Federal Office
for Information Security

Common Criteria Protection Profile

Cryptographic Modules, Security Level “Enhanced”

Common Criteria

BSI-CC-PP-0045

Endorsed by the
Bundesamt für Sicherheit in der Informationstechnik

Foreword

This ‘Protection Profile - Cryptographic Modules, Security Level „Enhanced“ - is issued by Bundesamt für Sicherheit in der Informationstechnik, Germany.

The document has been prepared as a Protection Profile (PP) following the rules and formats of Common Criteria version 3.1.

Correspondence and comments to this Protection Profile should be referred to:

CONTACT ADDRESS

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
D-53175 Bonn, Germany
Tel: 49 228 99 9582-111
Email: zertifizierung@bsi.bund.de
Internet: http://www.bsi.bund.de

Variables

Name	Value	Display
File name and sizes	Set automatically	pp0045_v101.doc (1546752 Byte)
Last Version	1.01	1.01
Date	24th July 2008	24th July 2008
Classification	unclassified	unclassified
Authors	Wolfgang Killmann, Kerstin Lemke-Rust	Wolfgang Killmann, Kerstin Lemke-Rust

This page is intentionally left blank.

Table of Content

1 PP Introduction

1.1 PP Reference

Title: Cryptographic Module, Security Level “Enhanced”
Sponsor: BSI
Editors: T-Systems GEI GmbH, Prüfstelle
CC Version: 3.1
Assurance Level: EAL 4 augmented
General Status: working draft
Version Number: 1.01
Registration: BSI-CC-PP-0045
Keywords: Cryptography

1.2 PP Overview

This protection profile describes the security requirements for cryptographic modules which provide Endorsed cryptographic security functions with secret or private cryptographic keys and is resistant against high attack potential.

The cryptographic module must not provide non-Endorsed cryptographic security functions. If a cryptographic module uses only asymmetric cryptographic algorithms with public keys (e.g., like a signature-verification application) some of the security requirements required by this protection profile may be not necessary relevant (e.g., side channel resistance).

1.3 TOE Description

TOE Definition

The Target of Evaluation (TOE) is a cryptographic module that implements Endorsed cryptographic security functions. These Endorsed cryptographic security functions protect the confidentiality or the integrity or both of user data according to a security policy of an IT system. The TOE uses, manages and protects the cryptographic keys for these Endorsed cryptographic security functions.

This PP is indented for cryptographic modules, which implement secret or private keys. The cryptographic modules must not provide non-Endorsed cryptographic security functions.

The TOE is physically defined as a set of hardware and software and/or firmware, which is contained within the cryptographic boundary.

The TOE is logically defined by the provided security functions depending on the implemented cryptographic algorithms and protocols. The cryptographic algorithms and protocols provide at least one of the following security functions based on cryptographic key management.

1. Encryption to protect the confidentiality of information represented in ciphertext data, which are known to an attacker if only the decryption key for these data is kept confidentially[1]. The encryption key shall be assigned to the authorized receiver of the information and in case of asymmetric cryptographic algorithm may be public.
2. Decryption to support the protection in confidentiality of information represented in ciphertext data. The decryption key for these data shall be kept confidentially.
3. Digital signature creation to support the services origin authentication, data integrity, and non-repudiation for the signed data to the signer. The signature-creation key shall be kept private.
4. Digital signature verification, which allow to detect any modification of the signed data and to proof the origin and the integrity of unmodified signed data. The signature-verification key shall be authentically assigned to the holder of the signature-creation key and may be public available to the verifier.
5. Generation and the verification of Message Authentication Codes to detect modification of the related data by anybody not knowing the message authentication key used for the Message Authentication Code of these data.
6. Prove of its own identity to an external entity based on the knowledge of a private key without revealing this secret to the verifier.
7. Verification of the identity of an external entity based on a public key assigned to this entity.

