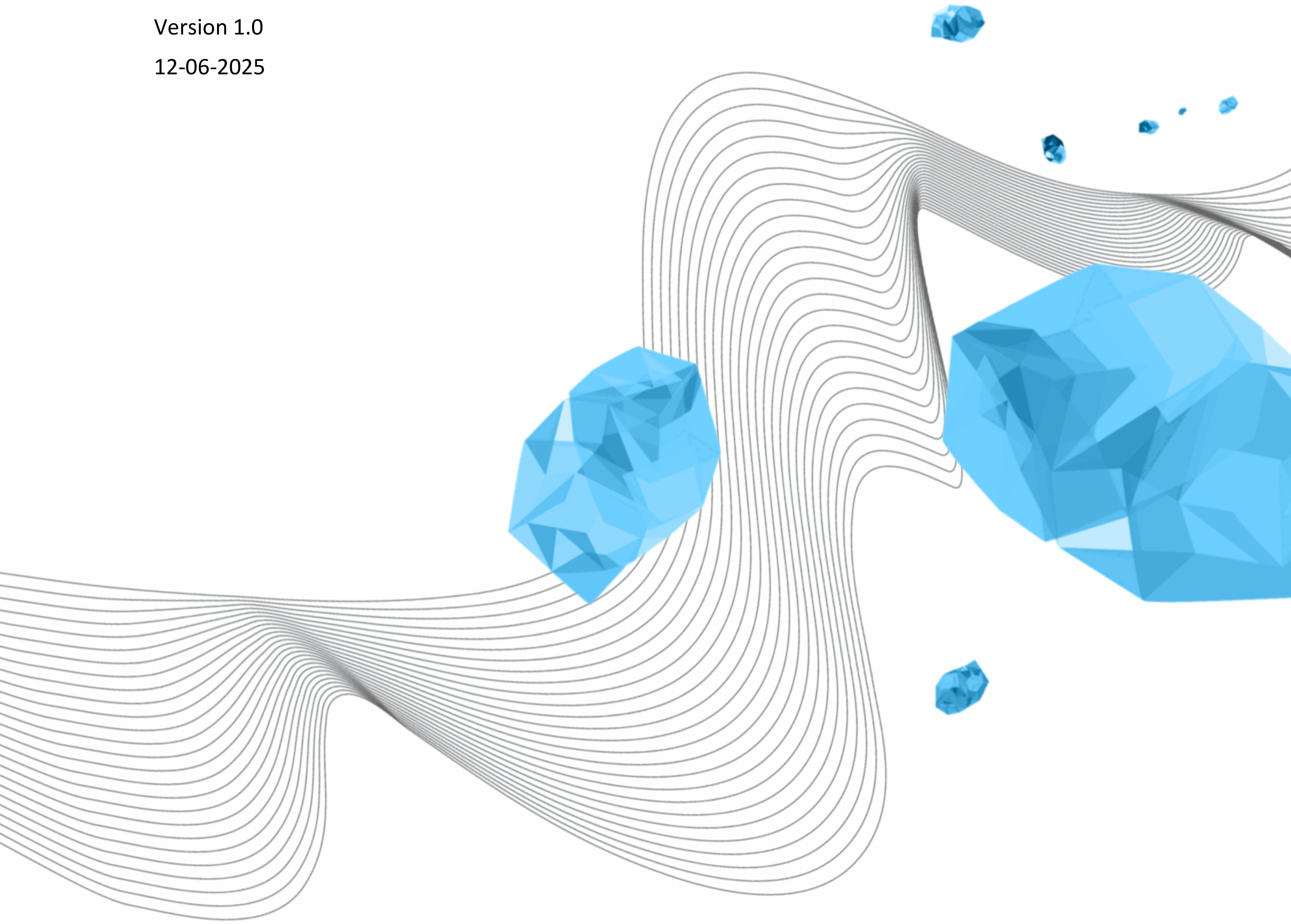
Status: Final
Date of adoption by LISA-MT: 10-06-2025
Revised:
Author: Peter Peters

CRYPTOGRAPHY POLICY

Peter Peters

Version 1.0

12-06-2025



UNIVERSITY OF TWENTE.

