ProCrypt KM-3000 Hardware Security Module

Security Target

Common Criteria EAL4+

Version 1.0
July 10th 2019

www.procenne.com

This page intentionally left blank.

Contents

List of Tables

List of Figures

Glossary of Terms

Black data	Cryptographically protected user data representing user information. If this information needs protection in confidentiality the data shall be encrypted. If this information needs protection in integrity a cryptographic MAC or digital signature shall be associated with this data to detect modification.
Compromise	The unauthorized disclosure, modification, substitution, or use of sensitive data (including plaintext cryptographic keys and other CSPs).
Confidentiality	The property that sensitive information is not disclosed to unauthorized individuals, entities, or processes.
Critical security parameter (CSP)	Security-related information (e.g., secret and private cryptographic keys, and TSF data like authentication data) whose disclosure or modification can compromise the security of a cryptographic module.
Critical TSF	TSF that, upon failure, could lead to (i) the disclosure of secret keys, private keys, or CSPs or (ii) modification of public root keys. Examples of the critical functionality include but are not limited to random number generation, operation of the cryptographic algorithm, and cryptographic bypass.
Security Officer	An authorized user who has been granted the authority to perform cryptographic initialization and management functions (including key management) cryptographically unprotected data in the red area of the IT system. These users are expected to use this authority only in the manner prescribed by the guidance given to them.
Crypto User	An authorized user assumed to perform general security services, including cryptographic operations and other Endorsed security functions.
Cryptographic algorithm	A well-defined computational procedure that takes variable inputs that usually includes a cryptographic key and produces an output, e.g., encryption, decryption, a private or a public operation in a dynamic authentication, signature creation, signature verification, generation of hash value.
Cryptographic boundary	An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module.
Cryptographic functions	TSF implementing cryptographic algorithms and/or protocols for - encryption and decryption, - signature creation or verification, - calculation of Message Authentication Code, - entity authentication, - key management.

Cryptographic key (key)	A parameter used in conjunction with a cryptographic algorithm that determines - the transformation of plaintext data into ciphertext data, - the transformation of ciphertext data into plaintext data, - a digital signature computed from data, - the verification of a digital signature computed from data, - a Message Authentication Code computed from data, - a proof of the knowledge of a secret, - a verification of the knowledge of a secret or - an exchange agreement of a shared secret.
Cryptographic key component (key component)	A parameter used in conjunction with other key components in an Endorsed security function to form a plaintext cryptographic key by a secret sharing algorithm (e.g., the cryptographic plaintext key is the xor-sum of two key components).
Cryptographic module	The set of hardware, software, and/or firmware that implements Endorsed security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.
Cryptographic protocol	A cryptographic algorithm including interaction with an external entity (e.g., key exchange).
Decryption algorithm	Algorithm of decoding a cipher text into the plaintext using a decryption key. The decryption algorithm reproduces the plaintext which where used to calculate the cipher text with the corresponding encryption algorithm and the corresponding encryption key.
Destruction of data	A method of erasing electronically stored data, cryptographic keys, and CSPs by altering or deleting the contents of the data storage to prevent recovery of the data.
Differential power analysis (DPA)	An analysis of the variations of the electrical power consumption of a cryptographic module, using advanced statistical methods and/or other techniques, for the purpose of extracting information correlated to cryptographic keys used in a cryptographic algorithm.
Digital signature	The result of a asymmetric cryptographic transformation of data which, when properly implemented, provides the services of 1. origin authentication, 2. data integrity, and 3. signer nonrepudiation.
Electromagnetic emanation analysis (EMEA)	Analysis of electromagnetic emissions from a device, equipment, or system to gain information about its internal secrets or processes.
Electronic key entry	The entry of cryptographic keys into a cryptographic module using electronic methods such as a smart card or a key-loading device. (The user of the key may have no knowledge of the value of the key being entered.)
Encrypted key	A cryptographic key that has been encrypted using an Endorsed security function with a key encrypting key, a PIN, or a password in order to disguise the value of the underlying plaintext key.

Encryption algorithm	Algorithm of processing a plaintext into a ciphertext using a encryption key in a way that decoding of the cipher text into the plain text without knowledge of the corresponding decryption key is computationally infeasible.
Endorsed security function	For this security target, a security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either a) specified in an Endorsed standard, b) adopted in an Endorsed standard and specified either in an appendix of the Endorsed standard or in a document referenced by the Endorsed standard, or c) specified in the list of Endorsed security functions.
Environmental failure protection (EFP)	The use of features to protect against a compromise of the security of a cryptographic module due to environmental conditions or fluctuations outside of the module's normal operating range.
Environmental failure testing (EFT)	The use of testing to provide a reasonable assurance that the security of a cryptographic module will not be compromised by environmental conditions or fluctuations outside of the module's normal operating range.
Error mode	Mode of operation when the cryptographic module has encountered an error condition as defined in FPT_FLS.1 (term is used for description of the Mode transition SFP.
Error state	State related to the Error mode in the Finite state model (cf. ADV_ARC.1).
Firmware	The programs and data components of a cryptographic module that are stored in hardware (e.g., ROM, PROM, EPROM, EEPROM or FLASH) and cannot be dynamically written or modified during execution.
Hardware	The physical equipment used to process programs and data.
Input data	Information that is entered into a cryptographic module for the purposes of transformation or computation using an Endorsed security function.
Integrity	The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
Key encrypting key	A cryptographic key that is used for the encryption or decryption of other keys.
Key management	The activities involving the handling of cryptographic keys and other related security parameters (e.g., Ivs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and destruction.
Key material	Any media storing key components or keys for offline key exchange.
Key usage type	Type of cryptographic algorithm a key can be used for (e.g., DES encryption, TDES MAC calculation, signature-creation with RSA PKCS#1 v1.5).

Key-CSP entry mode	Mode of operation in which cryptographic keys and CSPs enter the cryptographic module.
Key-CSP entry state	State related to the Key-CSP entry mode in the Finite state model (cf. ADV_ARC.1).
Manual key entry	The entry of cryptographic keys into a cryptographic module, using devices such as a keyboard.
Manual key transport	Non-electronic means of transporting cryptographic keys.
Physical protection	The safeguarding of a cryptographic module, cryptographic keys, or CSPs using physical means.
Plaintext key	An unencrypted cryptographic key.
Port	A physical input or output interface of a cryptographic module that provides access to the module for physical signals, represented by logical information flows. Physically separated ports do not share the same physical pin or wire. In the CC terminology a port is a physical external interface of the TOE.
Private key	A cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public.
Protection Profile	An implementation-independent set of security requirements for a category of Targets of Evaluation (TOEs) that meet specific consumer needs.
Public key	A cryptographic key used with a public key cryptographic algorithm that is uniquely associated with an entity and that may be made public.
Public key (asymmetric) cryptographic algorithm	A cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that deriving the private key from the public key is computationally infeasible.
Reference authentication data	Data known for the claimed identity and used by the TOE to verify the verification authentication data provided by an entity in an authentication attempt to prove their identity.
Red data	Cryptographically unprotected user data representing user information which need protection in confidentiality and / or integrity.
Secret key	A cryptographic key, used with a secret key cryptographic algorithm, that is uniquely associated with one or more entities and should not be made public.
Secret key (symmetric) cryptographic algorithm	A cryptographic algorithm which keys for both encryption and decryption respective MAC calculation and MAC verification are the same of can easily be derived from each other and therefore must be kept secret.
HSM Admin	An authorized user who has been granted the authority to manage the TOE. These users are expected to use this authority only in the manner prescribed by the guidance given to them.

Self-test mode	Mode of operation in which the cryptographic module performs initial start-up self-test, self-test at power-up, self-test at the request of the authorised user and may perform other self-tests identified in FPT_TST.2.6.
Side Channel Analysis	Class of passive attacks exploiting the physical emanation of a device, equipment, or system in order to gain information about its internal secrets or processes.
Simple power analysis (SPA)	A direct analysis of patterns of instruction execution (or execution of individual instructions), obtained through monitoring the variations in electrical power consumption of a cryptographic module, for the purpose of revealing the features and implementations of cryptographic algorithms and subsequently the values of cryptographic keys.
Split knowledge	A process by which a cryptographic key is split into multiple key components, individually sharing no knowledge of the original key, that can be subsequently input into, or output from, a cryptographic module by separate entities and combined to recreate the original cryptographic key.
Tamper detection	The automatic determination by a cryptographic module that an attempt has been made to compromise the physical security of the module.
Tamper response	The automatic action taken by a cryptographic module when a tamper detection has occurred (the minimum response action is the desctruction of plaintext keys and CSPs).
Target of Evaluation (TOE)	An information technology product or system and associated administrator and user guidance documentation that is the subject of an evaluation.
Timing analysis	Analysis of timing behaviour of a device, equipment, or system to gain information about its internal secrets or processes.
TOE Security Functions (TSF)	A set of the TOE consisting of all hardware, software, and firmware that must be relied upon for the correct enforcement of the TOE Security Policy.
TOE security functions interface (TSFI)	A set of interfaces, whether interactive (man-machine interface) or machine (machine-machine interface), through which TOE resources are accessed, mediated by the TSF, or information is obtained from the TSF.
TOE Security Policy (TSP)	A set of rules that regulate how assets are managed, protected, and distributed within a Target of Evaluation.
Unauthenticated User	An identified user not being authenticated and having rights as identified in the component FIA_UAU.1.
Unauthorized user	A user who may obtain access only to system provided public objects if any exist.
Unidentified User	A user not being identified and having rights as identified in the component FIA_UID.1

List of Acronyms and Abbreviations

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CC	Common Criteria
CMAC	Cipher-based Message Authentication Code
CSP	Critical Security Parameter
CU	Crypto User
DPA	Differential Power Analysis
DRBG	Deterministic Random Number Generation
EAL	Evaluation Assurance Level
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EFT	Environmental Failure Testing
EMEA	Electromagnetic Emanation Analysis
ETH	Ethernet
FIPS	Federal Information Processing Standards
FPGA	Field Programmable Gate Array
HA	HSM Admin
HMAC	Hash-based Message Authentication Code
HSM	Hardware Security Module
IP	Intellectual Property
IT	Information Technology
LCD	Liquid Crystal Display
MAC	Message Authentication Code
NAND	Not And
NIST	National Institute of Standards and Technology
NOR	Not Or
OAEP	Optimal Asymmetric Encryption Padding
OS	Operating System
OSP	Organizational Security Policy
PHY	Physical Layer

PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PP	Protection Profile
QSPI	Quad Serial Peripheral Interface
RSA	Rivest Shamir Adleman
RTC	Real Time Clock
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SO	Security Officer
SOM	System on Module
SPA	Simple Power Analysis
SSL	Secure Sockets Layer
ST	Security Target
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
TOE	Target of Evaluation
TRNG	True Random Number Generation
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
USB	Universal Serial Bus

1. Introduction

1.1. References

1.1.1. ST Reference

Title	ProCrypt KM-3000 Hardware Security Module Security Target
Version	V1.0
Reference	KM3-ST-0014
Assurance Level	EAL 4 augmented with ADV_IMP.2, ALC_CMC.5, ALC_DVS.2, AVA_VAN.5 and ALC_FLR.2
CC Identification	• Common Criteria Part 1 Version 3.1 Revision 5 • Common Criteria Part 2 Version 3.1 Revision 5 • Common Criteria Part 3 Version 3.1 Revision 5 • Common Methodology for Information Technology Security Evaluation (CEM) Version 3.1 Revision 5

1.1.2. TOE Reference

Vendor Name	Procenne
TOE Name	ProCrypt KM-3000 Hardware Security Module
TOE Version	v1.0

1.1.3. Related Documents

[1] CCMB-2017-04-001, Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 5, April 2017

[2] CCMB-2017-04-002, Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 5, April 2017

[3] CCMB-2017-04-003, Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5, April 2017

[4] CCMB-2017-04-004, Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 5, April 2017

[5] BSI-CC-PP-0045, Cryptographic Modules, Security Level [Enhanced]; Version 1.01B, February 2009

[6] FIPS 180-4, Secure Hash Standard (SHS); August 2015

[7] FIPS 197, Advanced Encryption Standard(AES); November 2001

[8] FIPS 198-1, The Keyed-Hash Message Authentication Code (HMAC); July 2008

[9] FIPS 186-4, Digital Signature Standard (DSS); July 2013

[10] NIST SP 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation; Second Draft, January 2016

[11] NIST SP 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators; Revision 1, June 2015

[12] FIPS 186-4, Digital Signature Standard (DSS); July 2013

[13] NIST SP 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher; Revision 2, November 2017

[14] NIST SP 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography; Revision 2, May 2013

[15] NIST SP 800-38B, Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication; May 2005

[16] ANSI X9.62, PUBLIC KEY CRYPTOGRAPHY FOR THE FINANCIAL SERVICES INDUSTRY: THE ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM (ECDSA); 2005 Edition, November 2005

[17] PKCS #11, Cryptographic Token Interface Standard; Version 2.20, June 2004

[18] RFC 1321, The MD5 Message-Digest Algorithm; April 1992

1.2. TOE Overview

The TOE is a general purpose hardware security module (HSM) which provides cryptographic processing (encryption/decryption, signature generation/verification, message digest generation/verification, MAC generation/verification), key generation and key management services to connected host systems, which might be SSL/TLS web servers, application servers, authentication servers and other IT systems that need secure storage of cryptographic keys and secure use of cryptographic operations.

The TOE communicates with host systems through its network interface (100/1000 Base-T) and PKCS#11 protocol. This enables easy integration to either existing system environments or future projects, for wide range of applications. In addition to the ethernet interface, a smartcard interface (ISO7876) is also available for importing/exporting cryptographic keys and for user authentication using smartcards.

The TOE is physically defined as a set of hardware and firmware, which is contained within the cryptographic boundary. The TOE is in system on module (SOM) form with a card edge connection and it is typically located within a custom carrier/host system(non-TOE).

The TOE has a tamper resistant casing and constantly monitors against physical tamper attempts that including drilling, breaking or removing its casing. The whole module, except the card edge connection area, is covered by the mentioned tamper resistant casing and hard, opaque potting material (epoxy resin) is also used to fill the gap between the module electronics and the casing. Additionally, the TOE also monitors temperature and input voltage, to harden its tamper resistance capability. Optionally, the TOE can be configured to output a separate tamper trigger signal, which can be used to protect case of its carrier/host system, making it difficult to open its enclosure without detection. The TOE zeroizes plaintext key material and security parameters in case of a tamper event.

The TOE records audit logs for all operational events and security relevant events.

1.2.1. TOE Usage and Major Security Features

The TOE is designed to protect all cryptographic keys and security parameters against unauthorized access, unauthorized modification, disclosure and it is responsible to provide TOE services only to authorized operators.

The TOE is intended to be used in systems which need high level protection of cryptographic keys and security parameters, such as banking systems, certificate authorities, certification service providers, registration authorities and government systems.

The TOE provides the following major security features:

- User authentication feature to control and limit usage of cryptographic keys and parameters, TOE services and TOE management functions.
- Role based user management to control access and limit usage of cryptographic keys and parameters, TOE services and TOE management functions.
- Securing storage and management of cryptographic keys through their lifecycle; from generation to destruction.

- Cryptographic services such as symmetric/asymmetric key generation, data encryption/decryption, signature generation/verification and other cryptographic services which are described in the next sections.
- Auditing operational events and security relevant events.
- System start-up and on-demand self-test of all cryptographic functions provided by the TOE.
- Tamper protection against physical tamper attempts, in order to protect cryptographic keys and parameters from unauthorized access.

1.2.2. TOE Type

The TOE is a hardware security module(HSM), which provides secure cryptographic key management services and cryptographic functions.

1.2.3. Hardware, Firmware and/or Software Requirements

The TOE requires a control and management software to be installed on the host computer, in order to access to TOE and perform cryptographic operations through the network. In addition, the software is also required for pulling audit logs and performing firmware updates. The mentioned software, which is named "ProCryptManager Setup", is developed by Procenne and provided with the TOE.

Hardware and software requirements for "ProCryptManager Setup" are listed below:

- Operating System:
  - Microsoft Windows 7 or higher (x86 and x64).
  - Microsoft Windows Server 2012 or higher (x64).
  - Linux (x64)[1].
- Processor: 1.5 GHz, 2 cores or higher.
- Memory: 2 GB RAM for x86 systems, 4 GB RAM for x64 systems.
- HDD: 500 MB of free disk space.
- Network interface.

[1] Tested on RHEL 7.4, Ubuntu 16.04 and Debian 9.

1.3. TOE Description

1.3.1. Physical Scope of the TOE

The TOE is in system on module (SOM) form with a card edge connection and tamper resistive mesh layers on top and bottom. The gap between the electronic components and tamper resistant layers are filled with hard, opaque potting material (epoxy resin). Whole circuit area of the TOE, except the card edge connection, is the physical TOE boundary.

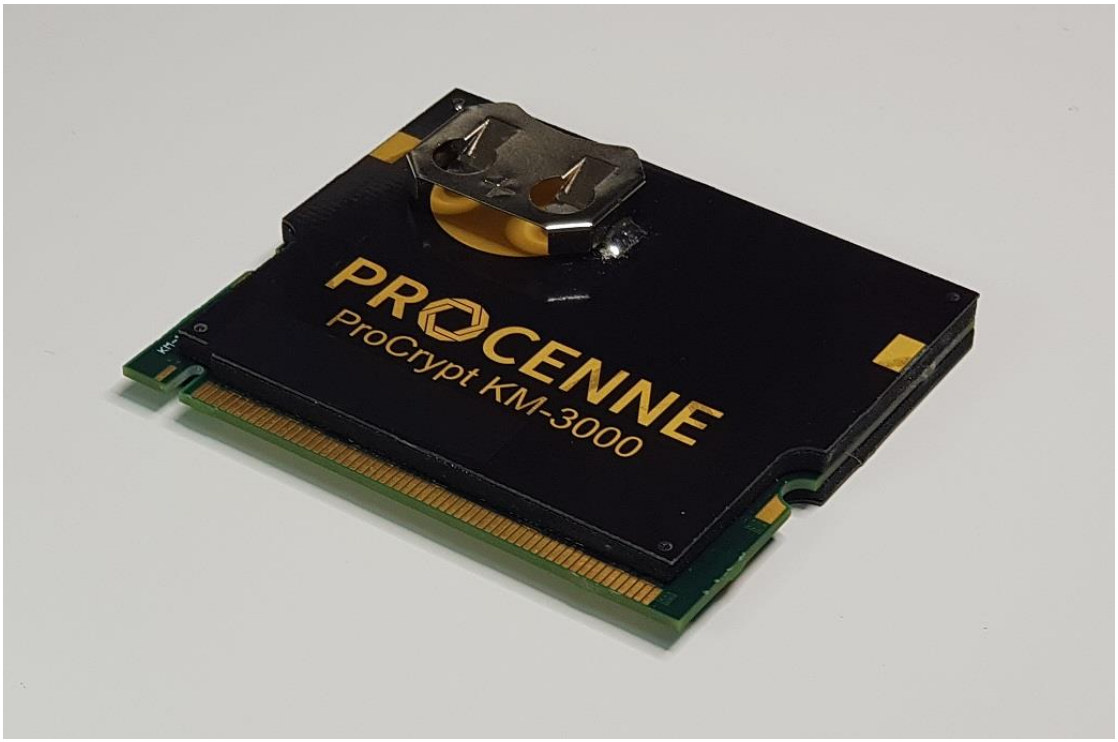


Figure 1: ProCrypt KM-3000 Module

The TOE has all necessary circuitry inside and is able to operate by itself. However, since it does not contain any connectors, a carrier board or a host system is needed to be able to make use of its electrical interfaces.