The TOE manages the cryptographic keys necessary for its implemented cryptographic algorithms and protocols. The cryptographic key management controls the access and the use of the cryptographic keys by the Endorsed cryptographic functions. The cryptographic key management includes at least one of the following techniques:

1. Generation of cryptographic keys using a random number generator and implementing the key generation algorithms depending on the intended use of the keys.
2. Import of cryptographic keys in encrypted form or cryptographic key components using split-knowledge procedures.
3. Key agreement protocols establishing common secrets with external entities.

The TOE may export cryptographic keys to authorized external entities while protecting the confidentiality and the integrity as required for the intended use of the cryptographic key.

In many cases the mutual authentication of communicating entities and the key agreement are combined to initiate secure communication between trusted parties protecting the confidentiality and integrity of the transmitted data.

Method of use

The IT system is assumed to protect the confidentiality, the integrity and the availability of the information processed, stored and transmitted according to the IT system security policy. The IT system will use the TOE to protect user data during transmission over channels or storage on media to which unauthorised user have access to. The IT systems security policy defines the protection of the confidentiality or the integrity or both of the user information. It

[1] In case of a symmetric encryption algorithm the confidentiality of the decryption key implies the confidentiality of the encryption key because they are identical or the decryption key can be easily derived from the encryption key.

is expressed by a security attribute with values “confidential”, “integrity sensitive” and “confidential and integrity sensitive” assigned to the user information and their user data. The need of protection for the user information defines the need for cryptographic protection of their user data provided by the TOE.

In case of encryption and message authentication with message recovery the information contained in cryptographically protected data cannot be processed until the cryptographic protection is removed. In case of message authentication with appendix the information contained in the cryptographically protected data may be directly processed but the cryptographic integrity protection should be created for the newly generated data. The TOE verifies the data integrity or origin of data received before output them to further processing by the IT system. The protection of the user data passes over to the protection of the cryptographic keys. The TOE IT environment ensures the availability of the user data and the cryptographic keys.

The TOE provides the following types of interfaces/ports[2]:

- 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).
- 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.

The key interfaces used for the input and output of plaintext cryptographic key components, CSPs and the authentication interface used for input of confidential authentication data, are logically separated from all other interfaces. All data output via the data output interface is inhibited when the TOE is in an error mode or in power-up self-test mode.

[2] A port is a physical implementation of an logical interface that provides access to the module for physical signals, represented by logical information flows.

2 Conformance Claims

This protection profile claims conformance to

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and General Model, Version 3.1, Revision 1, September 2006, CCMB-2006-09-001

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security Functional Requirements, Version 3.1, Revision 2, September 2007, CCMB-2007-09-002

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security Assurance Requirements, Version 3.1, Revision 2, September 2007, CCMB-2007-09-003

as follows:

- Part 2 extended,
- Part 3 conformant,
- Package conformant to EAL4 augmented with ADV_IMP.2, ALC_CMC.5, ALC_DVS.2, and AVA_VAN.5.

This protection profile does not claim conformance to any other protection profile.

The conformance claim for this PP is “strict-PP”. Demonstrable conformance is not allowed for this PP.

3 Security Problem Definition

3.1 Introduction

This protection profile describes the security problem for cryptographic modules, which may provide a wide range of cryptographic security functions depending on the intended protection of the user data. This intended protection of primary assets is addressed by organisational security policies. The TOE protects the user data in confidentiality and integrity. The use of cryptographic methods implies specific threats, which are common for all TOEs as cryptographic modules.

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.

Subjects

The following roles are defined in the context of this protection profile. A security target conform to this protection profile shall use all except the Maintenance personal if no maintenance functionality is provided by the TOE of the ST.

Roles	**Description**
Administrator	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.
Crypto officer[3]	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.
End User	An authorized user assumed to perform general security services, including cryptographic operations and other Endorsed security functions.
Maintenance Personal	An authorized user assumed to perform physical maintenance and/or logical maintenance services (e.g., hardware/software diagnostics).
Unidentified User	A user not being identified.
Unauthenticated User	An identified user not being authenticated.