COLOPHON

ORGANISATION
Library, ICT Services & Archive

TITLE
Cryptography Policy

SUBJECT
Identification

PROJECT
[Project]

REFERENCE
LISA-0368

VERSION (STATUS)
1.0

DATE
12-06-2025

AUTHOR(S)
Peter Peters

COPYRIGHT
© University of Twente, The Netherlands.

DOCUMENT HISTORY

VERSION	DATE	AUTHOR(S)	REMARKS
0.1	13-1-2025	Peter Peters	Initial concept, based on version 1.0 of "Template-Standaard-Cryptografie" by SURF.
0.2	12-2-2025	Peter Peters	Extra attention to local PKI, which was in the SURF template but removed in version 0.1 of this document. A little more alignment with the accompanying document **Guidelines on using Certificates**.
0.3	14-5-2025	Peter Peters	Comment from Security team processed
0.9	6-5-2025	Peter Peters	For evaluation by LISA-MT as preparation for adoption by the EB.
1.0	10-6-2025	Peter Peters	Version adopted by LISA-MT Published version.

CONTENT

1 Introduction ... 4

1.1 Purpose ... 4

1.2 Scope and Applicability ... 4

1.3 Roles and Responsibilities ... 4

2 Standard Cryptografy ... 5

2.1 Cryptography Principles ... 5

2.2 Cryptography Use ... 5

2.3 Data Protection ... 6

3 Cryptographic Keys and Certificates ... 7

3.1 Key Management ... 7

3.1.1 General ... 7

3.1.2 Key Generation ... 7

3.1.3 Key Storage ... 7

3.1.4 Key Distribution ... 8

3.1.5 Key Change and Revocation ... 8

3.1.6 Key Backup and Escrow ... 9

3.1.7 Key (Emergency) Access and Recovery ... 9

3.1.8 Key Deactivation and Destruction ... 10

3.2 Certificate Management ... 10

3.2.1 Certificate Issuance ... 10

3.2.2 Certification Life Cycle ... 11

3.2.3 Revoking Certificates ... 11

3.2.4 Securing Private Keys ... 11

3.2.5 Monitoring and Audits ... 11

3.2.6 Incident Response ... 11

4 Review of this Policy ... 12

1 INTRODUCTION

This document describes the policy for Cryptography within the University, including requirements for managing cryptographic keys and digital certificates throughout their lifecycle. Additionally, it sets out the principles that form the basis for the ***Guidelines on using Certificates*** and the Key Management Procedure. In Appendix 1, roles and responsibilities are described.

1.1 PURPOSE

This policy ensures the proper and effective use of cryptography throughout the University, aligning with the Information Security Policy, relevant laws, and all statutory and contractual obligations. Additionally, cryptography must comply with limitations on importing, exporting, and using cryptographic hardware and software. Compliance with this policy will be periodically evaluated to ensure that cryptographic processes align with the established principles. This includes the management of cryptographic keys and digital certificates.

1.2 SCOPE AND APPLICABILITY

The scope of this cryptography policy encompasses all cryptographic keys and digital certificates generated by or for the University, distributed, stored, used, withdrawn, or removed.

1.3 ROLES AND RESPONSIBILITIES

In addition to the Policy on Information Security, specific roles and responsibilities are assigned to ensure the effective implementation, monitoring, and compliance with cryptographic management measures. The explicit assignment of these cryptographic roles and responsibilities is essential for operational information security and risk management within the University. A central register is maintained for assigning cryptographic roles to personnel.

See Appendix 1 for a detailed description of these roles and responsibilities.

1.4 GUIDELINES

Accompanying this policy is the document “Guidelines on using Certificates”[1]. This document will contain guidelines on technical details regarding using and implementing certificates. This will include allowed Certificate Authorities, Cryptographic Solutions and Algorithms, and more. Adoption of the guidelines will be handled by LISA-MT. LISA Security Management is responsible for keeping the guidelines up to date in line with the latest technical information and best practices.

Once the guidelines are published, this document will be updated with the link to the publication.

1.5 POST-QUANTUM CRYPTOGRAPHY

This document does not yet consider the dangers of quantum computers to cryptography. In later versions, we will pay more attention to post-quantum cryptography[2].