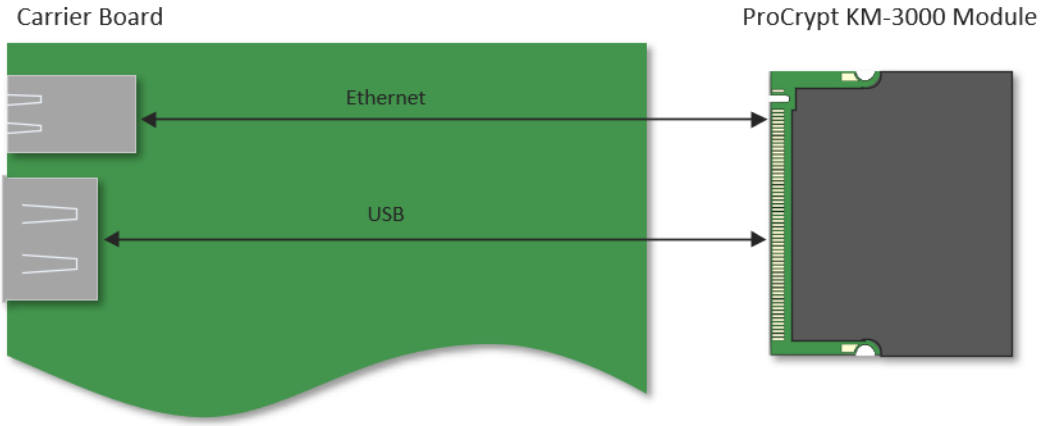


Figure 2: Carrier Board and TOE Interconnection

The figure below illustrates main hardware components of the TOE.

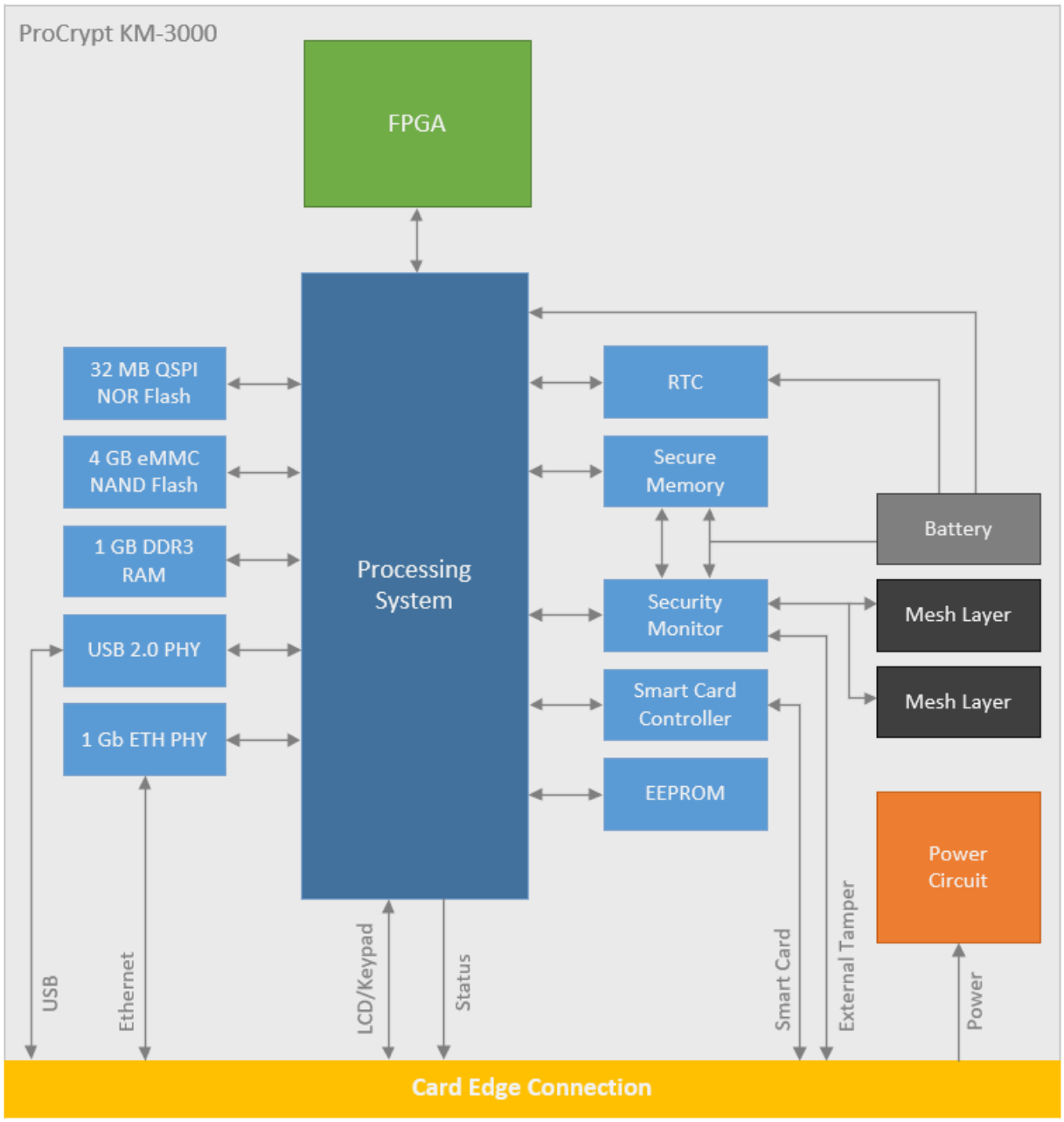


Figure 3: TOE Hardware Architecture

The following list describes the hardware components which are illustrated by the diagram above.

Component	Description
Processing System	Processing system is a microcontroller which consists of dual core CPUs (Central Processing Unit) and auxiliary units like memory interface units, storage elements and I/O peripherals. It runs main firmware of the TOE and is responsible of management of all other hardware components. In addition, the processing

Component	Description
	system has a key memory to store firmware encryption key which is backed by the battery.
FPGA	FPGA hosts cryptographic IP cores which are used to accelerate cryptographic operations.
QSPI NOR Flash	NOR Flash is used to store bootloader files in addition to some system configuration files which are needed on system startup.
eMMC NAND Flash	It is used to store filesystem of the operating system(OS). All cryptographic keys, key components and CSPs are encrypted using master key and also stored in the NAND memory.
USB 2.0 PHY	It is a physical layer interface component which generates USB 2.0 compliant electrical interface, in order to enable the processing system to communicate with USB devices.
1 Gb ETH PHY	It is a physical layer interface component which enables the processing system to communicate over computer networks.
RTC	Real time clock component is used to provide date/time information to the system. It is battery backed to retain data/time information when system power is lost.
Secure Memory	Secure memory is used to store master key of the device. It is battery backed to retain its content when system power is lost. It is able to rapidly destroy stored key data when tamper alarm signal is received by the security monitor.
Security Monitor	It constantly monitors the mesh layers and makes sure that they are physically intact. It also monitors module temperature and voltage supply inputs to detect abnormal events. In case of tamper event detection, it broadcasts an alarm signal. It is battery backed and continues its operation when system power is lost.
Smart Card Controller	It is an interface component that enables the processing system to communicate with smart cards.
EEPROM	It stores constant and unique module identification data which are set during manufacturing.
Battery	It is used to provide power to volatile memory components and security monitor, when system power is not present.
Mesh Layer	It provides protection against possible electrical and mechanical attacks. It covers the whole module electronics and enables the module to detect physical damage.
Power Circuit	It consists of several power regulators, power supervisor circuits and auxiliary components that regulate and monitor the power rails.

Table 1: Descriptions of some of the TOE's Hardware Components

Software and IP components of the TOE are listed below:

- Processing System Bootloader
- Operating System
- Device Drivers
- Firmware Packages
- FPGA IP Cores
- Secure SoC Bootloader
- Secure SoC Firmware

The TOE uses a Linux based operating system running on the processing system. The operating system just provides an environment for the firmware packages to run and it does not play a direct role at meeting security functional requirements.

The device drivers are mainly developed for interfacing the IP cores, which are hosted on the FPGA portion of the TOE. Their primary objective is to provide an abstraction layer between the devices and the firmware packages.

The TOE can be delivered to the customer either as a standalone hardware module or as a part of Procenne's carrier appliance. In both cases, it is delivered within a sealed box, using tamper evident labels, which enables the customer to see if the box is opened by someone else before.

Figure 4: ProCrypt KM-3000 Appliance

The TOE consists of the following components:

- ProCrypt KM-3000 Module
  - Hardware Version: 1.0.0
  - Operating System Version: 1.0.0
  - FPGA Suite Version: 1.0.0
  - Firmware Suite Version: 1.0.0
  - Documentation: ProCrypt KM-3000 Cryptographic Module User Guide Document v1.0.0

1.3.2. Logical Scope of the TOE

There are several firmware packages running on both the Processing System and the Secure SoC. The firmware packages on the Processing System perform main tasks of the TOE and they are responsible for managing life cycle of the TOE, parsing input messages to perform requested tasks and generating response messages, driving user interface peripherals (front panel LCD display, status LEDs, smartcard interface), generating audit logs and managing all hardware units existing in the system. The IP cores on the FPGA, the soft crypto cores and the Secure SoC are

driven by the mentioned firmware packages, in order to perform TOE security functions, which are listed in the table below.

The firmware running on the Secure SoC waits for Processing System to send command messages, performs requested tasks related to the Secure Memory, Security Monitor and Smart Card Controller, and generates response messages. The firmware plays a passive role and is controlled by the Processing System except for destroying Secure Memory content in case of tamper event detection. The firmware immediately zeroes the Secure Memory, then informs the Processing System, if the system is powered up, in such case. It is the only task the Secure SoC performs without receiving a request from the Processing System.

Security functions of the TOE are overviewed in the table below.

Security Function	Description
User Authentication	The TOE provides user authentication functionality.
Access Control	The TOE provides pre-defined user roles and each user role has access to certain TOE functionality. User roles and their access rights are described in the next sections.
Secure Key Management	The TOE provides functionality to securely generate, store, exchange, use and destroy cryptographic keys for supported cryptographic functions.
Cryptographic Services	The TOE provides access to several cryptographic algorithms such as asymmetric and symmetric encryption algorithms, hash algorithms, key generation algorithms and signature generation and verification algorithms. A full list of the supported cryptographic algorithms is provided in the next sections.
Auditing	The TOE has a logging mechanism to record significant events along with date/time information and status code.
Self-Test	The TOE performs various self-tests on system start up and provides the ability to re-run the same tests on user request. The self-tests are performed to verify functionality of the TOE's hardware components, cryptographic IP cores and soft cores and integrity of the firmware packages and other software.
Tamper Detection	The TOE has tamper detection mechanisms and it is designed to destroy content of its secure memory in case of tamper detection. The tamper detection mechanisms are battery backed and continues to operate when the system power is lost.

Table 2: Security Functions of the TOE

1.3.2.1. TOE Roles

The user roles supported by the TOE are listed and described in the table below.

User Role	Description	Rights
HSM Admin (HA)	An authorized user who has been granted the authority to manage the Crypto Module. These users are expected to use this authority only in the manner prescribed by the guidance given to them. The Crypto Module can only have one PO.	• Update the HSM software components. • Change Security Mode. • View Audit Logs • Tamper HSM. • Setting Up HSM Clock • HSM IP & Port Configurations • Other tasks that Unidentified and Unauthenticated Users are authorized to do.

HSM Operator (HO)	An authorized user who has been granted the authority to manage the Crypto Module. These users are expected to use this authority only in the manner prescribed by the guidance given to them. The Crypto Module can only have one PO.	• Create partitions.
		  ○ Create SO users and assign to partitions.
		  ○ Create CU user.
		  ○ Delete users.
		• Delete partitions.
		• Reset HSM.
		• Other tasks that Unidentified and Unauthenticated Users are authorized to do.

Security Officer (SO)	An authorized user who has been granted the authority to perform cryptographic initialization and management functions. These users are expected to use this authority only in the manner prescribed by the guidance given to them. A CO user can be created and assigned to a partition by the SO user. A partition can only have one CO user.	• Personalize the partition. • Depersonalize the partition. • Manage (generate, use, backup/restore, export, destroy) cryptographic objects. • Other tasks that CU, Unidentified and Unauthenticated Users are authorized to do.
Crypto User (CU)	An authorized user assumed to perform general security services, including cryptographic operations and other Endorsed security functions. A CU user can be created and assigned to a partition by the SO or CO users. A partition can only have one CU user.	• Use cryptographic objects. • Manage (generate, use, backup/restore, export, destroy) cryptographic objects. • Other tasks that Unidentified and Unauthenticated Users are authorized to do.
Unidentified User	A user not being identified.	• Identified in the FIA_UID.1 component.

Unauthenticated User	An identified user not being authenticated.	• Identified in the FIA_UAU.1 component.

Table 3: TOE Roles

The term "user" is used to include both authorized and unauthorized users. Authorized users are known to the TOE and their security attributes are maintained by the TOE as prerequisite for their identification and authentication. Unauthorized users are unknown to the TOE. An authenticated authorized user is an authorized user that has been successfully authenticated for one or more of the following roles: HSM Admin role, HSM Operator role, Security Officer role, Crypto User role.

A user in the Crypto User role may be a human user or an IT system communicating with the TOE.

The TOE maintains at least the following security attributes of authorized users:

1. Identity that identify uniquely the user,
2. Role for which the user is authorized,

And TSF data

3. Reference Authentication Data for users.

The TOE maintains at least the following security attributes of subjects:

1. Identity of the user bind to this subject,
2. Role for which this user is currently authenticated,

1.3.2.2. Cryptographic Services

Primary security functions supported by the TOE are listed below.

- Random Number Generation
- Symmetric and Asymmetric Key Generation
- Data Encryption/Decryption
- Digital Signature Generation and Verification
- Key Backup/Restore
- Message Digest (Hash) Generation and Verification
- MAC Generation and Verification

2. Conformance Claim

2.1. CC Conformance Claim

This ST claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 5 [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 5 [2], Extended
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5 [3], Conformant

The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 5 [4]

has to be taken into account.

2.2. PP Claim

While this ST does not claim conformance to any protection profile, it has been developed to be consistent with the Cryptographic Modules, Security Level [Enhanced] (Ref. [5]) with the following amendments:

- The user role names "Administrator" and "End-User" in the PP, have been renamed and used as "HSM Admin" and "Crypto User".
- ALC_FLR.2 component is added as an additional augmentation to EAL4.
- FAU_STG.4 component is removed.
- Maintenance Mode and Maintenance Role references have been removed.
- OSP.Access, OSP.Resist_High, OSP.Account, OSP.Roles and OSP.I&A policies are removed since the requirements of these policies are already met by the TOE.

2.3. Package Claim

Evaluation Assurance Level is EAL4, augmented with (EAL4+):

- ADV_IMP.2
- ALC_CMC.5
- ALC_DVS.2
- AVA_VAN.5
- ALC_FLR.2

3. Security Problem Definition

3.1. Introduction

The nature of the security problem that the TOE is designed to address is described in this section. The security problem is described through threats, organizational security policies and assumptions, after the introductory information is provided.

3.1.1. Assets

The cryptographic module is intended to protect primary assets:

1. Plaintext data containing information, which need protection in confidentiality.
2. Original data containing information, which need protection in integrity or a proof of origin and authenticity to third parties.

User data requires protection in confidentiality and integrity i.e. they may be original plaintext data.

The use of cryptographic algorithms and protocols requires the protection of the cryptographic keys as secondary assets. The cryptographic keys need protection as the primary assets they protect and depending on the cryptographic technique they are used for:

3. Secret keys of symmetric cryptographic algorithms and protocols need protection in confidentiality and integrity.
4. Private keys of asymmetric cryptographic algorithms and protocols need protection in confidentiality and integrity.
5. Public keys of asymmetric cryptographic algorithms and protocols need protection in integrity and authenticity.

Where the need of confidentiality of secret and private keys follows directly from the cryptographic technique the integrity protection for these keys prevents indirect attacks (e.g., substitution of an unknown secret key by a known key compromise the subsequent encryption of plaintext data, an undetected modification of a private key may enable attacks against this key).

The CC deals with cryptographic keys as user data and as TSF data depending on their specific use by the TSF. Cryptographic keys are user data in the terminology of CC if they are used to protect cryptographically the confidentiality or integrity of data provided by the IT system "cryptographically unprotected data" or to transform "black data" into "cryptographically unprotected data" by cryptographic functions. Encryption and decryption keys are examples of such keys. Cryptographic keys are TSF data in the terminology of CC if their information is used by the TSF in making TSP decisions. Root public keys are examples of cryptographic keys as TSF because they are used to verify the authenticity of all other public keys of the public key infrastructure, which may be provided by any user. Public keys may be used as authentication reference data for external entities as user of the TOE.

3.1.2. Subjects

The user roles supported by the TOE are:

- HSM Admin
- HSM Operator
- Security Officer
- Crypto User
- Unidentified User
- Unauthenticated User

The user roles listed above are described in the TOE Roles section.

3.1.3. Objects

The data elements protected by the TOE are listed and described in the table below.

Data Elements	Description
Plaintext Data	User data encoded in an public known way which will be transformed by an encryption algorithm into ciphertext data (i.e. plaintext input data) or which is the result of decryption of the corresponding ciphertext data (i.e. plaintext output data). Plaintext data contain confidential information.
Ciphertext Data	User data as result of the application of an encryption algorithm to plaintext data and an encryption key. The knowledge of ciphertext data by an attacker does not compromise the confidential information represented by the corresponding plaintext.
Original Data	User data for which a digital signature or a message authentication code is calculated or verified. Original data contain integrity sensitive information.
Cryptographic Keys	Parameters used in conjunction with a cryptographic algorithm that determines the transformation of plaintext data into ciphertext data, the transformation of ciphertext data into plaintext data, a digital signature computed from data, the verification of a digital signature computed from data, a message authentication code computed from data, a proof of the knowledge of a secret, a verification of the knowledge of a secret or an exchange agreement of a shared secret.
Cryptographic Key Component	Parameters used in split knowledge procedures for manual key export methods and manual key import methods.
Critical Security Parameters	Security-related information (e.g., secret and private cryptographic keys, and TSF data like authentication data) whose disclosure or modification can compromise the security of a cryptographic module.

Data Elements	Description
Digital Signature	The result of an (asymmetric) signature-creation algorithm applied to the original data using a signature-creation key. The digital signature may contain or be appended to the original data.
Message Authentication Code	The result of a (symmetric) message authentication algorithm applied to the original data using a message authentication key. The MAC will be appended to the original data.