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: Administrator role, Crypto Officer role, End User role or Maintenance Personal role. The roles may be refined, e.g., the administrator role may be split into a User administrator for user management (i.e. creation and deletion of user accounts), IT administrator (i.e. management of non-cryptographic functions of the TOE except user and audit management) and the Auditor role (i.e. configuration of the audit function, reading, exporting and deleting audit trails).

A user in the End 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,

Objects

[3] The "cryptographic administrator" is some times called "crypto officer" in the guidance documentation.

The following objects are defined in the context of this protection profile. The security target conform to this protection profile may use all or a subset of them depending on the implemented Endorsed cryptographic security functions.

Object	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
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 (MAC)	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.

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

Furthermore cryptographic keys, key components and CSP may be distinguished as

- Operational if they are used to protect user data,
- Maintenance if they are used for maintenance of the TOE by maintenance personal only.

Note that data used internally by known answer self test of the TOE instead of cryptographic keys are seen neither as operational nor as maintenance keys (CSP).

Operations

The following operations are defined in the context of this protection profile. The security target conform to this protection profile may use all or a subset of them depending on the implemented Endorsed cryptographic security functions.

Operation	**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
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	Input of user data with or without security attributes to the red area

Operation	Description
data	of the IT system cryptographically unprotected by cryptographic security functions of the TOE
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[4]

3.2 Assumptions

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.

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.

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.

A.Audit_Analysis Analysis of audit trails

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

[4] E.g., if an encryption key *A* is encrypted with a key-encryption key *B* than the *B* is “used as key” (not *A*).

A.Availability Availability of keys

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

3.3 Threats

The cryptographic modules protect user data as primary assets by means of cryptographic functions. The cryptographic functions, their keys and CSP itself are object of attacks. These attacks are described here.

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, which enables attacks against the confidentiality or integrity of user data protected by these CSPs or the TSF using these CSPs as TSF data.

T.Modif_CSP Modification of integrity sensitive CSP

An attacker with high attack potential may modify integrity sensitive CSP like permanent stored public keys and therefore compromise the confidentiality or integrity of user data protected by these CSPs or the TSF using these CSPs as TSF data.

T.Abuse_Func Abuse of function

An attacker with high attack potential may use TOE functions intended for installation, configuration or maintenance 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.

T.Inf_Leakage Information leakage

An attacker with high attack potential may observe and analyse 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.

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.

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.

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.

3.4 Organisational Security Policies

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.

OSP.Resist_High Resistance against high attack potential

The TOE shall resist attacks with high attack potential.

OSP.I&A Identification and authentication of users

All users must be identified and authenticated prior to accessing any controlled resources with the exception of read access to public objects.

OSP.Access Access control of TOE functions

The TOE must limit the extent of each user’s abilities to use the TOE functions in accordance with the TSP.

OSP.Account Accountability of users

The users of the TOE shall be held accountable for their actions within the system.

OSP.Roles Roles

The authorized administrator, cryptographic administrator (crypto officer) and end users shall have separate and distinct roles associated with them. If the TOE provides maintenance functionality the maintenance personal shall have distinct roles associated with them and separate from other roles.

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.

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.

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.

4 Security Objectives

4.1 Security Objectives for the TOE

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.

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.

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”.

O.Roles Roles known to TOE

The TOE shall provide at least the Administrator, the Cryptographic Administrator, and the End User roles. If the TOE provides maintenance functionality the TOE shall provide Maintenance Personal role.

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 an Administrator or by default.

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.

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.

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.

O.Key_Generation Generation of cryptographic keys by the TOE

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

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.

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 Cryptographic Administrator or by default.

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.

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 authorised user, and at the conditions installation and maintenance.

O.Physical_Protect Physical protection

The TOE shall resist physical attacks with high attack potential.

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.

4.2 Security Objectives for the Operational Environment

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.

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.

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.

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.

OE.Personal Personal security

The Administrator, Cryptographic Administrator, End User roles, and - if supported by the TOE - the Maintenance Personal role shall be assigned with distinct authorized persons. For manual key import at least two different authorized persons are assigned to cryptographic administrator role.

