POLICY AND GUIDANCE
Do not Photocopy

Document Information Classification: Unrestricted

Title:	**TRE Key Management Policy**
Effective Date:	**07 Jun 2019**
Reference Number:	**ISMS-09-07**
Version Number:	**1.5**
Owner:	**TRE Infrastructure and Security Management Process Owner,**
Review Date:	**07 Jun 2021**

Table of Contents

1. Purpose

A policy on the use of cryptographic controls for protection of information should be developed and implemented and a policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle.
This policy describes the methodology for cryptographic key management within the Trustworthy Research Environment (TRE).

The ability to encrypt sensitive information contained within the TRE is fundamental to operating a secure data analytics facility as it protects information against unauthorised access. Such measures are necessary to maintain the confidentiality and integrity of critical information such as research datasets, user accounts and device configuration, both in local storage and transmission across the network. Cryptographic controls protect confidential information against unauthorised access.

A robust and well-designed key management system is also essential in ensuring that data secured by cryptographic mechanisms does not become unrecoverable and hence unavailable to users.

2. Scope

This policy covers the *generation, destruction, revocation, distribution, replacement, storage* and *use* of cryptographic keys. These keys are used to secure the following data storage and access mechanisms that are provided by the Trustworthy Research Environment (TRE):

- Files and directories within a file-system (file-level encryption)
- Block storage such as an LVM container (block-level encryption)
- Secure shell connections (SSH key pairs)
- SSL server certificates for hosted web services (OpenSSL)

3. Responsibilities

The Information Security Manager (ISM) is responsible for:

- Maintaining awareness of cryptographic best practice and providing guidance for the development of TRE infrastructure and software applications hosted within the TRE
- Developing, implementing and managing measures put in place to minimise the likelihood or consequences of a key compromise
- Operating a recovery plan to tackle unauthorised disclosure of a key
- The management of cryptographic keys, including the ability to view keys in plain-text or cipher text form
- Conducting an investigation in the event data becomes unrecoverable (cannot be decrypted)
- Coordinating the key compromise and recovery plan

The Operations Manager is responsible for:

- Ensuring the cryptographic mechanisms and the key management system are installed, tested and operational, and that these mechanisms meet the requirements of data owners/controllers, are patched and kept up to date, and where possible provide the optimum levels of security
- Providing adequate training for system administrators to ensure they are suitable qualified and competent to operate the TRE key management system and to implement the necessary cryptographic measures within the TRE infrastructure

- Selecting the appropriate cryptographic and key management algorithms that meet the objectives of the data management application, for example; transmission/reception of data, or 'data at rest'.
- Coordinating the key compromise and recovery plan

The TRE System Administrators are responsible for:

- Installation and configuration of the key management system within the TRE
- Configuring components used for data storage and transfer to support the technical specification of the cryptographic measures implemented within the TRE infrastructure
- Assisting in the key compromise and recovery plan

4. Methodology

4.1. Key Usage

The TRE Key Management system handles cryptographic keys used for the following scenarios.

4.1.1. Mounted storage volumes

During boot, virtual machines provisioned by the TRE automatically mount to their associated block level storage volumes. These storage volumes are for the TRE user to store their data. When a block level storage volume is created, it is encrypted with dm-crypt using the virtual machine's kernel. When the virtual machine boots, the mounted storage volume is automatically decrypted. When the virtual machine is shut down and the storage volume un-mounted, the block level storage volume is automatically encrypted.

The Key Manager backs up the LUKS header of the block level storage volumes and stores the keys.

4.1.2. Local file encryption

TRE users who need to analyse and/or process datasets stored within the TRE must first move a copy of the data into a storage volume permanently attached to the virtual machine (e.g. /home or My Documents). TRE users protect their data using a passphrase that operates a symmetric encryption key.

The Key Manager stores these symmetric-keys.

4.1.3. SSL certificates for hosted web services

The TRE hosts various web services that can only be accessed via a web client (browser) running on a TRE provisioned virtual workstation. The web browsers must authenticate a trusted server source before a connection can be established. This is achieved by implementing self-signed SSL certificates within the web services.

The Key Manager creates and manages self-signed SSL certificates.

4.1.4. File level backups

Some file system directories on TRE virtual machines are backed up to a remote storage device. By default, this includes the users home directory. GPG keys are used to create encrypted blocks of directory contents on the remote storage device. The backups are created, restored and tested according to the TRE Data Backup Policy. Each backup is encrypted against three GPG keys, a project instance private key, a TRE admin public key and a TRE admin offline public key.

The off-line TRE admin key has never been installed on a networked machine and is considered a safe key (un-tampered with) and therefore is guaranteed to not be compromised.

The Key Manager creates and stores the GPG keys.

4.2. Key Selection

The choice of cryptographic algorithms used within the TRE has been determined by the objectives and security requirements of data applications needed by TRE users. For example, the requirements for data transit include the need to maintain the confidentiality and integrity of data, and to verify the authenticity of the source and destination.

These requirements have determined the type of cryptographic keys that are used to protect data and which will be controlled by the key management system. For example, to maintain confidentiality of data at rest, symmetric encryption keys are used. For data in transit, integrity protection keys such as MACs are used. TRE users are able to authenticate the services hosted in the TRE by means of pre-shared symmetric keys used for trusted certificates installed on the TRE servers.
Consideration is also made to the selection of keys used to encrypt other keys prior to distribution to users (symmetric key-wrapping keys).

4.3. Key Storage

The Key Management system stores all keys in a KeePass database on an encrypted portable storage device which is secured in a physical safe located at Vaughan House. Members of the Information Security Management System team can access a physical key for this safe.

The adopted security principle is that the cryptographic strength of keys used to encrypt this portable storage device and the KeePass database are equivalent to, or greater than the keys being protected. A minimum of the TRE System Administrator and the Information Security Manager keep keys to access the portable storage device and the KeePass database.

Software applications produced at CHI and operational within the TRE are designed such that the standard application level code never reads or uses cryptographic keys, and instead use key management libraries.

4.4. Key Recovery

The TRE Business and Continuity Plan (ISMS-03-03) describes how cryptographic keys are backed up, and what recovery scenarios are routinely tested. It includes the following stages:

- Notification of stakeholders in the event of planned and unplanned service unavailability
- The responsibilities of the personnel required to support and perform the recovery actions
- An inventory of all cryptographic keys and their use, including the storage devices used for backups
- Identification of all information that may be compromised as a result of the incident
- Identification of all signatures that may be invalid, due to the compromise of a signing key
- User SSH public keys are backed up with their /home directories
- Storage volume encryption keys are backed up
- Routine tests are conducted to restore and decrypt user data by recovering the associated storage volume and its encryption key

5. Cross-referenced ISMS Documents

Number	Type	Title
ISMS-03-03	ISMS\Policy & Guidance\TRE Operations - policy & guidance	TRE Disaster and Severe Incident Recovery Plan

6. Appendices

None