Table 4: Data Elements Protected by the TOE

Critical security parameters (CSP) have at least the security attributes

1. Identity of the CSP that uniquely identify the CSP,
2. CSP usage type identifying the purpose and methods of use of the CSP,
3. CSP access control rules.

The CSP access control rules may restrict the access for operation like import or export of the key.

Cryptographic keys have at least the security attributes

1. Identity of the key that uniquely identify the key,
2. Key entity, i.e. the identity of the entity this key is assigned to,
3. Key type, i.e. secret key, private key, public key,
4. Key usage type, i.e. the cryptographic algorithms a key can be used for,
5. Key access control rules, and
6. Key validity time period, i.e. the time period for operational use of the key.

The security attribute "key usage type" shall identify the cryptographic algorithm the key is intended to be used and may contain information about rang of this key in a key hierarchy, and other information. The security attribute "Key access control rules" restricts the access for operation like import or export of the key. The security attribute "key validity time period" restricts the time of operational use of the key; the key must not be used before or after this time slot.

Cryptographic key components have at least the security attributes

1. Identity of the key component that uniquely identify the key component,
2. Key entity, i.e. the identity of the key the key component belongs to,
3. Key entry method, i.e. the method the key component is used for

3.1.4. Services

Service	Description
Decryption	Processes a decryption algorithm to the ciphertext data using the decryption key and returns the corresponding plaintext data.
Encryption	Processes a encryption algorithm to the plaintext data using the encryption key and returns the corresponding ciphertext data.
Export of Key	Output of cryptographic keys in protected form.

Service	Description
Export of Protected Data	Output of user data with or without security attributes to the black area of the IT system protected in confidentiality or integrity or both by cryptographic security functions of the TOE.
Export of Unprotected Data	Output of user data with or without security attributes to the red area of the IT system cryptographically unprotected by cryptographic security functions of the TOE.
Import of Key	Input of cryptographic keys in protected form.
Import of Protected Data	Input of user data with or without security attributes from the black area of the IT system where the cryptographic security functions of the TOE support the protected in confidentiality by decryption or in integrity by detection modification or verification of data origin.
Import of Unprotected Data	Input of user data with or without security attributes to the red area of the IT system cryptographically unprotected by cryptographic security functions of the TOE.
Message Digest Calculation	Processes a hash algorithm to the original data and returns the corresponding Message Digest.
Message Digest Verification	Processes a hash algorithm to the presented user data and Message Digest and returns the result of checking whether the user data and the Message Digest fit together (integrity confirmed) or not (integrity not confirmed).
MAC Calculation	Processes a (symmetric) MAC algorithm to the original data using the secret message authentication key and returns the corresponding Message Authentication Code.
MAC Verification	Processes a (symmetric) MAC algorithm to the presented user data and MAC using the secret message authentication key and returns the result of checking whether the user data, the MAC and the key fit together (integrity confirmed) or not (integrity not confirmed).
Signature Creation	Processes a (asymmetric) signature-creation algorithm to the original data using the private signature-creation key of the signatory and returns the corresponding digital signature.
Signature Verification	Processes a (asymmetric) signature-verification algorithm to the signed data and the digital signature using the public key and returns the result of checking whether the original data, the electronic signature and the public key fit together (integrity confirmed) or not (integrity not confirmed).
Use of Key	Use of the cryptographic key by a cryptographic algorithm as key parameter.

Table 5: TOE Services

3.2. Threats

3.2.1. T.Compro_CSP - Compromise of Confidential CSP

An attacker with high attack potential may compromise confidential CSP like secret keys, private keys or confidential authentication data by trying to use this data with unintended cryptographic functions, unauthorizedly accessing this data using TOE services, using cryptographically insecure keys for export/import operations or using possible information leakage from physical or logical channels; which enables attacks against the confidentiality or integrity of user data protected by these CSPs or the TSF using these CSPs as TSF data.

3.2.2. T.Modif_CSP - Modification of Integrity Sensitive CSP

An attacker with high attack potential may modify integrity sensitive CSP like permanent stored public keys by unauthorizedly accessing this data using TOE services or altering data during key export and key import and therefore compromise the confidentiality or integrity of user data protected by these CSPs or the TSF using these CSPs as TSF data.

3.2.3. T.Abuse_Func - Abuse of Function

An attacker with high attack potential may use TOE functions intended for installation or configuration of the TOE which shall not be used for operational cryptographic keys or user data in order (i) to disclose or manipulate operational CSP or user data, or (ii) to enable attacks against the integrity or confidentiality of operational CSP or user data by (iia) manipulating (explore, bypass, deactivate or change) security features or functions of the TOE or (iib) disclosing or manipulating TSF Data.

3.2.4. T.Inf_Leakage - Information Leakage

An attacker with high attack potential may observe and analyze any energy consumed or emitted through the cryptographic boundary (i.e. including the external interfaces) of the TOE to get internal secrets (especially secret or private cryptographic keys) or confidential user data not intended for export. The information leakage may be inherent in the normal operation or caused by the attacker.

3.2.5. T.Malfunction - Malfunction of TSF

An attacker with high attack potential may use a malfunction of the hardware or software, which is accidental or deliberated by applying environmental stress or perturbation, in order to deactivate, modify, or circumvent security functions of the TOE to enable attacks against the integrity or confidentiality of the User data or the CSP.

3.2.6. T.Physical_Tamper - Physical Tampering

An attacker with high attack potential may tamper the cryptographic module to get secrets, to modify data on whose integrity the TSF relies, or to corrupt or de-activate the TSF inside the cryptographic boundary to violate the integrity or confidentiality of the User data, the CSP or the TSF data.

3.2.7. T.Masquerade - Masquerade Authorized Data Source or Receiver

An attacker with high attack potential may masquerade as an authorized data source or receiver to perform operations that will be attributed to the authorized user or may gain undetected access to cryptographic module causing potential violations of integrity or confidentiality of the User data, the CSP or the TSF data.

3.3. Organizational Security Policies

3.3.1. OSP.User_Data_Prot - Protection of User Data by Cryptographic Functions

The cryptographic module will be used to protect the confidentiality or integrity or both of information represented by user data which may be get known or modified by an attacker. The IT system will ensure the availability of the user data and the cryptographic keys outside the cryptographic module.

3.3.2. OSP.Endorsed_Crypto - Endorsed Cryptographic Functions

The TOE shall implement Endorsed cryptographic algorithms and Endorsed cryptographic protocols for the protection of the confidentiality or the integrity or both of the user data according to the organizational security policy OSP.User_Data_Prot and for the cryptographic key management according to the organizational security policy OSP.Key_Man. The cryptographic module must not provide any non-Endorsed cryptographic function.

3.3.3. OSP.Key_Man - Cryptographic Key Management

The CSP, cryptographic keys and cryptographic key components are assigned to cryptographic algorithms and protocols they are intended to be used with and the entities, which are allowed to use them.

3.3.4. OSP.Key_Personal - Personal Security for Cryptographic Keys

The cryptographic keys shall be managed in such a way that their integrity and confidentiality cannot be compromised by a single person.

3.4. Assumptions

3.4.1. A.User_Data - Protection of User Data by the IT System

The TOE environment uses the TOE for cryptographic protection of user data for transmission over channels or storage in media, which are not protected against access by unauthorised users. The TOE environment provides cryptographically unprotected user data to the TOE and identifies protection in confidentiality or integrity or both to be provided by the TOE.

3.4.2. A.Data_Sep - Separation of Cryptographically Protected and Unprotected Data

The TOE environment separates the cryptographically unprotected data from the cryptographically protected user data in the IT system

3.4.3. A.Key_Generation - Key Generation and Import to the Cryptographic Module

Cryptographic keys generated by the IT environment and imported into the TOE are cryptographically strong for the intended key usage and have secure security attributes.

3.4.4. A.Audit_Analysis - Analysis of Audit Trails

The TOE environment retrieves the audit records of the TOE and analyses them for security violations.

3.4.5. A.Availability - Availability of Keys

The TOE environment ensures the availability of cryptographic keys, key components, CSP and key material.

3.4.6. A.Environmental_Security – Environmental Security of systems accessing TOE interfaces

Environmental security of the systems to access TOE ensures protection against malicious software, malicious human/users and malicious usage of TOE access modules. These TOE access modules can be ProCrypt Manager, ProCrypt Key Manager and procryptoki library.

4. Security Objectives

4.1. Security Objectives for the TOE

4.1.1. O.Red-Black-Sep - Red-Black Separation of the TOE

The TOE shall protect confidential information for export into the black area by encryption of plaintext data and for import into the red area by decryption of ciphertext data. The TOE shall protect integrity sensitive information for export into the black area by calculation of MAC or digital signature on the red data and for import into the red area by verification of MAC or digital signature on black data. The TOE shall separate logical interfaces for red user data, black user data, CSP (including plaintext cryptographic keys and key components) and administrative functions.

4.1.2. O.Endorsed_Crypto - Endorsed Cryptographic Functions

The TOE shall provide Endorsed cryptographic functions and Endorsed cryptographic protocols to protect the user data as required by OSP.User_Data_Prot and for key management.

4.1.3. O.I&A - Identification and Authentication of Users

The TOE shall uniquely identify users and verify the claimed identity of the user before providing access to any controlled resources with the exception of read access to public objects. The security functions for authentication of users shall have strength “high”.

4.1.4. O.Roles - Roles Known to TOE

The TOE shall provide at least the HSM Admin, the HSM Operator, the Security Officer, the Crypto User user roles.

4.1.5. O.Control_Services - Access Control for Services

The TOE shall restrict the access to its services, depending on the user role, to those services explicitly assigned to this role. Assignment of services to roles shall be either done by explicit action of a HSM Admin or by default.

4.1.6. O.Control_Keys - Access Control for Cryptographic Keys

The TOE shall restrict the access to the keys, key components and other CSP according to their security attributes. Cryptographic keys intended for the use with Endorsed cryptographic functions must not be used by any non-endorsed functions.

4.1.7. O.Audit - Audit of the TOE

The TOE shall provide the capability to detect and create audit records of security relevant events associated with users.

4.1.8. O.Key_Export - Export of Cryptographic Keys

The TOE shall export cryptographic keys with their security attributes. The cryptographic keys and their security attributes shall be protected in integrity. The TOE shall ensure the confidentiality of secret and private keys exporting them in encrypted form to authorized entities or manually using split knowledge procedures only.

4.1.9. O.Key_Generation - Generation of Cryptographic Keys by the TOE

The TOE shall generate cryptographic strong keys using Endorsed cryptographic key generation algorithms.

4.1.10. O.Key_Import - Import of Cryptographic Keys

The TOE shall import keys with security attributes and verify their integrity. The TOE shall import secret or private keys in encrypted form or manually using split knowledge procedures only.

4.1.11. O.Key_Management - Management of Cryptographic Keys

The TOE shall securely manage cryptographic keys, cryptographic key components and CSP. The TOE shall associate security attributes of the entity the key is assigned to and of the intended cryptographic use of the key. Assignment of the security attributes to the cryptographic keys, cryptographic key components and CSP shall be either done by explicit action of a Security Officer or by default.

4.1.12. O.Key_Destruction - Destruction of Cryptographic Keys

The TOE shall destruct in a secure way the keys cryptographic key components and other CSP on demand of authorized users or when they will not be used any more that no information about these keys is left in the resources storing or handling these objects before destruction.

4.1.13. O.Check_Operation - Check for Correct Operation

The TOE shall perform regular checks to verify that its components operate correctly. This includes integrity checks of TOE software, firmware, internal TSF data and keys during initial start-up, at the request of the authorized user, and at the installation condition.

4.1.14. O.Physical_Protect - Physical Protection

The TOE shall resist physical attacks with high attack potential.

4.1.15. O.Prevent_Inf_Leakage - Prevent Leakage of Confidential Information

The TOE shall prevent information leakage about secret and private keys and confidential TSF data outside the cryptographic boundary and unintended output confidential user information. The TOE shall resist attacks with high attack potential, which are based on information leakage and that can be performed from outside the secure environment.

4.2. Security Objectives for the Operational Environment

4.2.1. OE.Assurance - Assurance Security Measures in Development and Manufacturing Environment

The developer and manufacture ensure that the TOE is designed and fabricated so that it requires a combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through attack. The developer provides necessary evaluation evidence that the TOE fulfils its security objectives and is resistant against attack with high attack potential.

4.2.2. OE.Key_Generation - Key Generation by IT Environment

The IT environment shall ensure the cryptographic strength, the confidentiality and integrity of secret and private keys, the integrity and authenticity of public keys and correct security attributes if they are generated outside the TOE and imported into the TOE.

4.2.3. OE.Red-Black-Sep - Separation of Red and Black Area of the IT System

The TOE environment protects the user data in the red area of the IT system and controls the exchange data between the red and black area of the IT system according to the IT security policy. It provides the red user data with their security attributes for cryptographic protection to the TOE and receives red user data with their security attributes from the TOE.

4.2.4. OE.Audit_Analysis - Analysis of TOE Audit Data

The TOE environment reviews the audit trails generated and exported from the TOE to detect security violation and making authenticated users accountable for their actions related to the TOE. The administrator is responsible for configuration of the audit function and provision of the complete chain of exported audit trails.

4.2.5. OE.Personal - Personal Security

The HSM Admin, Security Officer, Crypto User and HSM Operator roles shall be assigned with distinct authorized persons.

4.2.6. OE.Key_Availability - Availability of Cryptographic Key and Key Material

The IT environment shall ensure the availability of the user data, cryptographic keys key components, CSP and key material.

4.3. Security Objectives Rationale

The following table provides an overview for security objectives coverage.

	OSP.User_Data_Prot	OSP.Endorsed_Crypto	OSP.Key_Man	OSP.Key_Personal	T. Compro_CSP	T.Modif_CSP	T.Abuse_Func	T.Physical_Tamper	T.Inf_Leakage	T.Malfunction	T.Masquerade	A.User_Data	A.Data_Sep	A.Key_Generation	A.Audit_Analysis	A.Availability	A.Environmental_Sec
O.I&A				■							■						
O.Control_Services							■										
O.Control_Keys				■	■	■					■						
O.Roles							■										
O.Audit						■	■										
O.Key_Export			■	■	■	■											
O.Key_Generation			■		■												
O.Key_Import			■	■	■	■											
O.Key_Management			■	■	■	■											
O.Key_Destruction			■		■												
O.Red-Black-Sep					■						■						
O.Check_Operation						■				■							
O.Endorsed_Crypto	■	■															
O.Physical_Protect								■									
O.Prevent_Inf_Leakage					■				■								
OE.Assurance								■									
OE.Key_Generation			■		■									■			
OE.Red-Black-Sep												■	■				■
OE.Audit_Analysis															■		
OE.Personal				■			■										■
OE.Key_Availability	■															■	

Table 6: Security Objectives Rationale

The organisational security policy **OSP.User_Data_Prot** "Protection of user data by cryptographic functions" addresses the protection of the confidentiality or integrity or both of information represented by user data of the IT-system to be provided by the cryptographic module and the protection of availability of user data by the IT system. The security objective O.Endorsed_Crypto ensures that TOE provides Endorsed cryptographic functions to protect the

user data as required by OSP.User_Data_Prot. The security objective for the IT environment OE.Key_Availability ensures that IT system protects the availability of the user data and the cryptographic keys outside the cryptographic module.

The organisational security policy **OSP.Endorsed_Crypto** "Endorsed cryptographic functions" address the implementation of Endorsed cryptographic algorithms and Endorsed cryptographic protocols for the protection of the confidentiality or the integrity or both of the user data according to the organizational security policy OSP.User_Data_Prot and for the key management. This is ensured generally by the security objective O.Endorsed_Crypto.

The security objective **OSP.Key_Man** "Cryptographic key management" requires to manage and use the cryptographic keys as they are assigned to the entities, cryptographic algorithms and protocols. This OSP is implemented generally by the security objectives for the TOE O.Key_Management for secure key management and specifically for critical processes over the key life cycle by the security objectives O.Key_Generation, O.Key_Import, O.Key_Export and O.Key_Destruction. OE.Key_Generation ensures the cryptographic strength, the confidentiality and integrity of secret and private keys, the integrity and authenticity of public keys and correct security attributes if they are generated outside the TOE and imported into the TOE.

The organisational security policy **OSP.Key_Personal** "Personal security for cryptographic keys" addresses key management in a way that the integrity and confidentiality of key can not be compromised by a single person. This OSP is implemented generally by the security objectives O.Key_Management and O.Control_Keys for secure key management and use. Furthermore for critical processes, the security objectives O.Key_Import, O.Key_Export and O.Control_Keys enforce secure key import, key export and key usage. O.I&A ensures that the TOE uniquely identifies users and verifies the claimed identity of the user before providing access. OE.Personal requires assignment of roles to distinct authorized persons and that for manual key import at least two different authorized persons are assigned to cryptographic administrator role.

The threat **T.Compro_CSP** "Compromise of CSP" addresses the compromise confidential CSP which enables attacks against the confidentiality or integrity of user data and TSF data protected by these CSPs. The security objective O.Control_Keys requires the TOE to restrict the access to the keys, key components and CSP according to their security attributes. The security objective O.Key_Management ensures these security attributes are managed securely. The security objective O.Key_Export and O.Key_Import require the protection of secret or private keys in encrypted form or using split knowledge procedures for their export and import. The security objectives O.Key_Generation requires the TOE and the OE.Key_Generation requires the environment to generate cryptographic strong keys. O.Key_Destruction requires the secure destruction on demand of user. The security objective O.Red-Black-Sep requires protecting the confidentiality of CSP by logical separation of interfaces for CSP from other interfaces. The security objective O.Prevent_Inf_Leakage requires the TOE to prevent information leakage about secret and private keys and confidential TSF data outside the cryptographic boundary.

The threat **T.Modif_CSP** "Modification of integrity sensitive CSP" address the modification of the integrity sensitive CSP which enables attacks against the confidentiality or integrity of user data or the TSF protected by these CSPs . The security objective O.Control_Keys requires the TOE to restrict the access to the keys, key components and CSP according to their security attributes. The security objective O.Key_Management ensures these security attributes are managed securely. The security objective O.Key_Export and O.Key_Import require the protection of the integrity keys during their export and import. The security objective O.Check_Operation requires verification the integrity of CSP. The security objective O.Audit requires logging all CSP related actions to audit trail.

The threat **T.Abuse_Func** "Abuse of function" addresses the misuse of TOE functions intended for installation or configuration which shall not be used for operational cryptographic keys or user data. This is ensured by the security objective O.Control_Services that restricts the access to TOE services, depending on the user role, to those services explicitly assigned to this role. The security objective O.Roles requires the TOE to provide at least the HSM Admin, the Security Officer, the Crypto User, the HSM Operator roles. The HSM Admin, Security Officer, Crypto User and HSM Operator roles will be assigned to authorized distinct persons according to the security objective for the IT environment OE.Personal. The security objective O.Audit requires logging all user related actions to audit trail.

