SUNET Key Management Policy

Introduction

Overview

The Swedish University Network (SUNET) Key Management Infrastructure is a set of infrastructure component used to manage security-critical cryptographic keys. The SUNET Key Management Infrastructure includes servers, network equipment and hardware security modules. This document describes the policy for the SUNET Key Management Infrastructure.

The SUNET Key Management Policy (this document) along with a set of application specific Key Management Practice Statements and the SUNET Key Management Infrastructure constitute the SUNET Key Management Facility. This document follows the outline Key Management Policy from NIST SP 800-57, part 2 to the extent that it has been deemed applicable and commensurate with Swedish Law.

The SUNET Key Management Facility is a SUNET infrastructure service under the control of the SUNET office of the CEO. The SUNET Key Management Facility is available for use by applications and services offered by SUNET, NORDUnet and their direct customers.

Objectives

The keys managed by the SUNET Key Management Infrastructure are used to protect critical security infrastructure and personal identity information. The intrinsic value of the resources protected is low but the immaterial value of a security incident is comparatively large. SUNET and its partner organizations have been active Internet citizens for a long time and have been relatively successful in protecting against several forms of attack.

The services and infrastructure protected by the keys managed by the SUNET Key Management Infrastructure constitute an attractive attack target, not because of the value of transactions conducted on these systems but because of the potential PR-value of such an attack.

Threats

The primary threats are:

- theft of personal data including personal identifiable information and user credentials
- impersonation and subversion of critical system components
- impersonation of users at relying party services by subverting identity providers

Principles of Operation

The guiding principles of the SUNET Key Management Infrastructure are:

- Each private key belongs to a hierarchical sequence of security zones as follows: black zone is contained in red zone and has higher security requirements than red zone. Similarly red zone is contained in blue zone and has higher security requirements than blue zone.
- No private key may leave its designated security zone unless protected by another key which lives in a higher security zone.
- Security zones map to baseline security controls from NIST SP 800-54:

Zone	**NIST 800-54 / FIPS 199 Level**
Black	HIGH
Red	MODERATE
Blue	LOW

The precise employment of security controls to match these levels is described below. Normally the 'black' zone is reserved for long-term private keys, audit logs, hardware security module backups and other forms of off-line key containers. The 'red' zone is typically used for production online hardware security modules and other Key Containers used by user-facing services.

Community and Applicability

The SUNET Key Management Infrastructure is used for (among other things) the following applications:

- SUNET eduID Service
- SWAMID Metadata Service
- Dante Association REEP and FaaS service

All applications will publish a Key Management Practice Statement that describe the operational details specific to that application. Some applications will reference common Key Management Practice Statement documents if they are sufficiently similar. Key Management Infrastructure operates several logical and physical Key Containers (hardware security modules, servers etc.) and several Cryptographic Keys stored in those containers.

Central Oversight Authority and Key Materials Managers

The Central Oversight Authority for the SUNET Key Management Infrastructure is the SUNET CEO who may delegate this authority to the SUNET CISO ("Säkerhetsansvarig") role. Each application will identify an Application Key Materials Manager role which may be held by one or more individuals. Unless otherwise specified the Application Key Materials Manager role is assigned to the Product Manager ("systemförvaltare") of the SUNET service which uses the key(s).

Key Container Operators

Each Key Container is assigned a set of Key Container operators tasked with technical management of the Key Container. The Key Container Operator role is appointed by the Central Oversight Authority. Each Key Container Operator will be assigned a PGP key on a hardware token to be used for authentication. Each Key Container is also assigned an entry in the Key Container Audit Log (cf. below).

Contact Details

SUNET vid Vetenskapsrådet
Attn: Säkerhetsansvarig
Tulegatan 11, 2tr
113 53 Stockholm
e-mail: security@sunet.se

SUNET Key Management Policy (KMP)

General Provisions

Obligations

Central Oversight Authority

The SUNET Central Oversight Authority is responsible for the overall security and operations of the SUNET Key Management Infrastructure and is responsible for the secure operations of infrastructure common to all Key Management Infrastructure applications. This includes making sure that the appropriate contracts and agreements are in place to operate and maintain Key Management Infrastructure logical and physical infrastructure.