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.Resist_High	OSP.I&A	OSP.Access	OSP.Account	OSP.Roles	OSP.Endorsed_Crypto	OSP.Key_Man	OSP.Key_Personal	T. Compro_CSP	T.Modif_CSP	T.Abuse_Func	T.Physical_Tamper	T.Inf_Leakge	T.Malfunction	T.Masquerade	A.User_Data	A.Data_Sep	A.Key_Generation	A.Audit_Analysis	A.Availability
O.I&A		x	x		x				x							x					
O.Control_Services				x								x									
O.Control_Keys				x					x	x	x					x					
O.Roles				x		x						x									
O.Audit					x																
O.Key_Export								x	x	x	x										
O.Key_Generation								x		x											
O.Key_Import								x	x	x	x										
O.Key_Management								x	x	x	x										
O.Key_Destruction								x		x											
O.Red-Black-Sep										x						x					
O.Check_Operation											x				x						
O.Endorsed_Crypto	x						x														
O.Physical_Protect		x											x								
O.Prevent_Inf_Leakage		x								x				x							
OE.Assurance		x																			
OE.Key_Generation								x		x									x		
OE.Red-Black-Sep																	x	x			
OE.Audit_Analysis					x															x	
OE.Personal						x			x			x									
OE.Key_Availabilty	x																				x

Table 1: Security Objective 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_Availabilty ensures that IT system protects the availability of the user data and the cryptographic keys outside the cryptographic module.

The organisational security policy **OSP.Resist_High** “Resistance against high attack potential” requires the TOE to resist attacks with high attack potential. This is ensured by the security objective for the development environment OE.Assurance (cf. to last sentence). The security objectives O.I&A, O.Physical_Protect and O.Prevent_Inf_Leakage address directly the resistance against attacks with high attack potential.

The organisational security policy **OSP.I&A** “Identification and authentication of users” addresses identification and authentication of all users prior to accessing any controlled resources with the exception of public objects. This is directly ensured by the security objective O.I&A.

The organisational security policy **OSP.Access** “Access control of TOE functions” address the limitation of the extent of each user’s abilities to use the TOE functions in accordance with the TSP. The security objective O.Control_Services requires the TOE shall restrict the access to its services, depending on the user role, to those services explicitly assigned to this role which are provided according to the security objective O.Roles. The security objective O.Control_Keys limits user’s ability to use the TOE functions to ensure the cryptographic security as part of the TSP.

The organisational security policy **OSP.Account** “Accountability of users” requires the users be held accountable for their actions within the system. The TOE security is required to establish the identity of the users by the objective O.I&A and to provide the capability to detect and create audit records of security relevant events associated with users by the objective O.Audit. The security objective for the IT environment OE.Audit_Analysis ensures reviews of the audit trails generated and exported from the TOE making authenticated users accountable for their actions related to the TOE.

The organisational security policy **OSP.Roles** “Roles” addresses separate and distinct roles for authorized administrator, cryptographic administrator and end users. The security objective O.Roles requires the TOE to implement them and the security objective OE.Personal requires the IT environment to use them.

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 threat **T.Abuse_Func** “Abuse of function” addresses the misuse of TOE functions intended for installation, configuration or maintenance 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 Administrator, the Cryptographic Administrator, the End User roles, and Maintenance Personal if the TOE supports maintenance functionality. The Administrator, Cryptographic Administrator, End User roles and Maintenance Personal if the TOE supports maintenance functionality, will be assigned to authorized distinct persons according to the security objective for the IT environment OE.Personal.

The threat **T.Inf_Leakage** “Information leakage” describes that an attacker may observe and analyse 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.

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.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_Availabilty.

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.

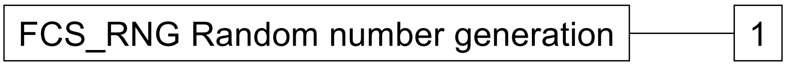
5 Extended Components Definition

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. The requirements address the type of the random number generator as defined in AIS 20/31[5] and quality of the random numbers.