The threat **T.Inf_Leakage** "Information leakage" describes that an attacker may observe and analyze any energy consumed or emitted through the cryptographic boundary (i.e. including the external interfaces) of the TOE to get internal secrets or confidential user data not intended for export. The protection against this threat is directly required by the security objective O.Prevent_Inf_Leakage.

The threat **T.Malfunction** "Malfunction of TSF" describes the use of a malfunction of the hardware or software in order to deactivate, modify, or circumvent security functions of the TOE to enable attacks against the integrity or confidentiality of the User data or the CSP. The security objective O.Check_Operation prevents this threat by regular checks verifying that TOE components operate correctly.

The threat **T.Physical_Tamper** "Physical tampering" describes tampering the cryptographic module to get secrets, to modify data on whose integrity the TSF relies, or to corrupt or deactivate the TSF inside the cryptographic boundary, which is directly addressed by the security objective O.Physical_Protect and OE.Assurance.

The threat **T.Masquerade** "Masquerade authorized data source or receiver" describes that an attacker may masquerade as an authorized data source or receiver to perform operations that will be attributed to the authorized user or gains undetected access to cryptographic module causing potential violations of integrity, or confidentiality. The security objective O.I&A requires the TOE to identify and authenticate the user before providing access to any controlled resources with the exception of public objects. The security objective O.I&A requires the security functions for authentication of users to have strength "high" to cover attacks with high attack potential as described in T.Masquerade. The security objective O.Control_Keys restricts the access to the keys, key components and other CSP according to their security attributes (including Key entity). Furthermore the security objective O.Red-Black-Sep requires the TOE to protect integrity sensitive information by verification of black data for import into the red area.

The assumptions **A.User_Data** "Protection of user data by the IT system" and A.Data_Sep "Separation of cryptographically protected and unprotected data " are covered by the security objective for the IT environment OE.Red-Black-Sep "Separation of red and black area of the IT system" dealing with protection of the user data in the red area of the IT system, their security attributes for cryptographic protection to the TOE and the control the exchange data between the red and black area of the IT system according to the IT security policy.

The assumption **A.Data_Sep** "Separation of Cryptographically Protected and Unprotected Data" describes that the IT environment ensures the separation of cryptographically unprotected data from the cryptographically protected user data as ensured by the security objective for the IT environment OE.Red-Black-Sep.

The assumption **A.Key_Generation** "Key generation and import to the cryptographic module" deals with the cryptographic strength and secure security attributes of cryptographic keys

generated by the IT environment and imported into the TOE. This assumption is directly and completely covered by the security objective for the IT environment OE.Key_Generation.

The assumption **A.Availability** "Availability of keys" describes that the IT environment ensures the availability of cryptographic keys and key material as ensured by the security objective for the IT environment OE.Key_Availability.

The assumption **A.Audit_Analysis** "Analysis of audit trails" addresses reading and analysis of audit records of the TOE as implemented by the security objective for the IT environment OE.Audit_Analysis.

The assumption **A. Environmental_Security** "Environmental Security of systems accessing TOE interfaces" addresses environmental security requirements that are implemented in security objectives of OE.Red-Black-Sep and OE.Personal.

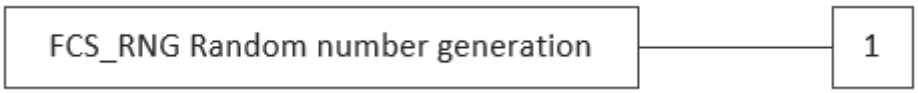
5. Extended Component Definition

5.1. Definition of the Family FCS_RNG

Family behaviour

This family defines requirements for the generation random number where the random numbers are intended to be used for cryptographic purposes.

Component leveling



FCS_RNG.1	Generation of random numbers requires that random numbers meet a defined quality metric.
Management:	FCS_RNG.1 There are no management activities foreseen.
Audit:	FCS_RNG.1 There are no actions defined to be auditable.

FCS_RNG.1 Random number generation

Hierarchical to:	No other components.
Dependencies:	FPT_TST.1.
FCS_RNG.1.1	The TSF shall provide a [selection: physical, non-physical true, deterministic, hybrid] random number generator that meet [assignment: list of security capabilities].
FCS_RNG.1.2	The TSF shall provide random numbers that meet [assignment: a defined quality metric].

5.2. Definition of the Family FPT_EMSEC

Family behaviour

This family defines requirements to mitigate intelligible emanations. The requirements address the level of resistance of the cryptographic module against side channel attacks such as timing analysis, Simple Power Analysis (SPA), Differential Power Analysis (DPA), Electromagnetic emanation analysis (EMEA), and template attacks. If the cryptographic module applies masking, the requirements also address the level of resistance of the cryptographic module against higher-order side channel analysis.

Component leveling

FPT_EMSEC.1	TOE Emanation requires not to emit intelligible physical leakage enabling access to TSF data or user data.
Management:	FPT_EMSEC.1 There are no management activities foreseen.
Audit:	FPT_EMSEC.1 There are no actions defined to be auditable.

FPT_EMSEC.1 TOE Emanation

Hierarchical to:	No other components.
Dependencies:	No other components.
FPT_EMSEC.1.1	The TOE shall not emit [assignment: types of emissions] in excess of [assignment: specified limits] enabling access to [assignment: list of types of TSF data] and [assignment: list of types of user data].
FPT_EMSEC.1.2	The TSF shall ensure [assignment: type of users] are unable to use [assignment: types of interfaces/ports] to gain access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

5.3. Definition of the Security Functional Component FPT_TST.2

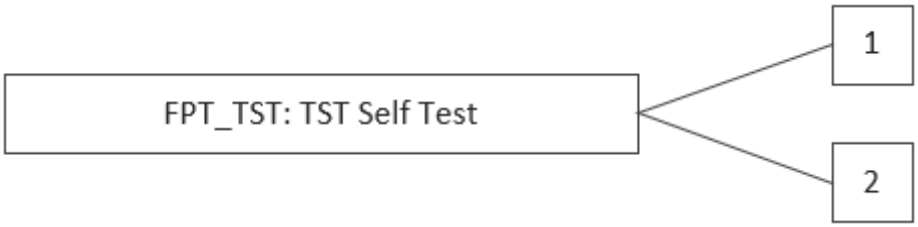
The following addition are made to "TSF self test (FPT_TST)" in Common Criteria, Part 2 to require the self-testing of TSF and of the integrity of the TSF-data and TSF-executable code. FPT_TST.2 requires the behaviour of TSF during self-testing and the actions to be performed by TSF in dependency of the results of the self-testing. This kind of requirements lies beyond FPT_TST.1 defined in Common Criteria, Part 2.

Family behaviour

The family defines the requirements for the self-testing of the TSF with respect to some expected correct operation. Examples are interfaces to enforcement functions, and sample arithmetical operations on critical parts of the TOE. These tests can be carried out at start-up, periodically, at the request of the authorized user, or when other conditions are met. The actions to be taken by the TOE as the result of self testing are defined in other families.

The requirements of this family are also needed to detect the corruption of TSF executable code (i.e. TSF software) and TSF data by various failures that do not necessarily stop the TOE's operation (which would be handled by other families). These checks must be performed because these failures may not necessarily be prevented. Such failures can occur either because of unforeseen failure modes or associated oversights in the design of hardware, firmware, or software, or because of malicious corruption of the TSF due to inadequate logical and/or physical protection.

Component leveling



FPT_TST.1	FPT_TST.1 TSF testing, provides the ability to test the TSF's correct operation. These tests may be performed at start-up, periodically, at the request of the authorized user, or when other conditions are met. It also provides the ability to verify the integrity of TSF data and executable code.
FPT_TST.2	FPT_TST.2 TSF self-testing requires self-testing capabilities of the TSF correct operation. These tests must be performed at start-up. Conditional and on demand by a user self-testing may be required. Particular TSF behaviour during self-testing and TSF-actions after selftesting are required.
Management:	FPT_TST.2 There are no management activities foreseen.
Audit:	FPT_TST.2 The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST: a) Basic: Execution of the TSF self tests and the results of the tests.

FPT_TST.2 self-testing

Hierarchical to:	No other components.
Dependencies:	FPT_FLS.1 Failure with preservation of secure state.
FPT_TST.2.1	The TSF shall perform self-testing at power-up to verify the correctness of [assignment: list of cryptographic algorithms] and of [assignment: list of critical TSF], and to verify the integrity of the TSF-software/firmware.
FPT_TST.2.2	The TSF shall perform self-testing at the conditions [assignment: list of conditions] to verify the correctness of [assignment: list of critical cryptographic algorithms].
FPT_TST.2.3	The TSF shall perform self-testing at the conditions [assignment: list of conditions] to verify the correctness of [assignment: list of critical TSF], and to verify the integrity of [assignment: list of TSF data].
FPT_TST.2.4	The TSF shall perform self-testing at the conditions [assignment: list of conditions] to verify the integrity of [assignment: list of TSF-objects].
FPT_TST.2.5	The TSF shall provide [assignment: list of users] with the capability to invoke the following self-tests [assignment: list of self-tests].
FPT_TST.2.6	During [assignment: list of self-tests] the TSF shall [assignment: list of actions to be performed].
FPT_TST.2.7	After completion of self-testing the TSF shall [assignment: list of actions to be performed].
FPT_TST.2.8	If the self-testing result is fail the TSF shall [assignment: list of actions to be performed].

6. Security Requirements

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is (i) denoted by the word "refinement" in **bold** text and the added/changed words are in **bold** text, or (ii) included in text as bold text and marked by a footnote. In cases where words from a CC requirement were deleted, a separate attachment indicates the words that were removed.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP or ST authors are denoted as *italic* text and the original text of the component is given by a footnote. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and are *italicized*.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP authors are denoted by showing as *italic* text and the original text of the component is given by a footnote. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are *italicized*.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.

6.1. Security Functional Requirements for the TOE

6.1.1. Cryptographic Operation and Key Management

6.1.1.1. FCS_CKM.1/RSA Cryptographic Key Generation

FCS_CKM.1.1/RSA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *RSA*] and specified cryptographic key sizes [assignment: *1024-4096 bits*] that meet the following: [assignment: *FIPS PUB 186-3*].

6.1.1.2. FCS_CKM.1/TDES Cryptographic Key Generation

FCS_CKM.1.1/TDES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *TDES*] and specified cryptographic key sizes [assignment: *168 bits*] that meet the following: [assignment: *NIST SP 800-67*].

6.1.1.3. FCS_CKM.1/AES Cryptographic Key Generation

FCS_CKM.1.1/AES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *AES*] and specified cryptographic key sizes [assignment: *128, 192 and 256 bits*] that meet the following: [assignment: *FIPS PUB 197*].

6.1.1.4. FCS_CKM.1/ECC Cryptographic Key Generation

FCS_CKM.1.1/ECC The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *Elliptic Curve*] and specified cryptographic key sizes [assignment: *192, 224, 256, 384 and 521 bits*] that meet the following: [assignment: *FIPS PUB 186-3 and ANSI X9.62*].

6.1.1.5. FCS_CKM.1/ECDH Cryptographic Key Generation

FCS_CKM.1.1/ECDH The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *Elliptic Curve Diffie-Hellman*] and specified cryptographic key sizes [assignment: *192*, *224, 256, 384 and 521*] that meet the following: [assignment: *NIST SP 800-56A*].

6.1.1.6. FCS_CKM.2/Import Cryptographic Key Distribution

FCS_CKM.2.1/Import The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method *key entry* [2] that meets the following: *secure proprietary electronic key distribution method.*

Refinement:

The key entry shall be performed using either manual or electronic methods. Manually-entered keys shall be verified for accuracy of the input into the TOE. Secret and private keys established using manual methods shall be entered either

1. **in encrypted for or**
2. **using split knowledge procedures.**

If split knowledge procedures are used:

1. **At least two key components shall be required to reconstruct the original cryptographic key,**
2. **if knowledge of n key components is required to reconstruct the original key, then knowledge of any n-1 key components provides no information about the original key other than the length.**

All secret or private keys that are imported into the TOE in encrypted form shall be encrypted and integrity protected using an Endorsed cryptographic algorithm. All public keys electronically entered into the TOE shall be integrity protected using an Endorsed cryptographic algorithm.

[2] [assignment: cryptographic key distribution method]

6.1.1.7. FCS_CKM.2/Export Cryptographic Key Distribution

FCS_CKM.2.1/Export The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method *key export* [3] that meets the following: *proprietary electronic key distribution method.*

Refinement:

The key export shall be performed using either manual or electronic key export methods.

Key components exported for manual key entry method shall support the verification for accuracy of the key material. Secret and private keys exported for manual key entry method shall be exported either

1. **in encrypted for or**
2. **using split knowledge procedures.**

If split knowledge procedures are used:

1. **At least two key components shall be required to reconstruct the original cryptographic key,**
2. **if knowledge of n key components is required to reconstruct the original key, then knowledge of any n-1 key components provides no information about the original key other than the length.**

All secret or private keys exported in encrypted form by the TOE shall be encrypted and integrity protected using an Endorsed cryptographic algorithm. All public keys exported for electronic key entry method shall be integrity protected using an Endorsed cryptographic algorithm.

6.1.1.8. FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [selection: *the TSF*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for *electronic key distribution according to FCS_CKM.2/Import and FCS_CKM.2/Export* [4].

[3] [assignment: cryptographic key distribution method]
[4] [assignment: list of functions for which a trusted channel is required]

6.1.1.9. FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *zeroization*] that meets the following: [assignment: *none*].

6.1.1.10. FCS_COP.1/ENC_DEC_AES Cryptographic Operation - AES Encrypt/Decrypt

FCS_COP.1.1/ENC_DEC_AES The TSF shall perform [assignment: *symmetric encryption and decryption*] in accordance with a specified cryptographic algorithm [assignment: *AES (ECB and CBC mode)*] and cryptographic key sizes [assignment: *128, 192 and 256 bits*] that meet the following: [assignment: *FIPS PUB 197*].

6.1.1.11. FCS_COP.1/ENC_DEC_TDES Cryptographic Operation - TDES Encrypt/Decrypt

FCS_COP.1.1/ENC_DEC_TDES The TSF shall perform [assignment: *symmetric encryption and decryption*] in accordance with a specified cryptographic algorithm [assignment: *TDES (ECB and CBC mode)*] and cryptographic key sizes [assignment: *168 bits*] that meet the following: [assignment: *NIST SP 800-67*].

6.1.1.12. FCS_COP.1/ENC_DEC_RSA Cryptographic Operation - RSA Encrypt/Decrypt

FCS_COP.1.1/ENC_DEC_RSA The TSF shall perform [assignment: a*symmetric encryption and decryption*] in accordance with a specified cryptographic algorithm [assignment: *RSA*] and cryptographic key sizes [assignment: *1024-4096 bits*] that meet the following: [assignment: *RSAES-OAEP from PKCS#1 v2.1*].

6.1.1.13. FCS_COP.1/SIGN_VERIFY Cryptographic Operation - Digital Signature Operations

FCS_COP.1.1/SIGN_VERIFY The TSF shall perform [assignment: *digital signature generation and verification*] in accordance with a specified cryptographic algorithm [assignment: *listed below*] and cryptographic key sizes [assignment: *specified for each algorithm*] that meet the following: [assignment: *specified for each algorithm*].

1. RSA 1024-4096 bits with MD5, SHA-1, SHA-256, SHA-384, SHA-512 (PKCS #1 v1.5)
2. RSA PSS 1024-4096 bits with SHA-1, SHA-256, SHA-384, SHA-512 (PKCS #1 PSS)
3. DSA 1024-3072 bits with SHA-1, SHA-256, SHA-384, SHA-512 (FIPS PUB 186-3)
4. ECDSA curves P-192, P-224, P-256, P-384 and P-521 with SHA-1, SHA-256, SHA-384 and SHA-512 (FIPS PUB 186-3)

6.1.1.14. FCS_COP.1/DIGEST Cryptographic Operation - Message Digest

FCS_COP.1.1/DIGEST The TSF shall perform [assignment: *message digest*] in accordance with a specified cryptographic algorithm [assignment: *listed below*] and cryptographic key sizes [assignment: *specified for each algorithm*] that meet the following: [assignment: *specified for each algorithm*].

1. MD5, 128 bits (RFC 1321)
2. SHA-1, 160 bits (FIPS PUB 180-4)
3. SHA-224, 224 bits (FIPS PUB 180-4)
4. SHA-256, 256 bits (FIPS PUB 180-4)
5. SHA-384, 384 bits (FIPS PUB 180-4)
6. SHA-512, 512 bits (FIPS PUB 180-4)

6.1.1.10. FCS_COP.1/MAC Cryptographic Operation - Message Authentication Code Generate/Verify

FCS_COP.1.1/MAC The TSF shall perform [assignment: *message authentication codes*] in accordance with a specified cryptographic algorithm [assignment: *listed below*] and cryptographic key sizes [assignment: *specified for each algorithm*] that meet the following: [assignment: *specified for each algorithm*].

1. HMAC with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (FIPS PUB 198-1)
2. TDES CMAC with 168 bits keys (NIST SP 800-38B)
3. AES CMAC with 128, 192 and 256 bits keys (NIST SP 800-38B)

6.1.1.11. FCS_RNG.1 Random Number Generation

FCS_RNG.1.1 The TSF shall provide a [selection: *physical true*] random number generator that meet [assignment: *NIST SP 800-90B requirements*].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment: *Shannon entropy of greater than 7.9999 bits per octet based on a 2^{64} bit data set*].

6.1.2. User Identification and Authentication

6.1.2.1. FIA_ATD.1 User Attribute Definition

FIA_ATD.1 The TSF shall maintain the following list of security attributes belonging to individual users:

1. Identity,
2. Role,
3. Reference authentication data,
4. [assignment: *User Login Try Counter*]

6.1.2.2. FIA_UID.1 Timing of Identification

FIA_UID.1.1 The TSF shall allow

1. Self test according to FPT_TST.2,
2. [assignment:
    a. *detection of the secure blocking state (FPT_FLS.1)*
    b. *resistance to physical attack (FPT_PHP.3)*]

on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.2.3. FIA_UAU.1 Timing of Authentication

FIA_UAU.1.1 The TSF shall allow

1. Self test according to FPT_TST.2,
2. Identification according to FIA_UID.1,
3. Selection of [selection: *a role*],
4. [assignment:
    a. *detection of the secure blocking state (FPT_FLS.1)*
    b. *resistance to physical attack (FPT_PHP.3)*]

on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.2.4. FIA_UAU.6 Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions

1. changing to a role not selected for the current valid authentication session,
2. power on or reset,
3. [assignment: *no other conditions* [5]]

6.1.2.5. FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only [assignment: *status messages through LCD/Keypad port*] to the user while the authentication is in progress.

[5] [assignment: list of other conditions under which re-authentication is required]

6.1.2.6. FIA_USB.1 User-Subject Binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

1. Identity,
2. Role,
3. [assignment: *Challenge*]

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: *the initial role of the user is Unidentified user*.