[1] https://www.utwente.nl/en/cyber-safety/cybersafety/legislation/guidelines-on-using-certificates.pdf

[2] https://www.aivd.nl/documenten/publicaties/2024/12/3/het-pqc-migratie-handboek

2 CRYPTOGRAPHY STANDARDS

2.1 CRYPTOGRAPHY PRINCIPLES

The University's cryptography policy is based on the following core principles:

1. **Minimum Access**
   Cryptographic keys and sensitive data must only be accessible to those who strictly need them for their work.
2. **Strong Cryptography**
   The University uses strong, accepted cryptographic algorithms and protocols that meet current international standards and guidelines.
3. **End-to-End Encryption**
   Sensitive data is protected using end-to-end encryption during storage, processing, and transmission.
4. **Regular Evaluation and Update**
   Cryptographic methods and techniques are regularly evaluated and updated per the latest scientific insights and technological developments.

2.2 CRYPTOGRAPHY USE

This policy outlines the following principles for using cryptography:

1. **Risk Assessment**
   Cryptographic controls are implemented based on a risk assessment, considering the sensitivity of the information. This is done per the BIA[3] and CIA[4]-classification described in the University’s Classification guidelines[5].
2. **Confidentiality**
   Cryptography protects the confidentiality of data while it is stored, processed, and/or transmitted.
3. **Integrity**
   Cryptography protects data integrity (e.g., by performing hash functions or digital signatures).
4. **Authenticity**
   Cryptography provides strong authentication for users and systems (e.g., digital certificates and smartcards).
5. **Irreversibility**
   Cryptography is used to prove the identity of an initiator of a critical transaction or communication and to demonstrate whether an event or action occurred (e.g., by digitally signing).
6. **Cryptographic Solutions**
   Only approved cryptographic solutions and tools are used. The specific list is maintained in the ***Guidelines on using Certificates***.

[3] Business Impact Analysis

[4] Confidentiality, Integrity and Availability

[5] https://www.utwente.nl/en/cyber-safety/cybersafety/legislation/classification-guideline-university-of-twente.pdf

7. **Cryptographic Algorithms**
   Only industry-accepted and standardized cryptographic protocols and algorithms with minimal and recommended versions and key lengths are used. The specific list will be maintained in the ***Guidelines on using Certificates***.
8. **Cryptographic Processes and Means**
   Those responsible within and outside our institution have access to processes, procedures, and means to manage cryptographic solutions, including:
   a. Assigning responsibilities for managing cryptographic solutions; see Appendix 1: Roles and Responsibilities.
   b. Dealing with conflicting legislation regarding using cryptographic solutions in different jurisdictions (e.g., by seeking advice from the Legal Department).
   c. Keeping cryptographic solutions up-to-date.
   d. Facilitating key management.
   e. Determining the impact of encrypted information on controls that rely on content inspection (e.g., detecting malware or filtering content).

2.3 DATA PROTECTION

This cryptography standard requires encryption to protect data in different stages.

1. **Data-at-Rest**
   Encryption encrypts sensitive data while it is stored, providing adequate protection against unauthorised access and theft.
2. **Data-in-Transit**
   Encryption protects all data during transmission against unauthorised interception, eavesdropping, manipulation, and access.
3. **Data-in-Use**
   Encryption protects data during use against unauthorised interception, access, and theft, particularly for data classified as “critical” or “(very) confidential” (e.g., Master keys, HSM keys, KMS keys).

3 CRYPTOGRAPHIC KEYS AND CERTIFICATES

3.1 KEY MANAGEMENT

Effective key management is crucial for securing processes related to generating, storing, archiving, restoring, retrieving, distributing, revoking, and destroying cryptographic keys. This policy outlines the minimum requirements for the University in this regard, based on ISO/IEC 11770-1 and ISO/IEC 27002:2022 section 8.24.

3.1.1 GENERAL

As a basis, the following issues should be taken into account:

1. **Key Lifecycle Management**
   All System Owners must have processes, procedures, and means to manage the lifecycle of cryptographic keys.
2. **Assigning Key Custodians**
   System Owners must assign Key Custodians to protect and manage cryptographic keys and key management systems.
3. **Protecting Cryptography**
   All cryptographic keys must be protected against modification and loss. Furthermore, secret and private keys must be protected against unauthorised use and disclosure. Equipment for generating, storing, and archiving keys must be physically protected.
4. **Ownership**
   Cryptographic keys used for protecting sensitive or confidential data of the University are the property of the organisational unit that is ultimately responsible for safeguarding this data.