Application Key Materials Manager

All Application Key Materials Managers will report on application security to the SUNET Central Oversight Authority and will respond to incidents and threats specific to that application.

Key Container Operator

All Key Container Operators will report on Key Container security to the SUNET Central Oversight Authority and will respond to incidents and threats specific to that Key Container.

Liability and Financial Responsibility

SUNET is a part of the Swedish Science Research Council (Vetenskapsrådet) and is covered by a Professional Services insurance from Kammarkollegiet.

Interpretation and Enforcement

These Terms and any dispute or claim arising out of or in connection with them or their subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the legislation of Sweden. The courts of Sweden will have exclusive jurisdiction over any such dispute or claim.

Fees

Fees are set down in the NORDUnet HSM Service agreement.

Publication and Repositories

The SUNET Key Management Policy (this document) along with any applicable Key Management Practice Statement documents is published on http://www.sunet.se/kmf

Each application will provide a repository where any public artefacts (eg. public keys, certificates, CRLs or fingerprints) related to the Key Management Infrastructure is made available. The SUNET Key Management Infrastructure website will provide informational links to each public repository.

Confidentiality Policy

SUNET Key Management Policy (KMP)

The SUNET Key Management Infrastructure is governed by Swedish law which regulate information dissemination and confidentiality for all government agencies. The public information principle (SFS 1949:105 §1) states that except under certain specific conditions, all government documents are public. The private keys and any related information, software and configuration used by the SUNET Key Management Infrastructure will be treated as secret information ("sekretess") in the sense of SFS 2009:400 §1 and will not be provided under the public information principle.

Intellectual Property Rights

All IPR related to the SUNET Key Management Facility owned by SUNET is made available under the SUNET BSD License (for software) and Creative Commons Attribution-Share Alike 3.0 Un-ported License for documentation including this document and any applicable Key Management Practice Statements.

Identification and Authentication

The SUNET Key Management Policy is mainly used to manage infrastructure component keys. Identification is therefore limited to duly designated Key Container Operators and Application Key Materials Managers responsible for key provisioning and application integration. Identification is to be done on the basis of either in-person validation of a government issued identification document (eg. passport or driver's license) or in-person verification of another form of credential for individuals whose identity is already well established by other means, for instance by verifying a PGP key fingerprint.

Application Key Management Practice Statement documents will describe the detailed key generation, re-generation, revocation and rollover mechanisms as they are application dependent.

Operational Requirements

The Key Management Infrastructure consists of several logical and physical Key Containers (hardware security modules, servers etc) and several Cryptographic Keys stored in those containers. A Key Container may be either online where the keys or cryptographic functions are available to other systems and devices, or offline where the Key Container is stored in an inert state and not actively use. Each Key Container is restricted to a single security zone and may not move to a lower security zone unless protected by a key belonging to a higher security zone.

Key Container Storage and Transport

Transport and offline storage of the Key Container Audit Log Device, Key Containers and Key Container in transport require the use of tamper evident bags . Suggested models include MMX Industries or AMPAC. It must not be possible to open a tamper evident bags without it being noticed upon inspection of the tamper evident bags. The use of tamper evident bags is to ensure that data stored on devices in the tamper evident bags has the same state as when it was deposited in the bag. This provides an additional level of protection against malicious tampering with Key Containers and Key Container Audit Logs.

When transporting a Key Container it must be protected by a tamper evident bag or if that is impractical, must be protected from tampering in such a way that it is impossible to extract or modify the keys contained in the Key Container. If a Key Container must be transported with active keys in it and the use of tamper evident bags is not possible, it must be accompanied by at least 2 duly appointed representatives of the Central Oversight Authority. All such activities must be logged in the Key Container Audit Log (cf below).

Key Container Initialization and Access Control

Initialization of a Key Container is the process by which a Key Container is prepared for use. This process must be followed both when a Key Container is received from a vendor and when it is being reused. Key Container initialization must involve a full reset of any data storage device included in the Key Container. The precise details of Key Container Initialization must be described in the Key Management Practice Statement.