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users:

1. the subject attribute Role shall be changed from Unidentified user to Unauthenticated user after successful identification;
2. after successful authentication the subject attribute Role shall be changed from Unauthenticated User to a role that the user has selected for the authentication session if the user is authorized for this role;
3. after successful re-authentication of the user the subject attribute Role shall be changed to a role that the user has selected for the authentication session if the user is authorized for this role;
4. [assignment: *no other rules* [6]]

6.1.2.7. FIA_AFL.1/HA Authentication Failure Handling

FIA_AFL.1.1/HA The TSF shall detect when [selection: [assignment: *fifteen(15)*]] unsuccessful authentication attempts occur related to [assignment: *HSM Admin authentication*].

FIA_AFL.1.2/HA When the defined number of unsuccessful authentication attempts has been *met* [7], the TSF shall [assignment: *block the user for authentication*].

Application Note: In case of a HA authentication block, the TOE must be re-initialized.

6.1.2.8. FIA_AFL.1/NON_HA Authentication Failure Handling

FIA_AFL.1.1/NON_HA The TSF shall detect when [selection: [assignment: *fifteen(15)*]] unsuccessful authentication attempts occur related to [assignment: *Security Officer and HSM Operator authentication*].

FIA_AFL.1.2/NON_HA When the defined number of unsuccessful authentication attempts has been *met* [8], the TSF shall [assignment: *block the user for authentication*].

[6] [assignment: rules for the changing of attributes]
[7] [selection: met, surpassed]
[8] [selection: met, surpassed]

6.1.3. Protection of User Data

6.1.3.1. FDP_ACC.2/Key_Man Complete Access Control

FDP_ACC.2.1/Key_Man The TSF shall enforce the *Key Management SFP*[9] on:

1. *all cryptographic keys, key components, CSP;*
2. *all user subjects*[10]

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2/Key_Man The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

6.1.3.2. FDP_ACF.1/Key_Man Security Attribute Based Access Control

FDP_ACF.1.1/Key_Man The TSF shall enforce the Key Management SFP[11] to objects based on the following:

1. *Subjects with security attributes: Identity of the user the subject is bind to, Role of this user;*
2. *Objects*
    a. *Cryptographic keys with security attributes: Identity of the key, Key entity, Key type, Key usage type, Key access control rules, Key validity time period;*
    b. *Key components with security attributes: Identity of the key component, Key entity, Key entry method,*
    c. *CSP with security attributes: Identity of the CSP, CSP usage type, CSP access control rules*[12]*.*

FDP_ACF.1.2/Key_Man The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. *Subject in Security Officer role is allowed to import encrypted secret and private keys if the security attribute Key access control rules of the key allows import;*
2. *Subject in Security Officer role is allowed to import one key component of a key with the key entry method assigned to the key component;*
3. *Subject in Security Officer role is allowed to import CSP,*
4. *Subject in Security Officer role is allowed to export encrypted secret or private keys if the security attribute Key access control rules of the key allows export;*
5. *Subject in Security Officer role is allowed to export one key component of a key with the key entry method assigned to the key component;*
6. *Subject in Security Officer role is allowed to export CSP if the security attribute CSP access control rules of the CSP allows export;*
7. *Subject in Security Officer role is allowed to destruct cryptographic keys, cryptographic key components and CSP;*

[9] [assignment: access control SFP]
[10] [assignment: list of subjects and objects]
[11] [assignment: access control SFP]
[12] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]

8. [assignment: *no other rules*][13].

FDP_ACF.1.3/Key_Man The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

1. ***none*** [14]
2. [assignment: *no rules*][15].

FDP_ACF.1.4/Key_Man The TSF shall explicitly deny access of subjects to objects based on the

1. *Subject in Security Officer role is not allowed to import a key component if the same subject or an other subject with the same Identity of the user already input a key component with a different Identity and the same Key entity;*
2. *Subject in Security Officer role is not allowed to export a key component if the same subject or an other subject with the same Identity of the user already export a key component with a different Identity and the same Key entity;*
3. *Subjects with other roles than Security Officer rule are not allowed to input operational public root key;*
4. *Subjects with other roles than Security Officer rule are not allowed to input permanent stored operational secret keys, private keys, key components and CSP;*
5. *No subject is allowed to import or export secret key or private keys in plaintext;*
6. *No subject is allowed to use keys by operation other than identified in Key usage type and the Key access control rules;*
7. [assignment: *no other rules*][16].

6.1.3.3. FDP_ACC.2/Oper Complete Access Control

FDP_ACC.2.1/Oper The TSF shall enforce the *Cryptographic Operation SFP* [17] on

1. *operational cryptographic keys, CSP,*
2. *plaintext data, ciphertext data, original data;*
3. *all user subjects* [18]

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2/Oper The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

[13] [assignment: other rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].
[14] Subjects in Maintenance Personal role are allowed to import and destruct maintenance cryptographic keys, key components and CSP
[15] [assignment: additional rules, based on security attributes, that explicitly authorise access of subjects to objects]
[16] [assignment: other rules, based on security attributes, that explicitly deny access of subjects to objects]
[17] [assignment: access control SFP]
[18] [assignment: list of subjects and objects]

6.1.3.4. FDP_ACF.1/Oper Security Attribute Based Access Control

FDP_ACF.1.1/Oper The TSF shall enforce the *Cryptographic Operation SFP* [19] to objects based on the following:

1. *Subjects with security attributes: Identity of the user the subject is bind to, Role of this user;*
2. *Objects*
    a. *Operational cryptographic keys with security attributes: Identity of the key, Key entity, Key type, Key usage type, Key access control rules, Key validity time period;*
    b. *Operational CSP with security attributes: Identity of the CSP, CSP usage type, CSP access control rules,*
    c. *plaintext data, ciphertext data, original data* [20].

FDP_ACF.1.2/Oper The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. *Subject in **Crypto User*** [21] *role is allowed to perform cryptographic operation in accordance with the security attributes of the used cryptographic keys and CSP;*
2. [assignment: *Subject in Security Officer role is allowed to perform cryptographic operation in accordance with the security attributes of the used cryptographic keys and CSP*][22].

FDP_ACF.1.3/Oper The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *none*][23].

FDP_ACF.1.4/Oper The TSF shall explicitly deny access of subjects to objects based on the following rules:

1. *No subject is allowed to use cryptographic keys by cryptographic operation other than identified in the security attributes Key usage type and the Key access control rules;*
2. *No subject is allowed to use CSP by cryptographic operation other than identified in the security attributes CSP usage type and the CSP access control rules;*
3. [assignment: *no other rules*][24].

[19] [assignment: access control SFP]
[20] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]
[21] End User
[22] [assignment: other rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[23] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
[24] [assignment: other rules, based on security attributes, that explicitly deny access of subjects to objects]

6.1.3.5. FDP_ACC.2/Mode_Trans Complete Access Control

FDP_ACC.2.1/Mode_Trans The TSF shall enforce the *Mode transition SFP* [25] on *all subjects and the mode variable* [26] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2/Mode_Trans The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

6.1.3.6. FDP_ACF.1/Mode_Trans Security Attribute Based Access Control

FDP_ACF.1.1/Mode_Trans The TSF shall enforce the *Mode transition SFP* [27] to objects based on the following: *all subjects and the mode variable* [28].

FDP_ACF.1.2/Mode_Trans The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. *the subject in Security Officer role is allowed to change the mode variable to a Security Officer mode, Key/CSP entry mode,* ***Crypto User*** [29] *mode;*
2. *the subject in* ***Crypto User*** [30] *role is allowed to change the mode variable to Key/CSP entry mode,* ***Crypto User*** [31] *mode;*

FDP_ACF.1.3/Mode_Trans The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

1. *the TOE shall enter automatically the Error mode from any mode of operation except* ***Power-off mode*** [32]*, when failure listed in FPT_FLS.1 occur,*
2. [assignment: *no other rules*][33].

FDP_ACF.1.4/Mode_Trans The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

1. *Subjects in other roles than the Security Officer are not allowed to change the mode variable to a Security Officer mode;*
2. [assignment: *no other rules*][34].

[25] [assignment: access control SFP]
[26] [assignment: list of subjects and objects]
[27] [assignment: access control SFP]
[28] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]
[29] User
[30] End User
[31] User
[32] Power-off mode and Maintenance mode
[33] [assignment: additional rules, based on security attributes, that explicitly authorise access of subjects to objects]
[34] [assignment: other rules, based on security attributes, that explicitly deny access of subjects to objects]

6.1.3.7. FDP_ITC.2 Import of User Data with Security Attributes

FDP_ITC.2.1 The TSF shall enforce the *Key Management SFP and Red-black separation SFP* [35] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE

1. *keys shall be imported with the security attributes Key identity, Key entity, Key type, Key usage type and Key validity time period;*
2. *key components shall be imported with the security attributes Identity of the Key, Key entity, Key entry method;*
3. *CSP shall be imported with security attributes Identity of the CSP and CSP usage type;*
4. *all secret and private keys imported controlled by the TSF shall be encrypted or entered using split knowledge procedures using an Endorsed algorithm* [36]*.*

Application Note: All secret and private keys entered into the TOE and used by an Endorsed function shall be imported in encrypted form or by split knowledge procedures (cf. FCS_CKM.2/Import).

6.1.3.8. FDP_ETC.2 Export of User Data with Security Attributes

FDP_ETC.2.1 The TSF shall enforce the *Key Management SFP and Red-black separation SFP* [37] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TOE:

1. *keys shall be exported with the security attributes Key identity, Key entity, Key type, Key usage type and Key validity time period;*
2. *secret and private keys exported in encrypted form shall be exported with additional security attribute: Identity of the key encryption key under which they are encrypted;*
3. *key components shall be exported with the security attributes Identity of the Key component, Key entity, Key entry method;*
4. *CSP shall be exported with security attributes Identity of the CSP and CSP usage type;*

[35] [assignment: access control SFP and/or information flow control SFP]
[36] [assignment: additional importation control rules]
[37] [assignment: access control SFP(s) and/or information flow control SFP(s)]

5. *all secret and private keys exported controlled by the TSF shall be encrypted or protected by split-knowledge procedure using an Endorsed algorithm* [38].

6.1.3.9. FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the *Red-black separation SFP* [39] on

1. *all user subjects;*
2. *cryptographic keys, cryptographic key components, CSP, plaintext data, ciphertext data, original data;*
3. *all operations* [40].

6.1.3.10. FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the *Red-black separation SFP* [41] based on the following types of subject and information security attributes:

1. *all user subjects;*
2. *objects*
   a. *cryptographic keys and cryptographic key components with security attributes: Identity of the key, Key entity, Key type, Key usage type, Key access control rules, Key validity time period;*
   b. *CSP with security attributes: Identity of the CSP, CSP usage type, CSP access control rules;*
   c. *plaintext data, ciphertext data, original data* [42].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

1. *Subject in a user role is allowed to import or export cryptographic keys, cryptographic key components and CSP in accordance with the security attributes of these objects* [43].

FDP_IFF.1.3 The TSF shall enforce the

1. *Subject in a user role is allowed to exchange cryptographic keys, cryptographic key components, CSP, plaintext data, ciphertext data and original data in accordance with the access rights of the operation that cause the information to flow to and from the subjects* [44].

---

[38] [assignment: additional exportation control rules]
[39] [assignment: information flow control SFP]
[40] [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP]
[41] [assignment: information flow control SFP]
[42] [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes]
[43] [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]
[44] [assignment: additional information flow control SFP rules]

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: *no explicit authorisation rules* [45].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: *no explicit denial rules* [46].

6.1.3.11. FDP_UCT.1 Basic Data Exchange Confidentiality

FDP_UCT.1.1 The TSF shall enforce the *Red-black separation SFP* [47] **by providing the ability to** *transmit and receive* [48] user data in a manner protected from unauthorised disclosure.

Application note: The element FDP_UCT.1 was refined by substituting "the TSF shall enforce … to be able to" by "the TSF shall enforce… by providing the ability to" to ensure the confidentiality of user data when it is transferred using an external channel between distinct TOEs or users on distinct TOEs.

6.1.3.12. FDP_UIT.1 Data Exchange Integrity

FDP_UIT.1.1 The TSF shall enforce the *Red-black separation SFP* [49] to be able to *transmit and receive* user data in a manner protected from modification [selection: *deletion, insertion and replay*][50] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether modification [selection: *deletion, insertion and replay*][51] has occurred.

6.1.3.13. FDP_RIP.2 Full Residual Information Protection

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to*][52] all objects.

[45] [assignment: rules, based on security attributes, that explicitly authorise information flows]
[46] [assignment: rules, based on security attributes, that explicitly deny information flows].
[47] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[48] [selection: transmit, receive]
[49] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[50] [selection: deletion, insertion, replay]
[51] [selection: deletion, insertion, replay]
[52] [selection: allocation of the resource to, deallocation of the resource from]

6.1.4. Audit

6.1.4.1. FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

1. *Start-up and shutdown of the audit functions;*
2. *All auditable events for the [selection, choose one of: not specified] level of audit; and*
3. *other auditable events*
    a. *Start-up after power-up*
    b. ***Software download*** [53]
    c. *Authentication failure handling (FIA_AFL.1): the reaching of the threshold for the unsuccessful authentication attempts and the actions,*
    d. *Timing of authentication (FIA_UAU.1): all unsuccessful authentication attempts of the authentication mechanism with the following information: claimed Identity of the user,*
    e. *Import of key components (FCS_CKM.2/Import) with the following information: Identity of the key component, Entity of the key, Identity of the user;*
    f. *Export of key components (FCS_CKM.2/Export) with the following information: Identity of the key component, Entity of the key, Identity of the user;*
    g. *Cryptographic key destruction (FCS_CKM.4): permanent stored keys;*
    h. *Failure with preservation of secure state (FPT_FLS.1): start-up after failure detection of the TSF and secure mode,*
    i. *Management of TSF data (FMT_MTD.1/AUDIT): Export and clear of audit data,*
    j. *Management of security functions behaviour (FMT_MOF.1/SO),*
    k. [assignment:
        i. *Resistance to Physical Attack (FPT_PHP.3): Detection of intrusion*
        ii. *TOE state changes*][54]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a. Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *event number*].

6.1.4.2. FAU_GEN.2 User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.4.3. FAU_SAR.1 Audit Review

[53] Maintenance with software download if supported by the TOE,
[54] [assignment: other specifically defined auditable events]

FAU_SAR.1.1 The TSF shall provide ***HSM Admin***[55] with the capability to *read all audit data* [56] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.4.4. FAU_SAR.2 Protected Audit Trail Storage

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records except those users that have been granted explicit read-access.

6.1.4.5. FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to *prevent* [57] unauthorized modifications to the stored audit records in the audit trail.

6.1.4.6. FAU_STG.3 Action in Case of Possible Audit Data Loss

FAU_STG.3.1 The TSF shall support the following actions

1. ***overwrite the oldest stored audit records*** [58]*,*
2. *[assignment: no other actions]* [59]*,*

if the audit trail exceeds *the audit trail storage capacity* [60].

6.1.4.7. FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Application Note: The reliable time stamp is used for audit TSF according to FAU_GEN.1 and to enforce the Key validity time period defined for a key according to FDP_ACF.1/Oper.

[55] [assignment: authorized users]
[56] [assignment: list of audit information]
[57] [selection, choose one of: prevent, detect]
[58] action to prevent audit data loss as defined in FAU_STG.4
[59] [assignment: actions to be taken in case of possible audit storage failure]
[60] [assignment: pre-defined limit]

6.1.5. Management of TSF and Protection of TSF Data

6.1.5.1. FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

1. management of security functions behavior (**FMT_MOF.1/SO**[61]),
2. management of Reference Authentication Data (FMT_MTD.1/Admin, FMT_MTD.1/User),
3. management of audit data (FMT_MTD.1/Audit)
4. management of security attributes of cryptographic keys, cryptographic key components and CSP (FMT_MSA.1/Key_Man_1, FMT_MSA.1/Key_Man_2, FMT_MSA.1/Key_Man_3, FMT_MSA.2, FMT_MSA.3/Key_Man)
5. [assignment: no other functions][62].

6.1.5.2. FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles: ***Crypto User***[63] *Role, Security Officer Role,* ***HSM Admin***[64] *Role, Unidentified User Role, Unauthenticated User Role,* [assignment: HSM Operator][65].

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions

1. Any user identity assigned to the **HSM Admin**[66] Role must not be assigned to the **Crypto User**[67] Role or the Security Officer Role,
2. Any user identity assigned to the Security Officer Role must not be assigned to the **Crypto User**[68] Role or the **HSM Admin**[69] Role,
3. [assignment: Any user identity assigned to the HSM Operator Role must not be assigned to the HSM Admin Role, Security Officer Role or the Crypto User Role][70]

are satisfied.

[61] FMT_MOF.1/Adm and FMT_MOF.1/SO
[62] [assignment: list of security management functions to be provided by the TSF]
[63] End User
[64] Administrator
[65] [assignment: authorised identified roles]
[66] Administrator
[67] End User
[68] End User
[69] Administrator
[70] [assignment: conditions for the different roles]

6.1.5.3. FMT_MOF.1/SO Management of Security Functions Behaviour

FMT_MOF.1.1/SO The TSF shall restrict the ability to [selection: *enable*] the functions [assignment: *the Crypto User role*][71] to *Security Officer* [72].

6.1.5.4. FMT_MTD.1/Admin Management of TSF Data

FMT_MTD.1.1/Admin The TSF shall restrict the ability to *create, clear and delete* [73] the *Reference Authentication Data* [74] to ***HSM Admin*** [75].

6.1.5.5. FMT_MTD.1/User Management of TSF Data

FMT_MTD.1.1/User The TSF shall restrict the ability to *modify* [76] the *Reference Authentication Data* [77] to *the authorized user* [78] for their own Reference Authentication Data.

6.1.5.6. FMT_MTD.1/Audit Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to *export and clear* [79] the *audit data* [80] to ***HSM Admin***[81].

6.1.5.7. FMT_MSA.1/Key_Man_1 Management of Security Attributes

FMT_MSA.1.1/Key_Man_1 The TSF shall enforce the *Key Management SFP* [82] to restrict the ability to *change_default and query* [83] the security attributes *Identity of the key, Key entity, Key type of the key, Key usage type, Identity of the key component, Key entity of the key component, Key entry method, Identity of the CSP, CSP usage type*[84] to *Security Officer* [85] *and Crypto User*.

---

[71] [assignment: list of functions]
[72] [assignment: the authorised identified roles]
[73] [selection: change_default, query, modify, delete, clear,[assignment: other operations]]
[74] [assignment: list of TSF data]
[75] [assignment: the authorised identified roles]
[76] [selection: change_default, query, modify, delete, clear,[assignment: other operations]]
[77] [assignment: list of TSF data]
[78] [assignment: the authorised identified roles]
[79] [selection: change_default, query, modify, delete, clear,[assignment: other operations]]
[80] [assignment: list of TSF data]
[81] [assignment: the authorised identified roles]
[82] [assignment: access control SFP, information flow control SFP]
[83] [selection: change_default, query, modify, delete, [assignment: other operations]]
[84] [assignment: list of security attributes]
[85] [assignment: the authorised identified roles]

6.1.5.8. FMT_MSA.1/Key_Man_2 Management of Security Attributes

FMT_MSA.1.1/Key_Man_2 The TSF shall enforce the *Key Management SFP* [86] to restrict the ability to *modify or delete* [87] the security attributes *Identity of the key, Key entity of the key, Key type, Key usage type, Key validity time period, Identity of the key component, Key entity of the key component, Key entry method, Identity of the CSP, CSP usage type* [88] to none[89].