3.1.2 KEY GENERATION

For generating cryptographic keys, it is required that they be generated:

- By the key owner or a trusted party (Key Custodian): The key must be generated by either the key owner or a trusted party authorised to create and provide keys securely.
- Using a hardware-, firmware- or software-based cryptographic module: The generation process must use a cryptographic module that meets legal requirements, regulations, and international standards.
- Per the ***Guidelines on using Certificates***.

3.1.3 KEY STORAGE

Cryptographic keys must be stored in a minimum number of locations. This ensures more control and oversight over all key locations and minimises the risk of misuse or unauthorised access to the keys.

Employees who handle cryptographic keys:

- Securely store them logically and physically.
- Store keys using an approved storage method (see also: ***Guidelines on using Certificates***)
- Record all locations, metadata, certificates, and logs of key management activities in a central key management system (Key Management System, KMS). These records must be protected against loss, destruction, or falsification and remain accessible for their entire storage period per legal requirements for decoding encrypted archives.

Note: Not applicable to public keys.

3.1.4 KEY DISTRIBUTION

The distribution of cryptographic keys with as few parties as possible helps the University keep track of and control all key locations and minimises the risk of keys being exposed to unauthorised parties.

Employees who handle cryptographic keys:

- Only share these keys with those who have been explicitly authorised.
- Limit the distribution of keys to as few recipients as possible.
- Ensure the confidentiality and integrity of transferred keys via approved cryptographic methods (see also: ***Guidelines on using Certificates***).
- Distribute keys via an approved transport mechanism (see also: ***Guidelines on using Certificates***).

Note: Not applicable to public keys.

3.1.5 KEY CHANGE AND REVOCATION

Timely replacing, disabling or revoking cryptographic keys per established processes, procedures, and methods (see also: ***Guidelines on using Certificates***) is essential to ensure the security of cryptographic systems.

When a service relationship or contractual agreement ends, cryptographic keys held by external parties or employees must be returned; this should coincide with revocation or cancellation processes for the affected keys in the central key management register.

Changes and revocations of cryptographic keys are:

- Carried out according to established processes, procedures, and methods.
- Documented, including reasons and dates of change or revocation, in a (central) key management system.
- Validated by authorised persons (such as the Key Owner) to ensure the process was carried out per policy.
- Monitored by IT Auditors, Security Managers and/or the Corporate Information Security Officer through periodic audits to ensure compliance with this key management policy.

Cryptographic keys are changed:

- When significant changes occur in the security risks.
- According to a predetermined rotation schedule per type of key.
- After critical updates or adjustments have been made to cryptographic algorithms.

Cryptographic keys are revoked:

- In case of suspected compromise (such as loss or theft), as part of an information security incident response.
- When a contractual relationship with an external party with access to the cryptographic keys ends.
- When employee roles change, or employment relationships with employees with access to the cryptographic keys end.
- When security requirements change for the end-of-life.

- When these are no longer needed.

3.1.6 KEY BACKUP AND ESCROW

Backups are made to recover cryptographic keys. Optionally, an Escrow may apply.

Key Backup

- Encrypted backup copies of cryptographic keys are stored in a highly secure environment that is physically separated from data and the primary key storage location to ensure physical security.
- Access to backup copies of cryptographic keys is strictly limited to authorised personnel (Key Custodian) and meets the principle of 'least privilege'.
- Periodic testing is performed to verify the integrity and availability of backup key backups.
- Owners of secret and private keys used for encrypting information about the University must make a compulsory backup copy of these encryption keys to prevent data loss.

Key Escrow

- The escrow process complies with legal and organizational requirements, ensuring the privacy and integrity of data.
- The trusted (third) party storing cryptographic keys in escrow is independent, reliable, and bound by strict security and privacy guidelines.
- Access to escrow key backups only occurs under strict conditions, as defined in the escrow policy, and is always documented and authorised by authorised personnel.
- The use of key escrow remains minimal to minimise the risks of misuse or unauthorised access.