All Key Containers must be initialized using equipment and services maintained in the same zone as the Key Container being initialized. Such equipment and services must not have material dependencies on equipment or services outside the zone in a way that may impact the Key Container initialization. Specifically all equipment used must

- be disconnected from anything except a network in the same zone
- must be provided with at least one source of true random entropy only available in the same zone
- be disconnected from any non-essential peripheral equipment
- be clearly identified with the zone it belongs to

In addition the following specific requirements apply:

- In the 'black' zone, all wireless and wired network cards must be disabled.
- In the 'red' zone all wireless network cards must be disabled.
- In the 'red' zone network connectivity is permitted.
- In the 'red' zone a firewalled connection to the Internet is permitted.
- In the 'red' zone only clearly defined services (including SSH) may be reachable from the 'blue' zone network.
- In the 'blue' zone, both wired and authenticated wireless networks are allowed.
- In the 'blue' zone, only clearly defined services may be reachable from the Internet.

Certain forms of Key Containers allow a form of virtualization. In this case the virtual Key Containers will be located in the same zone as the parent Key Container. When a Key Container is initialized an audit log covering all activities related to that Key Container is established (cf below).

Each Key Container is assigned a set of Key Container operators tasked with technical management of the Key Container. The Key Container Operator role is appointed by the Central Oversight Authority. Each Key Container Operator will be assigned a PGP key on a hardware token to be used for authentication. Each Key Container is also assigned an entry in the Key Container Audit Log (cf below).

SUNET Key Management Policy (KMP)

Access to a Key Container must be restricted to Key Container Operators and the Central Oversight Authority using technical, physical and logical access control. Physical access to Key Containers in the 'red' zone must be restricted using at least 3 independent access layers, 1 of which must be available only to the Key Container Operator and to the duly appointed representative of the Key Container Operator. Physical access to Key Containers in the 'black' zone must be restricted using at least 4 independent access layers when not in use, 2 of which must be available only to the Key Container Operator.

Entropy

Key Generation critically depends on the availability of a good source of true random numbers for the key generator. The entropy source used to derive the random numbers must be based on a physical process (eg. a source of quantum noise) and must not be a Pseudo Random Number Generator (PRNG).

Key Generation

Normally and if applicable, keys should be generated on the Key Container where it will be used. In certain situations it may be necessary to generate keys on a separate device and transfer to the Key Container. In that case great care must be taken to avoid key leakage, especially if the device used is in the 'black' zone.

Key Rollover

All conditions and requirements for key generation apply equally to key rollover.

Key Container Audit Log

The Key Container Audit Log will be maintained on a portable storage device containing a plain text file for each Key Container that clearly identifies the Key Container or class of Key Container it relates to. The files will be maintained in a Version Control System (VCS) supporting signed modifications. After each log annotation, the modification will be committed in the VCS and finally the update signed by a PGP key of the Key Container Operator.

Each time the Audit Log storage device is closed the hash of the last signed update is printed and affixed to a tamper evident bag used to store the Audit Log Device. Each time the Audit Log device is removed from the tamper evident bag, the last entry is verified with the label printed on the bag. If there is a mismatch, the signatures on all updates in the log must be verified for correctness by verifying against the set of trusted Key Container Operator PGP keys.

The format of Audit Log Message is unspecified but must include the following information:

- timestamp
- the affected Key Container
- operation performed on the Key Container
- people involved
- text annotations

It is expected that all Key Containers at a site will be able to share a common Key Container Audit Log Device in the form of a small laptop with USB sticks as a backup mechanism.

Key Termination

Decommissioned keys must be marked as ‘do not use’ in the appropriate application and must be overwritten in the applicable key containers before the container is allowed to leave the zone it is in.

Key Container Termination

Key Containers must be destroyed by shredding or other mechanism that ensure destruction of any remaining key materials.

Key Management Infrastructure Termination

Should it become necessary to terminate the SUNET Key Management Infrastructure, all active Key Containers must be securely destroyed by the mechanism described above.

Cryptographic Key and Certificate Formats

Industry standard formats must be used throughout. The SUNET Key Management Infrastructure will normally publish public keys as X.509 self-signed certificates.

Specification and Administration

Change control for this specification is controlled by the SUNET Central Oversight Authority.