6.1.5.9. FMT_MSA.1/Key_Man_3 Management of Security Attributes

FMT_MSA.1.1/Key_Man_3 The TSF shall enforce the *Key Management SFP* [90] to restrict the ability to *modify* [91] the security attributes *Key access control rules, CSP access control rules* [92] to *Security Officer* [93].

[86] [assignment: access control SFP, information flow control SFP]
[87] [selection: change_default, query, modify, delete, [assignment: other operations]]
[88] [assignment: list of security attributes]
[89] [assignment: the authorised identified roles]
[90] [assignment: access control SFP, information flow control SFP]
[91] [selection: change_default, query, modify, delete, [assignment: other operations]]
[92] [assignment: list of security attributes]
[93] [assignment: the authorised identified roles]

6.1.5.10. FMT_MSA.2 Secure Security Attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for *Identity of the key, Key entity, Key type of the key, Key usage type, Key access control rules, Key validity time period, Identity of the key component, Key entity of the key component, Key entry method, Identity of the CSP, CSP usage type, CSP access control rules* [94].

6.1.5.11. FMT_MSA.3/Key_Man Static Attribute Initialisation

FMT_MSA.3.1/Key_Man The TSF shall enforce the *Key Management SFP* [95] to provide *permisive* [96] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/Key_Man The TSF shall allow the Security Officer[97] and Crypto User to specify alternative initial values to override the default values when an object or information is created.

Application Note: SO and CU has same permissions about attribute initialization except key export attribute. If an object is defined with attribute Modifiable is false, then no change in attributes is possible after creation of object.

6.1.5.12. FMT_MSA.3/Oper Static Attribute Initialisation

FMT_MSA.3.1/Oper The TSF shall enforce the *Cryptographic Operation SFP* [98] to provide *restrictive* [99] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/Oper The TSF shall allow the **none**[100] to specify alternative initial values to override the default values when an object or information is created.

6.1.5.13. FMT_MSA.3/Mode_Trans Static Attribute Initialisation

FMT_MSA.3.1/Mode_Trans The TSF shall enforce the *Mode Transition SFP* [101] to provide *restrictive* [102] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/Mode_Trans The TSF shall allow the **none**[103] to specify alternative initial values to override the default values when an object or information is created.

---

[94] [assignment: list of security attributes]
[95] [assignment: access control SFP, information flow control SFP]
[96] [selection, choose one of: restrictive, permissive,[assignment: other property]]
[97] [assignment: the authorised identified roles]
[98] [assignment: access control SFP, information flow control SFP]
[99] [selection, choose one of: restrictive, permissive,[assignment: other property]]
[100] [assignment: the authorised identified roles]
[101] [assignment: access control SFP, information flow control SFP]
[102] [selection, choose one of: restrictive, permissive,[assignment: other property]]
[103] [assignment: the authorised identified roles]

6.1.6. TSF Protection

6.1.6.1. FPT_TDC.1 Inter-TSF Basic TSF Data Consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret *security attributes of cryptographic keys, key components and CSP* [104] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use the following rules:

1. *the TOE reports about conflicts between the Identity of the key of stored cryptographic keys and cryptographic keys to be imported,*
2. *the TOE does not change the security attributes Identity of the key, Key entity of the key, Key type, Key usage type and Key validity time period of keys being imported or exported,*
3. *the TOE reports about conflicts between the Identity of cryptographic key components of stored key components and cryptographic key components to be imported,*
4. *the TOE does not change the security attributes Identity of the key component, Key entity, Key entry method of components keys being imported,*
5. *the TOE reports about conflicts between the Identity of the CSP of stored CSP and CSP to imported,*
6. *the TOE does not change the security attributes Identity of the CSP and CSP usage type of CSP being imported or exported* [105]

when interpreting the TSF data from another trusted IT product.

6.1.6.2. FPT_FLS.1 Failure with Preservation of Secure State

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: *self test fails* [106].

Refinement:

When the TOE is in a secure error mode the TSF shall not perform any cryptographic operations and all data output interfaces/ports shall be inhibited by the TSF.

6.1.6.3. FPT_EMSEC.1 TOE Emanation

FPT_EMSEC.1.1 The TOE shall not emit [assignment: conducted emission, radiated emission] in excess of [assignment: state of the art in order to have unintelligible emission] enabling access to

1. *confidential authentication data,*

[104] [assignment: list of TSF data types]
[105] [assignment: list of interpretation rules to be applied by the TSF]
[106] [assignment: list of types of failures in the TSF]

2. [assignment: *no other TSF data*][107]

and

1. *"red data" containing confidential information,*
2. *plaintext cryptographic secret or private key,*
3. *cryptographic key components,*
4. *confidential CSP,*
5. [assignment: *no other user data*][108].

FPT_EMSEC.1.2 The TSF shall ensure [assignment: *unidentified users and unauthenticated users*] are unable to use *any interface or port with exception identified below* [109] to gain access to

1. *confidential authentication data (except the authentication interface/port during authentication process of the user),*
2. [assignment: *no other TSF data*]

and

1. *"red data" containing confidential information (except the red data input and output interface/port),*
2. *plaintext cryptographic secret or private key,*
3. *cryptographic key components (except key interface during import of the cryptographic key component)*
4. *confidential CSP (except key interface during import of the confidential CSP),*
5. [assignment: *no other user data*][110]

6.1.6.4. FPT_TST.1 TSF Testing

FPT_TST.1.1 The TSF shall run a suite of self tests [selection: *during initial start-up*] to demonstrate the correct operation of [selection: *the TSF*].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [selection: *TSF data*].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

6.1.6.5. FPT_TST.2 TSF Self-Testing

FPT_TST.2.1 The TSF shall perform self-testing at power-up to verify the correctness of [assignment: *AES, TDES, RSA, DSA, ECDSA, ECDH, MD5, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, HMAC SHA-1, HMAC SHA-224, HMAC-SHA256, HMAC SHA-384, HMAC SHA-512, CTR-DRBG, TRNG*] and of [assignment: *encryption/decryption, signature generation/verification, hash*

[107] [assignment: list of types of TSF data]
[108] [assignment: list of types of user data]
[109] [assignment: types of interfaces/ports]
[110] [assignment: list of types of user data]

generation/verification, keyed hash generation/verification, random number generation], and to verify the integrity of the TSF-software/firmware.

FPT_TST.2.2 The TSF shall perform self-testing at the conditions [assignment: *random number generation, asymmetric key generation*] to verify the correctness of [assignment: *TRNG, CTR-DRBG, RSA, DSA, ECDSA*].

FPT_TST.2.3 The TSF shall perform self-testing at the conditions [assignment: *firmware update*] to verify the correctness of [assignment: *encryption/decryption, signature generation/verification, hash generation/verification, keyed hash generation/verification, random number generation*], and to verify the integrity of [assignment: *firmware*].

FPT_TST.2.4 The TSF shall perform self-testing at the conditions [assignment: *none*] to verify the integrity of [assignment: *none*].

FPT_TST.2.5 The TSF shall provide [assignment: *HSM Admin*] with the capability to invoke the following self-tests [assignment*: encryption/decryption, signature generation/verification, hash generation/verification, keyed hash generation/verification, random number generation, firmware integrity and authenticity*].

FPT_TST.2.6 *During initial start-up self-test, power-up self-test [assignment: no other self-tests]* [111] the TSF shall *inhibit all output via the data interfaces/ports, and [assignment: prevent authentication to the TOE, any cryptographic operations]* [112].

FPT_TST.2.7 After completion of self-testing the TSF shall *output the results of the self tests via the status output interface/port, and [assignment: none]* [113].

FPT_TST.2.8 If the self-testing result is fail the TSF shall *enter a secure state (see FPT_FLS.1) and output an error indicator via the status output interface/port, and [assignment: prevent any cryptographic operations]* [114].

Refinement:

A start-up test shall be performed when the TOE is powered up (after being powered off) or on reset. A list of cryptographic algorithms shall include all Endorsed cryptographic algorithms employed by the TOE.

In order to verify the correctness of cryptographic algorithms self-testing shall perform a known answer or a pair-wise consistency test. If the TOE module includes two independent implementations of the same cryptographic algorithm, then the outputs of two implementations shall be compared.

In order to verify the integrity of the TSF-software/firmware a self-testing using an Endorsed error detection code (EDC) or Endorsed authentication technique shall be applied.

The self-testing at the conditions shall cover the following conditions: i) when a critical cryptographic algorithm or critical TSF operation is invoked, ii) pairwise consistency test for newly generated asymmetric key-pairs, iii) on software/firmware load test, iv) and on manual key entry events.

---

[111] [assignment: list of self-tests]
[112] [assignment: list of actions to be performed]
[113] [assignment: list of actions to be performed]
[114] [assignment: list of actions to be performed]

The following pair-wise consistency tests for public and private keys shall be performed. A public key shall encrypt a plaintext value. The resulting ciphertext value shall be compared to the original plaintext value. If the two values are equal, then the test shall fail. If the two values differ, then the private key shall be used to decrypt the ciphertext and the resulting value shall be compared to the original plaintext value. If the two values are not equal, the test shall fail. Also, consistency of the keys shall be tested by the calculation and verification of a digital signature. If the digital signature cannot be verified, the test shall fail.

The following software/firmware load tests shall be performed. An Endorsed authentication technique shall be applied to all validated software and firmware components when the components are externally loaded into the TOE. The calculated result shall be compared with a previously generated result. If the calculated result does not equal the previously generated result, the software/firmware integrity test shall fail.

Application Note: A cryptographic algorithm shall have an independent known-answer self-test or the known-answer self-test shall be included with the associated cryptographic algorithm self-test. If the calculated output does not equal the known answer, the known answer self-test shall fail. If a known-answer self-test is not appropriate because the output of the cryptographic algorithms vary for a given set of inputs (e.g., a digital signature generated by means of the Digital Signature Algorithm) it shall be tested using a known-answer test or using the inverse cryptographic function (e.g., a digital signature is verified). Random number generators shall implement statistical or other appropriate tests.

6.1.6.6. FPT_PHP.3 Resistance to Physical Attack

FPT_PHP.3.1 The TSF shall resist physical manipulation and probing[115] to the TSF[116] by responding automatically such that the SFRs are always enforced.

Refinement:

The TOE shall contain tamper response circuitry, which shall immediately destruct all plaintext secret and private keys and CSPs upon the detection of physical tampering.

Application Note: The TOE should implement specific security mechanisms to resist physical tampering scenarios with high attack potential.

If the TOE contains circuitry for implementing physical attack response (e.g., destruction of keys), than this circuitry shall remain operational as long as plaintext cryptographic keys, cryptographic key components and CPSs are contained within the TOE. A tamper detection envelope may be, e.g., a flexible mylar printed circuit with a serpentine geometric pattern of conductors.

[115] [assignment: physical tampering scenarios]
[116] [assignment: list of TSF devices/elements]

6.2. Security Assurance Requirements

The TOE meets the security assurance requirements for EAL4, augmented with ADV_IMP.2, ALC_CMC.5, ALC_DVS.2, AVA_VAN.5 and ALC_FLR.2. The following table is the summary for the assurance requirements.

Some of the assurance components are refined in the "Cryptographic Modules, Security Level [Enhanced]" and those are introduced in the subchapters of this chapter. Only the refined security assurance requirement elements are introduced and the unchanged elements are not stated in this ST.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security Architecture
	ADV_FSP.4 Functional Specification
	ADV_IMP.2[117] Implementation Representation
	ADV_TDS.3 TOE Design
AGD: Guidance Documents Activities	AGD_OPE.1 Operational User Guidance
	AGD_PRE.1 Preparative Procedures
ALC: Life Cycle Support	ALC_CMC.5[118] CM Capabilities
	ALC_CMS.4 CM Scope
	ALC_DEL.1 Delivery
	ALC_DVS.2[119] Development Security
	ALC_FLR.2[120] Flaw Remediation
	ALC_LCD.1 Life Cycle Definition
	ALC_TAT.1

[117] Augmented by developer.
[118] Augmented by developer.
[119] Augmented by developer.
[120] Augmented by developer.

Assurance Class	Assurance Components
	Tools and Techniques
ASE: Security Target Evaluation	ASE_CCL.1 Conformance Claims
	ASE_ECD.1 Extended Components Definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.2 Security Objectives
	ASE_REQ.2 Security Requirements
	ASE_SPD.1 Security Problem Definition
	ASE_TSS.1 TOE Summary Specification
ATE: Tests Activities	ATE_COV.2 Coverage
	ATE_DPT.2 Depth
	ATE_FUN.1 Functional Tests
	ATE_IND.2 Independent Testing
AVA: Vulnerability Assessment	AVA_VAN.5[121] Vulnerability Analysis

Table 7: Security Assurance Requirements

6.2.1. Refinement of ADV_ARC.1

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

Refinement:

The security architecture description shall describe domain separation in terms of red-black separation. The red-black separation shall describe that the TOE physically or logically separates the interfaces for red user data, black user data, CSP (including plaintext cryptographic keys and cryptographic key components) and administrative functions. Further, the security architecture description shall describe that the data output is disabled while performing (1) key generation and manual key entry for the

[121] Augmented by developer.

communication through this data port, (2) self-tests, (3) software loading and key destruction.

The security architecture description shall describe domain separation in terms of a semiformal Finite state model.

The Finite state model of the TOE shall describe at least the following modes

1. **Power on/off modes**
2. **Security Officer modes**
3. **Key/CSP entry modes.**
4. **Crypto User modes**[122]
5. **Self-test modes**
6. **Error modes**

The Finite state model of the TOE shall describe the mode transition in terms of the input and internal events and internal conditions that cause transitions from one mode to another and the output events resulting from transitions from one mode to another. The security architecture description shall describe that the data output interface is inhibited when the TOE is in an error mode or in self-test mode.

ADV_ACR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Refinement:

The evaluator shall confirm that the security architecture for the red-black separation and the finite state model is consistent with the TSF presentation in the functional specification, TOE design, TSF implementation, guidance documentation, and evaluator tests.

Application Note: The term "mode" for the states in the model is used according to the mode addressed in FDP_ACC.2/Mode_Trans and FDP_ACF.1/Mode_Trans. The term "finite state model" stands for a semiformal style model that is used for the analysis. The model describes domain separation in terms of a finite set of states in the model related to the modes of operation of the cryptographic module. State transition in the model should be described in terms of internal actions and conditions for changing the modes of operation of the cryptographic module. Note that the cryptographic module can only reside in one active mode in the finite state model. If the behaviour of operational modes (Security Officer modes, Key/CSP entry modes, User modes, Self-test modes, Error modes) depends on the available power supply, this changed behaviour shall be mapped to a refinement of the respective operational modes. Domain separation in the finite state model can correspond to the separation of modes.

6.2.2. Refinement of ADV_FSP

ADV_FSP.4.2C The functional specification shall describe the purpose and method of use for all TSFI.

Refinement:

[122] User modes

The *functional specification* shall describe *all details of all effects*. It shall also specify as minimum the normal voltage and temperature operating ranges of the cryptographic module.

The *functional specification* shall describe the interface indicating the selection of an Endorsed mode of operation and the interfaces for user data and TSF data as Endorsed modes of operation.

The *functional specification* shall identify the logical interfaces and physical ports as of the following types ("input" and "output" are indicated from the perspective of the module):

- **Data input interface/port: All data (except control data entered via the control input interface) that is input to and processed by the cryptographic module (including plaintext data, ciphertext data, cryptographic keys and CSPs, authentication data, and status information from another entities),**
- **Data output interface/port: All data (except status data output via the status output interface) that is output from the cryptographic module (including plaintext data, ciphertext data, cryptographic keys and CSPs, authentication data, and control information for another entity). All data output via the data output interface shall be inhibited when the TOE is in an error mode or in self-test mode,**
- **Control input interface/port: All input commands, signals, and control data (including function calls and manual controls such as switches, buttons, and keyboards) used to control the operation of a cryptographic module shall enter via the "control input" interface.**
- **Status output interface/port: All output signals, indicators, and status data (including return codes and physical indicators such as Light Emitting Diodes and displays) used to indicate the status of a cryptographic module shall exit via the "status output" interface,**
- **Power interface/port: all external electrical power supply.**

Application Note: Note the TOE shall separate logically the interfaces for red user data, black user data, CSP (including plaintext cryptographic keys and cryptographic key components) and administrative functions according to refinement of ADV_ARC.1. The functional specification shall describe this logical separation according to ADV_FSP.4.3C, ADV_FSP.4.4C and ADV_FSP.4.5C.

6.2.3. Refinement of ADV_IMP.2

ADV_IMP.2.1C The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.

Refinement:

The implementation representation for all software and firmware of the TOE shall be done in a high-level language. The exceptional limited usage of low-level language (e.g., assembly language or microcode) is allowed if essential to the performance of the TOE or when a high-level language is not available. The implementation representation for all hardware components of the TOE within the cryptographic module shall be done in a high-level specification language. The source code of implementation representation for each hardware, software, and firmware

component (of the TOE) shall be annotated with comments that specify the preconditions required upon entry into the component (of the TOE), function, or procedure in order to execute correctly and the post-conditions expected to be true when execution of the component (of the TOE), function, or procedure is complete.

6.2.4. Refinement of ADV_TDS.3.3C

ADV_TDS.3.3C The design shall identify all subsystems of the TSF.

Refinement:

The TOE design shall identify the subsystem with the interface providing the physical port for the import of secret key, private keys and key component. This subsystem and all subsystem which transfer or store any secret key, private keys and key module shall be SFR-enforcing.

The TOE design shall specify the key storage methods employed by the TOE.

The TOE design shall specify methods to destruct all plaintext secret and private cryptographic keys, key components and CSPs within the module.

The TOE design shall identify the modules with the interface providing the physical port for the import of secret key, private keys and key component. This module and all modules which transfer or store any secret key, private keys and key components shall be SFR-enforcing.

The TOE design shall describe the physical enclosure of the TOE. This description shall demonstrate that the enclosure is production grade. The demonstration must either show that an enclosure of the same material has been used commercially, or provide data to show that it is equivalent to a commercial product.

The TOE design shall describe that the quality metric of FCS_RNG.1 for the random number generator is accomplished.

6.2.5. Refinement of AGD_OPE.1

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

Refinement:

The guidance documentation shall describe how the user is able to determine when an Endorsed mode of operation is selected and what the current status of the cryptographic module is.

6.3. Security Requirements Rationale

6.3.1. Security Functional Requirements Rationale

The following table provides an overview on how the TOE security functional requirements cover the TOE security objectives.