Component levelling:



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.

[5] New version currently under development

Component levelling:

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 identified that should be auditable if FAU_GEN Audit data generation is included in the PP/ST.

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

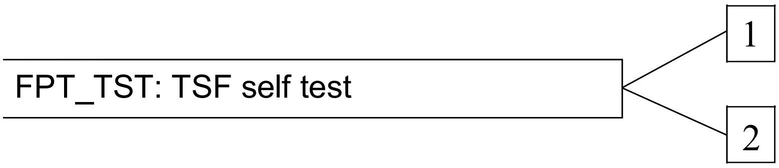
The following addition are made to “TSF self test (FPT_TST)” in Common Criteria, Part 2 to require the self-testing of TSF and of the integrity of the TSF-data and TSF-executable code. FPT_TST.2 requires the behaviour of TSF during self-testing and the actions to be performed by TSF in dependency of 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 authorised 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 levelling:



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 authorised 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 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 self-testing 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 TSF 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 CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph 2.1.4 of part 2 of the CC. Each of these operations is used in this PP.

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 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

The TOE shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below (Common Criteria Part 2).

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*assignment: cryptographic key generation algorithm*] and specified cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: [assignment: *list of* ***Endorsed*** *standards*].

Application note 1: The ST writer shall perform the missing operations in the element FCS_CKM.1.1. If the TOE implements more than one key generation method the component shall be iterated to describe all key generation methods under evaluation. The assignment of the standard shall indicate Endorsed algorithms only. All keys used for Endorsed functions shall be generated by Endorsed key generation algorithms. Endorsed key generation algorithms use Endorsed random generators only.

FCS_CKM.2/Import Cryptographic key distribution

Hierarchical to: No other components.

Dependencies: [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.2.1/Import The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method *key entry*[6] that meets the following: [assignment: *list of* ***Endorsed*** *standards*].

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 form 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.

Application note 2: The ST writer shall perform the missing operations in the element FCS_CKM.2.1/Import. The ST writer shall describe all methods of key import provided by the TOE. If the TOE implements more than one method of key import the component should be iterated. The assignment of the standards shall assign Endorsed algorithms only. Manual key input may be used, e.g., for secret transport keys for symmetric encryption of keys.

FCS_CKM.2/Export Cryptographic key distribution

Hierarchical to: No other components.

Dependencies: [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

[6] [assignment: *cryptographic key distribution method*]

FCS_CKM.2.1/Export The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method *key export*[7] that meets the following: [assignment: *list of* ***Endorsed*** *standards*].

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 form 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 hall be integrity protected using an Endorsed cryptographic algorithm.

Application note 3: The ST writer shall perform the missing operations in the element FCS_CKM.2.1/Export. The ST writer shall describe all methods of key export provided by the TOE. The assignment of the standards shall assign Endorsed algorithms only. If the TOE implements more than one method of key import the component should be iterated.

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.
Dependencies: No dependencies.

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, another trusted IT product*] 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*[8].

Application note 4: The ST writer shall perform the missing operation in the element FTP_ITC.1.2. The trusted channel for key import and key export will be established for electronic key distribution.

[7] [assignment: *cryptographic key distribution method*]

[8] [assignment: *list of functions for which a trusted channel is required*]

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [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.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of* ***Endorsed*** *standards*].

Application note 5: The ST writer shall perform the missing operations in the element FCS_CKM.4.1. If the TOE implements more than one key destruction method the component should be iterated. The assignment of the standards shall assign Endorsed algorithms only.

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [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_COP.1.1 The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of* ***Endorsed*** *standards*].

Application note 6: The ST writer shall perform the missing operations in the element FCS_COP.1.1. The assignment of the standards shall assign Endorsed algorithms only. If the TOE implements more than one cryptographic operation the component shall be iterated.

FCS_RNG.1 Random number generation

Hierarchical to: No other components.