3.1.7 KEY (EMERGENCY) ACCESS AND RECOVERY

Key Access:

- Access to cryptographic keys is restricted to only authorised individuals based on the principle of 'least privilege' (minimum access rights).
- The IAM process for identity lifecycle management applies to roles within the cryptographic process (Ingress, Egress, Transit).

Emergency Access:

- Procedures have been developed for safe and controlled emergency access to cryptographic keys in case of an incident or emergency situation.
- Emergency access can only be granted to authorized individuals after approval by the competent authorities and only for the duration of the emergency situation.
- Every form of emergency access is fully documented, including reasons, time of access, granted access rights, and actions taken.

In response to legal requests for access to encrypted data, a strict process is followed for the controlled release of cryptographic keys. All requests and actions are recorded and carried out under the supervision of legal and security personnel.

Key Recovery:

- Procedures have been established for the safe and controlled recovery of cryptographic keys in case of loss, damage, or emergency situations.

- Recovery procedures are only accessible to authorised individuals and are equipped with strong authentication and authorisation to prevent unauthorised access.
- All key recovery activities are recorded, including the steps taken, involved personnel, and timelines for the recovery process. Recovery actions must be evaluated after completion for future improvement of disaster recovery plans.

3.1.8 KEY DEACTIVATION AND DESTRUCTION

Key Deactivation:

- Cryptographic keys are immediately deactivated and/or withdrawn when they are no longer needed, such as after a contract ends, the key lifetime expires, or suspicion of compromise arises.
- Deactivation processes must ensure that the keys are no longer accessible or usable and that all involved systems and users are notified of the deactivation.
- Deactivated keys are stored in a secure environment until a decision is made about their definitive destruction or reuse.

Key Destruction:

- Keys are safely and irretrievably destroyed as soon as they are no longer needed or when security regulations require them to prevent unauthorised access or reuse.
- Devices containing cryptographic keys must be securely removed or destroyed at the end of their lifecycle.
- Destruction of keys is carried out through approved methods per the sensitivity of the data protected by the keys, such as physical destruction, overwrite, and/or cryptographic processes for erasure, as specified in the ***Guidelines on using Certificates***.

All actions related to key deactivation and destruction, including the date, method of destruction, and responsible personnel, are documented and stored for audit and compliance purposes.

3.2 CERTIFICATE MANAGEMENT

Digital certificates are used to authenticate identity, encrypt data, and facilitate secure communication within the University's infrastructure and in interactions with external partners. The certificate management processes must comply with international norms, standards, and guidelines defined by organizations such as ISO, NCSC, NIST, ETSI, IETF, and CA/B Forum.

3.2.1 CERTIFICATE ISSUANCE

- Certificates are only issued by trusted certificate authorities (CAs). Security Management maintains the list of approved CAs in the ***Guidelines on using Certificates***.
- LISA can set up an internal Public Key Infrastructure (PKI) for issuing digital certificates that are only trusted within the University, with the issuing and management processes fully under the control of LISA. This PKI serves as the basis of trust ("Root-of-Trust") for the University. See the ***Guidelines on using Certificates*** for details.
- Certificates for external purposes are issued by external, globally recognised public CAs that meet the requirements of the CA/Browser Forum and international standards such as ISO/IEC 21188 and ETSI EN 319 411-1. This way, external parties can trust that communication with the University is secure. See the ***Guidelines on using Certificates*** for details.

3.2.2 CERTIFICATION LIFE CYCLE

- The life cycle of digital certificates is managed and supported by the University's central certificate management system, which is entirely under LISA’s control.
- Certificate management processes are highly automated to minimise human errors, prevent system downtime due to expired certificates, and efficiently renew certificates.

3.2.3 REVOKING CERTIFICATES

- A certificate is revoked immediately upon compromise of the key, incorrect data, service or contract termination, or changes in security requirements.
- The University uses authorised mechanisms to validate the status of certificates, as specified in the ***Guidelines on using Certificates***.