	O.Red-Black-Sep	O.Endorsed_Crypto	O.I&A	O.Control_Services	O.Control_Keys	O.Roles	O.Audit	O.Key_Export	O.Key_Generation	O.Key_Import	O.Key_Management	O.Key_Destruction	O.Check_Operation	O.Physical_Protect	O.Prevent_Inf_Leakage
FCS_CKM.1/RSA		■							■		■				
FCS_CKM.1/TDES		■							■		■				
FCS_CKM.1/AES		■							■		■				
FCS_CKM.1/ECC		■							■		■				
FCS_CKM.1/ECDH		■							■		■				
FCS_CKM.2/Import		■								■	■				
FCS_CKM.2/Export		■						■			■				
FCS_CKM.4		■									■	■			
FTP_ITC.1								■		■	■				
FCS_COP.1/ENC_DEC_AES	■	■													
FCS_COP.1/ENC_DEC_TDES	■	■													
FCS_COP.1/ENC_DEC_RSA	■	■													
FCS_COP.1/SIGN_VERIFY	■	■													
FCS_COP.1/DIGEST	■	■													
FCS_COP.1/MAC	■	■													
FCS_RNG.1		■							■						
FIA_ATD.1			■												
FIA_UID.1			■												
FIA_UAU.1			■												
FIA_UAU.6			■												
FIA_UAU.7			■												
FIA_USB.1			■												
FIA_AFL.1/HA			■												
FIA_AFL.1/NON_HA			■												
FDP_ACC.2/Key_Man				■	■						■	■			

	O.Red-Black-Sep	O.Endorsed_Crypto	O.I&A	O.Control_Services	O.Control_Keys	O.Roles	O.Audit	O.Key_Export	O.Key_Generation	O.Key_Import	O.Key_Management	O.Key_Destruction	O.Check_Operation	O.Physical_Protect	O.Prevent_Inf_Leakage
FDP_ACF.1/Key_Man				■	■						■	■			
FDP_ACC.2/Oper				■	■										
FDP_ACF.1/Oper				■	■										
FDP_ACC.2/Mode_Trans				■	■										
FDP_ACF.1/Mode_Trans				■	■										
FDP_ITC.2	■	■								■	■				
FDP_ETC.2	■	■						■			■				
FDP_IFC.1	■			■	■			■		■	■				
FDP_IFF.1	■			■	■			■		■	■				
FDP_UCT.1	■							■		■	■				
FDP_UIT.1	■							■		■	■				
FDP_RIP.2															■
FAU_GEN.1							■								
FAU_GEN.2							■								
FAU_SAR.1							■								
FAU_SAR.2							■								
FAU_STG.1							■								
FAU_STG.3							■								
FPT_STM.1					■		■								
FMT_SMF.1				■							■				
FMT_SMR.2				■		■					■				
FMT_MOF.1/SO				■											
FMT_MTD.1/Admin			■												
FMT_MTD.1/User			■												
FMT_MTD.1/Audit							■								
FMT_MSA.1/Key_Man_1				■	■						■				
FMT_MSA.1/Key_Man_2				■	■						■				
FMT_MSA.1/Key_Man_3				■	■						■				
FMT_MSA.2				■	■						■				
FMT_MSA.3/Key_Man				■					■		■				
FMT_MSA.3/Oper				■											
FMT_MSA.3/Mode_Trans				■											

	O.Red-Black-Sep	O.Endorsed_Crypto	O.I&A	O.Control_Services	O.Control_Keys	O.Roles	O.Audit	O.Key_Export	O.Key_Generation	O.Key_Import	O.Key_Management	O.Key_Destruction	O.Check_Operation	O.Physical_Protect	O.Prevent_Inf_Leakage
FPT_TDC.1								■		■	■				
FPT_FLS.1													■		
FPT_EMSEC.1	■														■
FPT_TST.1													■		
FPT_TST.2													■		
FPT_PHP.3														■	

Table 8: Coverage of Security Objective for the TOE by SFR

The security objective **O.Red-Black-Sep** "Red-black separation of the TOE" is provided by the following SFR:

- FCS_COP.1/ENC_DEC_AES, FCS_COP.1/ENC_DEC_TDES, FCS_COP.1/ENC_DEC_RSA, FCS_COP.1/SIGN_VERIFY, FCS_COP.1/DIGEST, FCS_COP.1/MAC require the necessary cryptographic operations needed for encryption, decryption of data containing confidential information and integrity protection for data containing integrity sensitive information.
- FDP_IFC.1, FDP_IFF.1, FDP_ITC.2 and FDP_ETC.2 ensure the import and export of cryptographic keys, cryptographic key components and CSP with security attribute, which are associated with these objects.
- FDP_UCT.1 addresses the protection of the data containing confidential information during data exchange.
- FDP_UIT.1 addresses the protection of the data containing integrity sensitive information during data exchange.
- FPT_EMSEC.1 requires protection of confidential information against emanation.

The security objective **O.Endorsed_Crypto** "Endorsed cryptographic functions" requires the TOE to provide Endorsed cryptographic functions and Endorsed cryptographic protocols to protect the user data as required by OSP.User_Data_Prot and for key management. This security objective is provided by the SFR FCS_CKM.1/RSA, FCS_CKM.1/TDES, FCS_CKM.1/AES, FCS_CKM.1/ECC, FCS_CKM.1/ECDH, FCS_CKM.2/Import, FCS_CKM.2/Export, FCS_CKM.4, FCS_COP.1/ENC_DEC_AES, FCS_COP.1/ENC_DEC_TDES, FCS_COP.1/ENC_DEC_RSA, FCS_COP.1/SIGN_VERIFY, FCS_COP.1/DIGEST, FCS_COP.1/MAC and FCS_RNG.1, which require meeting Endorsed standards for cryptographic functions. FDP_ITC.2 and FDP_ETC.2 enforce the use of Endorsed cryptographic functions for import and export of confidential cryptographic keys.

The security objective **O.I&A** "Identification and authentication of users" requires the TOE to identify uniquely users and to verify the claimed identity of the user before providing access to any controlled resources with the exception of read access to public objects. This security objective is provided by the following SFR:

- FIA_UID.1 allows unidentified users to run self test of the TOE only and requires identification before any other TSF mediated action.

- FIA_UAU.1 allows unauthenticated users to run self test of the TOE, identification according FIA_UID.1 and selection of a claimed role and requires authentication before any other TSF mediated action.
- FIA_UAU.6 requires re-authentication after start-up of the TOE and if the user changes the role after authentication.
- FIA_UAU.7 requires limitation of the feedback to the user while authentication is in progress.
- FIA_AFL.1 requires detection and reaction to unsuccessful authentication attempts.
- FIA_ATD.1 requires maintaining security attributes to individual users including Identity, Role and Reference authentication data as prerequisite for identification and authentication of authorized users.
- FIA_USB.1 requires associating the identity and the role with the subjects acting for the authenticated user.
- FMT_MTD.1/Admin restricts the creation, clearing and deletion of Authentication Reference Data to the role Administrator.
- FMT_MTD.1/User restricts the ability to modify the Reference authentication data the user to which belongs this security attribute.

The security objective **O.Roles** "Roles known to TOE" is implemented by the SFR FMT_SMR.2 which requires the TOE to provide at least the HSM Admin, the Security Officer, the Crypto User roles, Unidentified User Role and the Unauthenticated User Role.

The security objective **O.Control_Services** "Access control for services" requires the TOE to restrict the access to its services, depending on the user role, to those services explicitly assigned to the role. Assignment of services to roles shall be either done by explicit action of an HSM Admin or by default. This security objective is provided by the following SFR:

- FDP_ACC.2/Key_Man and FDP_ACF.1/Key_Man require access control to the key management services of the TOE.
- FDP_ACC.2/Oper and FDP_ACF.1/Oper require access control to the cryptographic operation services of the TOE.
- FDP_ACC.2/Mode_Trans and FDP_ACF.1/Mode_Trans require access control to the operational modes of the TOE which limit the available services.
- FDP_IFC.1 and FDP_IFF.1 require access control to services that cause information to flow to and from subjects.
- FMT_SMF.1 lists the security management functions including the management of TSF behaviour FMT_MOF.1.
- FMT_SMR.2 describing the minimum list of roles and restrictions to these roles.
- FMT_MSA.1/Key_Man_1, FMT_MSA.1/Key_Man_2 and FMT_MSA.1/Key_Man_3 require limitation to the management of security attributes of cryptographic keys, key components and CSP describing the available services for these objects.
- FMT_MSA.2, FMT_MSA.3/Key_Man, FMT_MSA.3/Oper and FMT_MSA.3/Mode_Trans describe additional requirements to the management of security attributes to enforce the access control SFP for FDP_ACF.1/Key_Man, FDP_ACF.1/Oper and FDP_ACF.1/Mode_Trans.

The security objective **O.Control_Keys** "Access control for cryptographic keys" requires the TOE to restrict the access to the keys, key components and other CSP according to their security attributes. This security objective is provided by the following SFR:

- FDP_IFC.1, FDP_IFF.1, FDP_ACC.2/Key_Man and FDP_ACF.1/Key_Man require access control to the key keys, key components and other CSP according to their security attributes,

- FDP_IFC.1, FDP_IFF.1, FDP_ACC.2/Oper and FDP_ACF.1/Oper require access control to the keys and other CSP of the TOE according to their security attributes,
- FMT_MSA.1/Key_Man_1, FMT_MSA.1/Key_Man_2 and FMT_MSA.1/Key_Man_3 require limitation to the management of security attributes of cryptographic keys, cryptographic key components and CSP describing the access rights, available services and properties for these objects.
- FMT_MSA.2 ensures that only secure values for cryptographic keys, key components and CSP are accepted for security attributes.
- FPT_STM.1 requires the TSF to provide reliable time stamp that is necessary for FDP_ACF.1/Oper to enforce the use of cryptographic keys in the limits of the Key validity time period defined as security attribute of this key.
- FDP_ACF.1/Mode_Trans, FDP_ACC.2/Mode_Trans and the refinement to the SAR ADV_ARC.1 ensures that operational keys and CSP can not be used outside the operational mode to protect user data.

The security objective **O.Audit** "Audit of the TOE" requires the TOE to provide the capability to detect and create audit records of security relevant events associated with users. This security objective is provided by the following SFR:

- FAU_GEN.1 lists the auditable events to be provided by the TOE,
- FAU_GEN.2 requires to associate auditable event with the identity of the user that caused the event.
- FAU_SAR.1 requires to provide with HSM Admin the capability to read all audit data from the audit records
- FAU_SAR.2 requires limitation of the capability to read the audit data to the HSM Admin.
- FAU_STG.1 requires protection of the stored audit records from unauthorised deletion and prevention of modification.
- FAU_STG.3 requires action if the audit trail exceeds audit trail storage capacity by (1) overwrite the oldest stored audit records.
- FMT_MTD.1/Audit restricts the ability to export and clear the audit data to HSM Admin.
- FPT_STM.1 requires the TOE to provide reliable time stamps for its own use.

The security objective **O.Key_Management** "Management of cryptographic keys" requires the TOE to manage securely cryptographic keys, cryptographic key components and CSP. This security objective is provided by the following SFR:

- FCS_CKM.1/RSA, FCS_CKM.1/TDES, FCS_CKM.1/AES, FCS_CKM.1/ECC, FCS_CKM.1/ECDH, FCS_CKM.2/Import, FCS_CKM.2/Export, and FCS_CKM.4 provide the Endorsed cryptographic functions used by key management.
- FTP_ITC.1 provides a trusted channel for key import and export.
- FDP_ACC.2/Key_Man and FDP_ACF.1/Key_Man provide the access control to the key management functions.
- FDP_IFC.1, FDP_IFF.1, FDP_ITC.2 and FDP_ETC.2 ensure the import and export of cryptographic keys, cryptographic key components and CSP with security attribute, which are associated with these objects for key management.
- FDP_UCT.1 and FDP_UIT.1 requires the TSF to ensure confidentiality and integrity of keys exchanged by import and export of user data including cryptographic keys.
- FMT_SMF.1 list the security management functions and FMT_SMR.2 the roles for key management (i.e. the Security Officer for operational keys).
- FMT_MSA.1/Key_Man_1, FMT_MSA.1/Key_Man_2, FMT_MSA.2 and FMT_MSA.3/Key_Man describes the management of security attributes of cryptographic keys, cryptographic key components and CSP.

- FPT_TDC.1 ensures the consistency of the security attributes of cryptographic keys, cryptographic key components and CSP.

The security objective **O.Key_Export** "Export of cryptographic keys" requires the TOE to export keys with their security attributes and protected in integrity. This is provided by the following SFR:

- FCS_CKM.2/Export requires the TSF to distribute keys by export methods meeting Endorsed standards and provides a refinement for keys exported for manual import.
- FTP_ITC.1 requires the TSF to provide a trusted channel of key export.
- FDP_IFC.1, FDP_IFF.1 and FDP_ETC.2 requires the TSF to export keys unambiguously associated with their security attributes.
- FDP_UCT.1 requires the ability to protect confidentiality of exchanged user data which includes cryptographic keys.
- FDP_UIT.1 requires the ability to protect integrity of exchanged user data which includes cryptographic keys.
- FPT_TDC.1 requires to ensure inter-TSF basic TSF data consistency for exported security attributes of cryptographic keys, key components and CSP.

The security objective **O.Key_Generation** "Generation of cryptographic keys by the TOE" requires the TOE to generate cryptographic strong keys using Endorsed cryptographic key generation algorithms. This is provided by the SFR FCS_CKM.1/RSA, FCS_CKM.1/TDES, FCS_CKM.1/AES, FCS_CKM.1/ECC, FCS_CKM.1/ECDH which requires the use of Endorsed key generation algorithms and FCS_RNG.1 describing requirements for the random number generator needed for key generation. The SFR FMT_MSA.3/Key_Man requires restrictive values of security attributes for cryptographic keys and limits the ability to specify their initial value to the Security Officer.

The security objective **O.Key_Import** "Import of cryptographic keys" requires the TOE to import keys with security attributes and verify their integrity. The TOE shall import secret or private keys in encrypted form or manually using split knowledge procedures only. This is provided by the following SFR:

- FCS_CKM.2/Import requires the TSF to distribute by key import methods meeting Endorsed standards and provides a refinement for manually imported keys.
- FTP_ITC.1 requires the TSF to provide a trusted channel of key import.
- FDP_UCT.1 requires the ability to protect confidentiality of exchanged user data which includes cryptographic keys.
- FDP_UIT.1 requires the ability to protect integrity of exchanged user data which includes cryptographic keys.
- FDP_IFC.1, FDP_IFF.1 and FDP_ITC.2 requires the TSF to import keys unambiguously associated with their security attributes.
- FPT_TDC.1 requires to ensure inter-TSF basic TSF data consistency for imported security attributes of cryptographic keys, key components and CSP.

The security objective **O.Key_Destruction** "Destruction of cryptographic keys" requires the TOE to destruct keys cryptographic key components and other CSP on demand of authorized users or when they will not be used any more in a secure way that no information about these keys is left in the resources storing or handling these objects before destruction. This is provided by the following SFR:

- FCS_CKM.4 requires the TSF to provide Endorsed mechanisms for key destruction.
- FDP_ACC.2/Key_Man and FDP_ACF.1/Key_Man limits key destruction to users in the Security Officer role.

The security objective **O.Check_Operation** "Check for correct operation" requires the TOE to perform regular checks to verify that its components operate correctly including integrity checks of TOE software, firmware, internal TSF data and keys. This is provided by the SFR:

- FPT_TST.1 and FPT_TST.2 requiring TSF self tests.
- FPT_FLS.1 requires the TSF to preserve a secure state when self-test fails.

The security objective **O.Physical_Protect** "Physical protection" requires the TOE to unambiguous detect physical tampering at the cryptographic boundary and respond automatically such that the SFRs are not violated. Upon the detection of tampering, the TOE shall immediately destruct all plaintext secret and private cryptographic keys and CSPs. This is provided by the SFR FPT_PHP.3.

The security objective **O.Prevent_Inf_Leakage** "Prevent leakage of confidential information" requires the TOE to prevent information leakage about secret and private keys and confidential TSF data outside the cryptographic boundary and unintended output confidential user information. This is provided by the following SFR:

- FDP_RIP.2 requires the TOE to ensure that any previous information content of a resource is made unavailable.
- FPT_EMSEC.1 requires to prevent illicit flow of confidential information through any emanation and the "black data" interface.

6.3.2. Dependency Rationale

SFR	Dependencies	Support of the Dependencies
FAU_GEN.1	FPT_STM.1 Reliable time stamps	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 Audit data generation, FIA_UID.1 Timing of identification	FAU_GEN.1, FIA_UID.1
FAU_SAR.1	FAU_GEN.1 Audit data generation	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1 Audit Review	FAU_SAR.1
FAU_STG.1	FAU_GEN.1 Audit data generation	FAU_GEN.1
FAU_STG.3	FAU_STG.1 Protected audit trail storage	FAU_STG.1
FCS_CKM.1/RSA	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.2/Export, FCS_COP.1/ENC_DEC_RSA, FCS_COP.1/SIGN_VERIFY, FCS_CKM.4
FCS_CKM.1/TDES	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.2/Export, FCS_COP.1/ENC_DEC_TDES, FCS_COP.1/MAC, FCS_CKM.4
FCS_CKM.1/AES	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.2/Export, FCS_COP.1/ENC_DEC_AES, FCS_COP.1/MAC, FCS_CKM.4
FCS_CKM.1/ECC	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.2/Export, FCS_COP.1/SIGN_VERIFY, FCS_CKM.4
FCS_CKM.1/ECDH	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.2/Export, FCS_COP.1/SIGN_VERIFY, FCS_CKM.4
FCS_CKM.2/Export	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/RSA, FCS_CKM.1/TDES, FCS_CKM.1/AES, FCS_CKM.1/ECC, FCS_CKM.1/ECDH, FCS_CKM.4
FCS_CKM.2/Import	[FDP_ITC.1 Import of user data without security attributes, or	FDP_ITC.2, FCS_CKM.1/RSA,

SFR	Dependencies	Support of the Dependencies
	FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/TDES, FCS_CKM.1/AES, FCS_CKM.1/ECC, FCS_CKM.1/ECDH, FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	FDP_ITC.2, FCS_CKM.1/RSA, FCS_CKM.1/TDES, FCS_CKM.1/AES, FCS_CKM.1/ECC, FCS_CKM.1/ECDH
FCS_COP.1/ENC_DEC_AES	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	FDP_ITC.2, FCS_CKM.1/AES, FCS_CKM.4
FCS_COP.1/ENC_DEC_TDES	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	FDP_ITC.2, FCS_CKM.1/TDES, FCS_CKM.4
FCS_COP.1/ENC_DEC_RSA	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	FDP_ITC.2, FCS_CKM.1/RSA, FCS_CKM.4
FCS_COP.1/SIGN_VERIFY	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	FDP_ITC.2, FCS_CKM.1/RSA, FCS_CKM.1/ECC, FCS_CKM.1/ECDH, FCS_CKM.4
FCS_COP.1/DIGEST	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data	FDP_ITC.2[123]

[123] FCS_CKM.1 and FCS_CKM.4 can not be mapped to FCS_COP.1/DIGEST since, FCS_COP.1/DIGEST does not use or consume cryptographic keys.