Dependencies: FPT_TST.1 TSF testing.

FCS_RNG.1.1 The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid*] random number generator that meet *[selection: Endorsed RNG class]*[9].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment: *a defined quality metric*].

Application note 7: The ST writer shall perform the missing operations in the elements FCS_RNG.1.1 and FCS_RNG.1.2. The ST writer shall describe the requirements for all RNG used in the TOE by FCS_RNG.1, possibly by iterations. Endorsed functions use only Endorsed RNG according to FCS_RNG.1. A physical random number generator (RNG) produces the random number by a noise source based on physical random processes. A non-physical true RNG uses a noise source based on non-physical random processes like human interaction (key strokes, mouse movement). A deterministic RNG uses a random seed to produce a pseudorandom output. A hybrid RNG combines the principles of physical and deterministic RNGs, e.g., a physical RNG with cryptographic post-processing. Endorsed

[9] [assignment: *list of security capabilities*]

functions use only Endorsed RNG according to FCS_RNG.1. The security capabilities for the assignment in FCS_RNG.1.1 are provided by the Endorsed RNG class. If the seed of a DRNG is entered during key generation, shall be entered as key according with FCS_CKM.2. The quality metric of the random numbers should be chosen depending on the RNG type and the intended application of the random numbers. For example, a DRNG used to generate key pairs for qualified electronic signatures shall have to be seeded with minimum 100 bit Min-entropy and for AES keys 128 bit Min-entropy.

User I&A

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

(1) *Identity*,

(2) *Role*,

(3) *Reference authentication data*,

(4) *[assignment: list of additional security attributes]*[10].

Application note 8: The element FIA_ATD.1.1 contains an assignment of the list of security attributes in the bullet (1), (2) and (3) and allows the ST writer to add none or an additional list of security attributes in bullet (4).

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow

(1) Self test according to FPT_TST.2,

(2) *[assignment: list of other TSF-mediated actions]*[11]

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.

Application note 9: The ST writer shall perform the missing operation in the element FIA_UID.1.1 by adding other TSF mediated actions or none of them if the Unidentified User is not allowed to run other TSF mediated actions than self test.

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow

(1) Self test according to FPT_TST.2,

[10] [assignment: *list of security attributes*]

[11] [assignment: *list of TSF mediated actions*]

(2) Identification according to FIA_UID.1,

(3) Selection of [selection: a role, a set of role],

(4) *[assignment: list of other TSF mediated actions]*[12]

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.

Application note 10: The ST writer shall perform the missing operations in the element FIA_UAU.1.1. The list of TSF mediated actions defines the rights assigned to the role Unauthenticated User. Note a role is "a predefined set of rules establishing the allowed interactions between a user and the TOE" (CC part 1, para. 45). The selection in the third bullet allows the ST writer to describe how the user may take the role or the roles for the user session. The selection in the fourth bullet allows the ST writer to add other TSF mediated actions or none of them. The TSF for authentication of the users shall have a high strength of function as required by AVA_SOF.1. For each attempt to use the authentication mechanism the probability shall be less or equal than 10^{-6} that a random attempt will succeed or a false acceptance will occur. For multiple attempts to use the authentication mechanism the probability shall be or equal less than 3×10^{-6} that a random attempt will succeed or a false acceptance will occur.

FIA_UAU.6 Re-authenticating

Hierarchical to: No other components.

Dependencies: No dependencies.

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: *list of other conditions under which re-authentication is required*][13].

Application note 11: The ST writer shall perform the missing operation in the element FIA_UAU.6.1 by adding other conditions or none of them in the third bullet. The use may select a role or a set of roles (if supported by the TOE cf. selection in bullet (3) of the element FIA_UAU.1.1). If the TOE supports the authentication of a user for a set of roles (cf. to FIA_UAU.1.1), the user is authorized the role or the set of roles and successfully authenticated the TSF may bind subjects to the claimed roles. The user may change the role without re-authentication within this set of roles for which the user is authenticated.