3.2.4 SECURING PRIVATE KEYS

- Private keys are securely generated, distributed, and stored per the ***Guidelines on using Certificates***.
- Access to private keys is strictly controlled and logged.
- Multi-factor authentication (MFA) is applied to secure access.

3.2.5 MONITORING AND AUDITS

- Continuous monitoring is performed to ensure the validity and integrity of certificates.
- Regular audits of the certificate management process are conducted to ensure compliance with laws, international standards, and guidelines.

3.2.6 INCIDENT RESPONSE

- In the event of an incident related to cryptographic certificates, such as a data breach or compromise of a CA, the University's Cyber Security Incident Response Plan is immediately activated.
- There are clear procedures for escalating certificate-related incidents and for timely informing relevant parties (stakeholders).

4 REVIEW OF THIS POLICY

This policy will be reviewed at least every three years. The following review will be in mid-2028. There may be grounds for an interim evaluation. If that evaluation gives cause to do so, this policy will be adjusted sooner.

The review will be conducted in cooperation with the Product Focus Group for Certificate Services.

The CISO of the University of Twente is responsible for these guidelines.

MT-LISA determines these guidelines. In cases not provided for in this regulation, MT-LISA decides with the CISO.

5 APPENDIX I ROLES

Rol	Description	Responsibilities
Key Owner	A **Key Owner** is the person or entity[6] responsible for the functional accountability of a cryptographic key. The **Key Owner** is ultimately responsible for the security and correct use of the cryptographic key throughout its life cycle and has the authority to make decisions regarding the use of the key. The "Systeemeigenaar" is also the Key Owner for all information systems within the University.	**Access Control**: Assigning access rights to authorised users, such as the **Key Manager** and **Key Custodian**, and registering this in a central key management register. **Security**: Establishing security measures surrounding the use and storage of the key. **Compliance**: Ensuring compliance with internal and external cryptographic standards, guidelines, and procedures. **Incident Management**: Making decisions regarding key rotation, revocation, or removal in the event of IT security incidents such as key compromise or loss.
Key Manager	A **Key Manager** is responsible for the day-to-day operational management of cryptographic keys throughout their life cycle. A **Key Manager** uses a Key Management System (KMS) and ensures that keys are used and stored correctly according to this Policy, and operational procedures. Within the University, the role of **Key Manager** has been delegated to a System or Application Administrator who has the delegated responsibility (on behalf of the **Key Owner**) for using and managing cryptographic keys per this Policy.	**Implement**: Implement approved cryptographic solutions, methods, and algorithms in their respective systems. **Configure**: Ensure correct configuration and keeping up-to-date with cryptographic solutions and tools. **Document**: Documenting the applied cryptographic solutions, methods, and algorithms, with cryptographic components included in the System Baseline and Maintenance (SBoM) of the information system. **Log**: Registering all key management activities, such as generation, access, rotation, revocation (deactivation), and destruction of keys, supported by a central key management system ('Key Management System', KMS).

[6] Group, organization, device, system, or cryptographic module

		Manage: Managing the lifecycle of system-specific cryptographic keys. **Monitor**: Monitor the effectiveness of cryptographic management measures and report any problems. **Incident response**: Assist in cybersecurity incident response related to cryptographic keys and digital certificates (e.g., key compromise or certificate expiration). **Awareness & training**: Participate in relevant training to stay up-to-date with cryptographic practices.
Key Custodian	A **Key Custodian** is a highly trusted official within the University or with a trusted third party who has delegated responsibility for managing the physical and logical security of cryptographic keys. The **Key Custodian** ensures that only authorized individuals (such as **Key Managers**) have access to the keys and supports the distribution of keys. A **Key Custodian** is NOT responsible for generating keys, but may be involved in documenting the key management process and implementing security protocols. Within the University**, Key Custodians** are coordinated by a Security Manager and are Administrators of LISA.	**Secure Storage**: Storing cryptographic keys according to established procedures. **Distribution**: Distributing cryptographic keys according to established procedures **Deactivation**: Taking out of use and revoking cryptographic keys according to established procedures. **Destruction**: Destroying cryptographic keys according to established procedures. **Logging**: Recording all physical and logical access actions with cryptographic keys in a key management system. **Key Ceremony**: Participating in a key generation ceremony by (partially) introducing a cryptographic key.