SFR	Dependencies	Support of the Dependencies
	with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	
FCS_COP.1/MAC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	FDP_ITC.2, FCS_CKM.1/TDES, FCS_CKM.1/AES, FCS_CKM.4
FCS_RNG.1	FPT_TST.1 TSF testing	FPT_TST.1
FDP_ACC.2/Key_Man	FDP_ACF.1 Security attribute based access control	FDP_ACF.1/Key_Man
FDP_ACC.2/Mode_Trans	FDP_ACF.1 Security attribute based access control	FDP_ACF.1/Mode_Trans
FDP_ACC.2/Oper	FDP_ACF.1 Security attribute based access control	FDP_ACF.1/Oper
FDP_ACF.1/Key_Man	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	FDP_ACC.2/Key_Man (hierarchical to FDP_ACC.1), FMT_MSA.3/Key_Man
FDP_ACF.1/Mode_Trans	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	FDP_ACC.2/Mode_Trans (hierarchical to FDP_ACC.1), FMT_MSA.3/Mode_Trans
FDP_ACF.1/Oper	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	FDP_ACC.2/Oper (hierarchical to FDP_ACC.1), FMT_MSA.3/Oper
FDP_ETC.2	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.2/Key_Man, FDP_ACC.2/Oper (hierarchical to FDP_ACC.1), FDP_IFC.1
FDP_IFC.1	FDP_IFF.1 Simple security attributes	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 Subset information flow control, FMT_MSA.3 Static attribute initialisation	FDP_IFC.1, FMT_MSA.3/Key_Man
FDP_ITC.2	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], [FTP_ITC.1 Inter-TSF trusted	FDP_ACC.2/Key_Man, FDP_ACC.2/Oper (hierarchical to FDP_ACC.1),

SFR	Dependencies	Support of the Dependencies
	channel, or FTP_TRP.1 Trusted path], FPT_TDC.1 Inter-TSF basic TSF data consistency	FTP_ITC.1, FPT_TDC.1, FDP_IFC.1
FDP_UCT.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]	FDP_ACC.2/Oper (hierarchical to FDP_ACC.1), FTP_ITC.1, FDP_IFC.1
FDP_UIT.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]	FDP_ACC.2/Oper (hierarchical to FDP_ACC.1), FTP_ITC.1, FDP_IFC.1
FDP_RIP.2	No dependencies	N/A
FIA_AFL.1/HA	FIA_UAU.1 Timing of authentication	FIA_UAU.1
FIA_AFL.1/NON_HA	FIA_UAU.1 Timing of authentication	FIA_UAU.1
FIA_ATD.1	No dependencies	N/A
FIA_UAU.1	FIA_UID.1 Timing of identification	FIA_UID.1
FIA_UAU.6	No dependencies	N/A
FIA_UAU.7	FIA_UAU.1 Timing of authentication	FIA_UAU.1
FIA_UID.1	No dependencies	N/A
FIA_USB.1	FIA_ATD.1 User attribute definition	FIA_ATD.1
FMT_MOF.1/SO	FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions	FMT_SMR.2 (hierarchical to FMT_SMR.1), FMT_SMF.1
FMT_MSA.1/Key_Man_1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions	FDP_ACC.2/Key_Man, FDP_ACC.2/Oper (hierarchical to FDP_ACC.1), FMT_SMR.2 (hierarchical to FMT_SMR.1), FMT_SMF.1
FMT_MSA.1/Key_Man_2	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles,	FDP_ACC.2/Key_Man, FDP_ACC.2/Oper (hierarchical to FDP_ACC.1) FMT_SMR.2 (hierarchical to

SFR	Dependencies	Support of the Dependencies
	FMT_SMF.1 Specification of Management Functions	FMT_SMR.1), FMT_SMF.1, FDP_IFC.1
FMT_MSA.1/Key_Man_3	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions	FDP_ACC.2/Key_Man, FDP_ACC.2/Oper (hierarchical to FDP_ACC.1) FMT_SMR.2 (hierarchical to FMT_SMR.1), FMT_SMF.1, FDP_IFC.1
FMT_MSA.2	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles	FDP_ACC.2 (all iterations, hierarchical to FDP_ACC.1), FMT_MSA.1/Key_Man_1, FMT_MSA.1/Key_Man_2, FMT_SMR.2 (hierarchical to FMT_SMR.1), FDP_IFC.1
FMT_MSA.3/Key_Man	FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles	FMT_MSA.1/Key_Man_1, FMT_MSA.1/Key_Man_2, FMT_SMR.2 (hierarchical to FMT_SMR.1)
FMT_MSA.3/Oper	FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles	FMT_SMR.2 (hierarchical to FMT_SMR.1)[124]
FMT_MSA.3/Mode_Trans	FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles	FMT_SMR.2 (hierarchical to FMT_SMR.1)[125]
FMT_MTD.1/Admin	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	FMT_SMR.2 (hierarchical to FMT_SMR.1), FMT_SMF.1
FMT_MTD.1/User	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	FMT_SMR.2 (hierarchical to FMT_SMR.1), FMT_SMF.1
FMT_MTD.1/Audit	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	FMT_SMR.2 (hierarchical to FMT_SMR.1), FMT_SMF.1
FMT_SMF.1	No dependencies	No dependencies
FMT_SMR.2	FIA_UID.1 Timing of identification	FIA_UID.1
FPT_EMSEC. 1	No dependencies	No dependencies
FPT_FLS.1	No dependencies	No dependencies
FPT_PHP.3	No dependencies	No dependencies

[124] FMT_MSA.1 is not mapped to FMT_MSA.3/Oper because, Cryptographic Operations SFP does not have user manageable security attributes.
[125] FMT_MSA.1 is not mapped to FMT_MSA.3/Mode_Trans because, Mode Transition SFP does not have user manageable security attributes.

SFR	Dependencies	Support of the Dependencies
FPT_STM.1	No dependencies	No dependencies
FPT_TDC.1	No dependencies	No dependencies
FPT_TST.1	No dependencies	No dependencies
FPT_TST.2	FPT_FLS.1 Failure with preservation of secure state	FPT_FLS.1
FTP_ITC.1	No dependencies	No dependencies

Table 9: Dependencies Between the SFR for the TOE

6.3.3. Security Assurance Requirements Rationale

EAL4 is applicable in those circumstances where developers or users require high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

The selection of component ADV_IMP.2 provides a higher assurance for the implementation of the TOE especially for the absence of unintended functionality.

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE. In the particular case of a cryptographic module the TOE implements security mechanisms in hardware which details about the implementation, (e.g., from design, test and development tools) may make such attacks easier. Therefore, in the case of a cryptographic module, maintaining the confidentiality of the design and protected manufacturing is very important. Therefore ALC_DVS.2 was selected.

The selection of the component AVA_VAN.5 provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential.

The selection of the component ALC_FLR.2 provides ability to act appropriately upon security flaw reports from TOE users, and to know to whom to send corrective fixes.

The component ADV_IMP.2 has the following dependencies:

- ADV_TDS.3 Basic modular design
- ALC_TAT.1 Well-defined development tools
- ALC_CMC.5 Advanced support

ADV_TDS.3 and ALC_TAT.1 are met in the EAL4 assurance package. ALC_CMC.5 is added to the chosen security assurance package in order to fulfil the dependency.

The component ALC_DVS.2 has no dependencies.

The component AVA_VAN.5 has the following dependencies:

- ADV_ARC.1 Security architecture description
- ADV_FSP.2 Security-enforcing functional specification
- ADV_TDS.3 Basic modular design

- ADV_IMP.1 Subset of the implementation of the TSF
- AGD_OPE.1 Operational user guidance
- AGD_USR.1 Preparative procedures

The component ALC_FLR.2 has no dependencies.

All of these are met or exceeded in the EAL4 assurance package.

7. TOE Summary Specification

7.1. TOE Security Functions

7.1.1. Cryptographic Operations and Key Management

The TOE provides the following cryptographic operation capabilities:

- Cryptographic Key Generation
  - RSA 1024-4096 bits key pairs in accordance with FIPS PUB 186-3.
  - TDES 168 bits keys in accordance with NIST SP 800-67.
  - AES 128, 192 and 256 bits keys in accordance with FIPS PUB 197.
  - Elliptic Curve P-192, P-224, P-256, P-384, P-521 key pairs in accordance with FIPS PUB 186-3 and ANSI X9.62.
  - EC Diffie-Hellman Key Agreement curves P-192, P-224, P-256, P-384, P-521 curves in accordance with NIST SP 800-56A.
- Random Number Generation
  - Shannon entropy of greater than 7.9999 bits per octet based on a 2^{64} bit data set.
  - TRNG which meets NIST SP 800-90B requirements.
- Cryptographic Key Distribution
  - Manual key distribution is performed using split knowledge procedures or key wrapping.
  - Electronic key distribution is performed using a proprietary secure channel protocol that is established between the TOE and a key storage smart card.
- Cryptographic Key Destruction
- Data Encryption and Decryption
  - AES 128, 192 and 256 bits, ECB and CBC modes, in accordance with FIPS PUB 197.
  - TDES 168 bits, ECB and CBC modes, in accordance with NIST SP 800-67.
  - RSA 1024-4096 bits key pairs, in accordance with RSAES-OAEP from PKCS#1 v2.1.
- Signature Generation and Verification
  - RSA 1024-4096 bits with MD5, SHA-1, SHA-256, SHA-384, SHA-512 (PKCS #1 v1.5)
  - RSA PSS 1024-4096 bits with SHA-1, SHA-256, SHA-384, SHA-512 (PKCS #1 PSS)
  - DSA 1024-3072 bits with SHA-1, SHA-256, SHA-384, SHA-512 (FIPS PUB 186-3)
  - ECDSA curves P-192, P-224, P-256, P-384 and P-521 with SHA-1, SHA-256, SHA-384 and SHA-512 (FIPS PUB 186-3)
- Message Digest Generation and Verification
  - MD5, 128 bits (RFC 1321)
  - SHA-1, 160 bits (FIPS PUB 180-4)
  - SHA-224, 224 bits (FIPS PUB 180-4)
  - SHA-256, 256 bits (FIPS PUB 180-4)
  - SHA-384, 384 bits (FIPS PUB 180-4)
  - SHA-512, 512 bits (FIPS PUB 180-4)
- MAC Generation and Verification
  - HMAC with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (FIPS PUB 198-1)

- TDES CMAC with 168 bits keys (NIST SP 800-38B)
- AES CMAC with 128, 192 and 256 bits keys (NIST SP 800-38B)

7.1.2. User Identification and Authentication

The Identification and Authentication security function provides ability to the users to authenticate themselves in order to access restricted functions of the TOE. Access control in the TOE is based upon statically defined user roles which are listed below:

- HSM Admin
- Security Officer
- Crypto User
- HSM Operator

Only a single user role can be assigned to a TOE user.

The TOE security functions which do not require identification of the above roles are accessible by unidentified and unauthenticated(anonymous) users.

The TOE associates the following security attributes to a subject that acts on the user's behalf:

- User Identity
- User Role
- Challenge

User Role attribute of the subject is set to Unidentified initially. It is changed to Unauthenticated after successful user identification and it is changed to a role that user has selected for the authentication session, if authentication or re-authentication is successful and if user is authorized for this role.

Identification and authentication to the TOE is possible using one of the following methods:

- Using a smartcard and passphrase to authenticating to the TOE locally. This is the only method for HSM Admin users to access to the restricted security functions and can optionally used by Security Officer, Crypto User and HSM Operator users.
- Using a username and passphrase to authenticating locally or remotely. This method can not be used by HSM Admin users.

Each TOE user has a *User Login Try Counter* assigned, which increments in case of unsuccessful login attempts, until reaching to the *User Login Try Limit,* and resets when correct authentication information is provided, only if, it has not reached to the *User Login Try Limit*. If it is reached to the *User Login Try Limit*, the associated user is blocked for authentication. In such a case, *User Login Try Counter* of a Crypto User can be zeroized either the associated Security Officer. User Login Try Counter of a Security Officer user can only be zeroized by the HSM Operator. User Login Try Counter of a HSM Operator user can only be zeroized by the HSM Admin. In case of a HSM Admin authentication block, the TOE must be re-initialized. *User Login Try Limit* for all users is statically defined as fifteen(15).

All authorized users have right to modify their reference authentication data by changing their passphrase or issuing/removing a smartcard associated with their user account.

The TOE provides status messages through its LCD/Keypad interface and Status interface to inform the user while the authentication is in progress.

The TOE imposes 5 seconds of waiting time between login attempts.

Re-authentication is required when changing to a role not selected for the current valid authentication session or after power cycling the TOE.

The TOE allows user authentication only if it is successfully performed the self tests at least once after it is powered up, according to FPT_TST.2 meaning, it is not in the secure blocking state (FPT_FLS.1).

7.1.3. Protection of User Data

All cryptographic keys, key components, CSPs and user information are stored with their security attributes, within the associated data structures and they are always imported and exported with their security attributes.

All key objects are stored, imported and exported with the following security attributes:

- Key identity
- Key entity
- Key type
- Key usage type
- Key access control rules
- Key validity time period

Encrypted secret and private key objects are stored, imported and exported with the additional, Identity of the key encryption key security attribute.

Key components are stored, imported and exported with the following security attributes:

- Identity of the key component
- Key entity
- Key entry method

All CSPs are stored, imported and exported with the following security attributes:

- Identity of the CSP
- CSP usage type
- CSP access control rules

All user subjects are stored with the following security attributes:

- Identity of the user the subject is bind to
- Role of the user

The TOE implements a role based access control mechanism for accessing to all cryptographic keys, key components, CSPs and all user subjects; makes sure that the authorized users have access only to allocated data. The TOE checks Key Usage Type and CSP Usage Type attributes to make sure that cryptographic keys and CSPs are only used in allowed cryptographic operations by users in Crypto User and Security Officer roles.

All operations among subjects and objects are controlled in accordance with the mode variable of the TOE. While a user in Security Officer role can set the mode variable to Security Officer mode, Crypto User mode, Key/CSP Entry mode and Self-Test mode; the applicable modes for a user in Crypto User role are Crypto User mode and Key/CSP Entry mode. The TOE enters the Error Mode

from any mode of operation except Power-Off mode, in case of a Self-Test error. It does not respond on any interfaces, does not perform any cryptographic operations, drives the self-test failure bit of the status interface and outputs self-test error code which indicates the failed self-tests via the LCD/Keypad port. All cryptographic operations and access to objects are prohibited in Error Mode, Self-Test Mode and Power-Off Mode.

The TOE is able to transmit and receive user data in a manner protected from unauthorised disclosure and modification by using proprietary and non-proprietary data transfer protocols. The mentioned protocols enable the TOE to determine partial deletion, insertion and replay of the protected user data on receipt.

The TOE zeroizes a memory space before allocating it to a data object, in order to make sure, there are no residual information of a previously stored data object, in the subject memory space.

7.1.4. Audit

The TOE generates audit logs of various auditable events and associates them with the authenticated user and with a reliable time stamp. The TOE provides the capability for HSM Admin users to read, view and export all the recorded logs. The TSF prevents the HSM Admin user from modifying or deleting audit logs. When audit trail becomes full, the TOE overwrites the oldest stored audit records with the new ones.

7.1.5. Management of TSF and Protection of TSF Data

The TOE provides capability for the HSM Admin user to perform the following management functions:

- Management of security functions behaviour.
- Management of reference authentication data.
- Management of audit data.
- Management of security attributes of cryptographic keys, cryptographic key components and CSP.

The TOE provides capability for the Security Officer user to change default values, specify alternative initial values to override the default values and query the following security attributes:

- Identity of the key
- Key entity
- Key type of the key
- Key usage type
- Key validity time period
- Identity of the key component
- Key entity of the key component
- Key entry method
- Identity of the CSP
- CSP usage type

The default values and alternative initial values can only be changed if the new data entered by the Security Officer is considered secure by the TOE.

Only the following security attributes can be modified by the Security Officer:

- Key access control rules
- CSP access control rules

Users in Crypto User role can be created and assigned to a partition or can be deleted by Security Officer users.

7.1.6. TSF Protection

7.1.6.1. Physical Protection

The TOE is in system on module (SOM) form with a card edge connection and tamper resistive mesh layers on top and bottom. The gap between the electronic components and tamper resistant layers are filled with hard, opaque potting material (epoxy resin).

Security monitor of the TOE continuously generates random data, transmits it via top and bottom mesh layers and expects the data to return back. In case of any intervention that will break physical integrity of the mesh layers and prevent the generated random data to return back, the security monitor generates an alarm that cause secure memory to immediately zeroized the Internal Key Encryption Key which is used to encrypt other keys and CSPs.

Besides direct physical interventions, the security monitor also check battery power input, main power input and environmental temperature continuously. Any of the following conditions cause tamper response:

- Out of range battery voltage.
- Out of range main supply voltage.
- Out of range storage temperature.
- Out of range operational temperature.
- Power fluctuation.
- Total power loss (battery and main supply).

In case of tamper detection, the TOE enters a secure error state, does not respond on any interfaces, does not perform any cryptographic operations and drives the tamper detection bit of the status interface.

7.1.6.2. TOE Emanation

Schematics and printed circuit board of the TOE hardware is designed to limit conducted and radiated emissions in order to avert possible attack attempts.

Additionally, algorithm and platform specific design and implementation techniques are used to develop the cryptographic IP cores which makes it very complicated to obtain meaningful information using the radiated emissions.

7.1.6.3. Self Test

The TOE performs the following self-tests:

- Hardware Self-Tests: These tests are performed to check health status of the various hardware components of the TOE.
- Firmware Self-Tests: These tests are performed to check integrity and authenticity of the firmware packages of the TOE, including FPGA bitstream files.
- Cryptographic Self-Tests: Known answer tests (KAT) are performed to check health status of the cryptographic software and hardware components.
- TRNG Self-Tests: A pre-defined size of random numbers are generated and statistical tests are applied to check health status of the TRNG.
- Key Tests: Integrity of the master keys (and authenticity for some keys) are tested.

All the listed self-tests are performed

- during power-up
- after firmware update.

TRNG Self-tests are performed continuously during random number generation.

In case of a self-test failure, the TOE enters a secure error state, does not respond on any interfaces, does not perform any cryptographic operations, drives the self-test failure bit of the status interface, outputs self-test error code which indicates the failed self-tests via the LCD/Keypad port and generates an audit record which reports the incident.

7.1.6.4. Data Consistency

The TOE has mechanisms to consistently interpret and preserve security attributes of cryptographic keys, key components and CSPs during import and export operations.

The following security attributes are never changed by the TOE during import and export operations:

- For cryptographic keys:
  - Identity of the key
  - Key entity
  - Key type
  - Key usage type
  - Key validity time period
- For key components:
  - Identity of the key component
  - Key entity
  - Key entry method
- For CSPs:
  - Identity of the CSP
  - CSP usage type

The TOE stops import operation and reports its status in case of an identity conflict between a stored cryptographic key, key component or CSP and the object being imported.