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [assignment: *list of feedback*] to the user while the authentication is in progress.

[12] [assignment: *list of TSF mediated actions*]

[13] [assignment: *list of conditions under which re-authentication is required*]

Application note 12: The ST writer shall perform the missing operation in the element FIA_UAU.7.1. The feedback provided to the user must not include (i) any information about the verification authentication data or (ii) any information about failure or success of the authentication attempt before the authentication procedure is finished. The feedback may indicate the left authentication attempts for the selected identification. The feedback after the defined number of unsuccessful authentication attempts has been met or surpassed shall be described in the element FIA_AFL.1.2.

FIA_USB.1 User-subject binding

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

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: list of additional user security attributes]*[14].

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*[15].

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: additional rules for the changing of attributes]*[16].

Application note 13: The ST writer shall perform the missing operation in the elements FIA_USB.1.1 by adding additional security attributes or none of them in the third bullet. The ST writer shall perform the missing operation in the elements FIA_USB.1.3 by adding additional rules or none of them in the fourth bullet. The authentication session is the time between the successful authentication and next re-authentication or logout of the user.

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of*

[14] [assignment: *list of user security attributes*]

[15] [assignment: *rules for the initial association of attributes*]

[16] [assignment: *rules for the changing of attributes*]

acceptable values]] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met or surpassed*[17], the TSF shall [assignment: *list of actions*].

6.1.2 Protection of user data

FDP_ACC.2/Key_Man Complete access control

Hierarchical to: FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.2.1/Key_Man The TSF shall enforce the *Key Management SFP* [18] on

(1) all cryptographic keys, key components, CSP;

(2) *all user subjects* [19]

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.

FDP_ACF.1/Key_Man Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/Key_Man The TSF shall enforce the *Key Management SFP* [20] 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*[21].

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:

[17] [selection: *met, surpassed*]

[18] [assignment: *access control SFP*]

[19] [assignment: *list of subjects and objects*]

[20] [assignment: *access control SFP*]

[21] [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*]

(1) Subject in crypto 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 crypto 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 crypto officer role is allowed to import CSP,

(4) Subject in crypto 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 crypto 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 crypto officer role is allowed to export CSP if the security attribute CSP access control rules of the CSP allows export;

(7) *Subject in crypto officer role is allowed to destruct cryptographic keys, cryptographic key components and CSP;*

(8) *[assignment: other rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]*[22].

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

(1) *Subjects in Maintenance Personal role are allowed to import and destruct maintenance cryptographic keys, key components and CSP;*

(2) *[assignment: additional rules, based on security attributes, that explicitly authorise access of subjects to objects]*[23].

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

(1) Subject in crypto 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 crypto 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 crypto officer rule are not allowed to input operational public root key;

(4) Subjects with other roles than crypto 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;

[22] [assignment: *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*]

(7) *[assignment: other rules, based on security attributes, that explicitly deny access of subjects to objects]*[24].

Application note 14: The ST writer shall perform the missing operation in the element FDP_ACF.1.2, FDP_ACF.1.3 and FDP_ACF.1.4. The operation in the element FDP_ACF.1.2 shall describe

(1) The Key access control rules protecting secret keys, private keys, and CSPs within the cryptographic module from unauthorized disclosure, modification, and substitution,

(2) The Key access control rules protecting public keys within the cryptographic module against unauthorized modification and substitution.

The other rules in the element FDP_ACF.1.2 may address, e.g., the export of public keys. Note if a subject, an object or an operation identified in any rule in the component FDP_ACF.1/Key_Man is not supported by the TOE the access rule is fulfilled obviously. (End of Application note.)

FDP_ACC.2/Oper Complete access control

Hierarchical to: FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.2.1/Oper The TSF shall enforce the *Cryptographic Operation SFP*[25] on

(1) operational cryptographic keys, CSP,

(2) plaintext data, ciphertext data, original data;

(3) *all user subjects* [26]

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.

