SUNET

Document Information

SUNET Asymmetric HSM Service KMPS

Introduction

This document is the key management practice statement for the SUNET Asymmetric HSM Service relative to the SUNET Key Management Policy (SUNET KMP). Note that this document does not specify a KMPS for all services using the HSM Service although by technical necessity the choices for which technical controls are implemented at the application level is restricted by the technical choices for the HSM Service. Such limitations are called out below.

Terminology

- SUNET KMP: Key Management Policy - a document describing the SUNET KMF.
- SUNET KMF: Key Management Facility - the combination of procedures and resources covered by the SUNET KMP.
- PED: Secure path authentication terminal used by Luna HSMs
- PED Key: Secure path authentication token used by Luna HSMs
- Partition: Logical PKCS11-device in an HSM. A partition may contain multiple keys.
- Domain: Logical administrative separation in Luna HSMs, contains multiple Partitions
- Zone: An area of protection of the KMF.
- HSM Appliance: The server physically enclosing the cryptographic engine of the HSM
- Service: A logical set of clients of the HSM sharing a single partition.
- Service KMPS: The Key Management Practice Statement of a Service.
- Client: A credential used to identify and authenticate a connection to an HSM partition.

Service Description

The SUNET Asymmetric HSM Service operates a virtualiazable HSM environment based on clustered Luna SA network HSM for use by other services. Each connected service is assigned a partition in the HSM and communicate with the HSM cluster with TLS tunnels.

In addition to the network HSMs the services operates protected backup of HSM partitions using special offline Backup HSMs. In terms of the SUNET KMP the HSMs are zoned as follows:

- The Network HSMs are operating in RED zone (cf SUNET KMP)
- The Backup HSMs are operating in BLACK zone (cf SUNET KMP)

Logical Access Control

The following logical protections are in place for the HSM environment:

- network level access control implemented in Juniper SRX firewalls set to a default-deny policy for both incoming and outgoing connections.
- all HSMs are connected to a management network which allows connection of an HSM

management laptop for use with remote PED.
- TLS-based access control for PKCS11 access to the HSM cluster nodes tying each client certificate to a single partition.
- PED-based authentication for all HSM, Domain and Partition operations
- M-by-N in place for all HSM and Domain PED keysets

Physical Access Control

The HSM cluster is located in 2 sites: TUG and FRE. At TUG the 3 levels of physical protection for the network HSMs specified by the SUNET KMP are: outer door, data center door and rack door. Each door is locked and only SUNET and authorized NUNOC personnel have access to keys and/or RF access tags required to open the door(s). The Backup HSMs are stored in safes mounted in the same racks as the network HSMs. The safe door constitutes the BLACK zone 4th level of physical protection.

Environmental Controls

HSMs are located in datacenters equipped with fire-suppression, intrusion detection and alarms, and electronic door access control.

Roles and Responsibilities

Key Container Operator

The HSM Key Container Operator (KCO) is a system administratrator role. The KCO is able to SSH to the HSM appliance and will have access to an Orange Remote PED Key and (if applicable) a Purple Resplit Key.

Security Officer

The HSM Service Security Officer (SO) is the Application Key Materials Manager (cf KMP) for the HSM service. It is a role split over several trusted employees of SUNET and NUNOC. The SO will share (in a 2 by 5 configuration) HSM Admin and HSM SO Domain keysets. These keys will be stored in individual compartments in tamper-evident bags in a locked safe between use.

Changes and Procedures

All procedures described below must be performed in such a way that logs are kept. If at any step, a fault or unexpected event occurs that can call the security of the process into question, the process must be terminated and incident management must be initialized.

All procedures in the KMPS are documented separately. Each time a procedure is executed a copy of the procedure document PDF is printed and filled out as a written record. The resulting bundle is stapled together with the tear-off serial tags from the tamper evident bag s used to store outgoing SO key chains and included in the log binder.