FDP_ACF.1/Oper Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/Oper The TSF shall enforce the *Cryptographic Operation SFP* [27] 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;

[24] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

[25] [assignment: *access control SFP*]

[26] [assignment: *list of subjects and objects*]

[27] [assignment: *access control SFP*]

(b) *Operational CSP with security attributes: Identity of the CSP, CSP usage type, CSP access control rules,*

(c) *plaintext data, ciphertext data, original data*[28].

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 End User role is allowed to perform cryptographic operation in accordance with the security attributes of the used cryptographic keys and CSP;*

(2) *[assignment: other rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]*[29].

FDP_ACF.1.3/Oper The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

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

(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: other rules, based on security attributes, that explicitly deny access of subjects to objects]*[30].

Application note 15: The ST writer shall perform the missing operation in the element FDP_ACF.1.2/Oper, FDP_ACF.1.3/Oper and FDP_ACF.1.4/Oper.

FDP_ACC.2/Mode_Trans Complete access control

Hierarchical to: FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.2.1/Mode_Trans The TSF shall enforce the *Mode transition SFP*[31] on *all subjects and the mode variable*[32] 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.

Application note 16: The mode variable defines the current mode of the TOE in the finite state model (cf. ADV_ARC.1 for more details). TOE modes of operation define a set of functionality available within the mode. E.g., in User mode the data interfaces are open for

[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] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

[30] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

[31] [assignment: *access control SFP*]

[32] [assignment: *list of subjects and objects*]

encryption/ decryption of user data with operational keys but key management functions are blocked. In Crypto officer mode key management functions are available but the data interfaces for the encryption/ decryption of user data with operational key are blocked.

FDP_ACF.1/Mode_Trans Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/Mode_Trans The TSF shall enforce the *Mode transition SFP*[33] to objects based on the following: *all subjects and the mode variable*[34].

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 Crypto officer role is allowed to change the mode variable to a Crypto officer mode, Key/CSP entry mode, User mode, and Self-test mode;

(2) the subject in End User role is allowed to change the mode variable to User mode;

(3) *the subject in the Maintenance Personal role is allowed to change the mode variable to a Maintenance mode after destruction of all operational secret and private keys and unprotected CSP,*

(4) *the subject in the Maintenance Personal role is allowed to change the mode variable from a Maintenance mode to other value only after destruction of all maintenance key and CSP*[35].

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 and Maintenance mode, when failure listed in FPT_FLS.1 occur,

(2) *[assignment: additional rules, based on security attributes, that explicitly authorise access of subjects to objects]*.[36]

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

(1) Subjects in other roles than the Crypto officer are not allowed to change the mode variable to a Crypto officer mode or a Key/CSP entry mode;

(2) Subjects in other roles than the Maintenance Personal role are not allowed to change the mode variable to a Maintenance mode;

(3) *[assignment: other rules, based on security attributes, that explicitly deny access of subjects to objects]*[37].

[33] [assignment: *access control SFP*]

[34] [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*]

[35] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

[36] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

[37] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

Application note 17: If the TOE does not provide any maintenance functionality the Maintenance modes do not exist and the Maintenance Personal Role is superfluous (cf. to FMT_SMR.2). In this case the rules (2) and (3) in FDP_ACF.1.2/Mode_Trans, (1) in FDP_ACF.1.2/Mode_Trans and (2) in FDP_ACF.1.4/Mode_Trans are obviously fulfilled.

FDP_ITC.2 Import of user data with security attributes

Hierarchical to: No other components.

Dependencies: [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]
FPT_TDC.1 Inter-TSF basic TSF data consistency

FDP_ITC.2.1 The TSF shall enforce the *Key Management SFP and Red-black separation SFP*[38] 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*[39].

Application note 18: 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).

FDP_ETC.2 Export of user data with security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

[38] [assignment: *access control SFP and/or information flow control SFP*]

[39] [assignment: *additional importation control rules*]

FDP_ETC.2.1 The TSF shall enforce the *Key Management SFP and Red-black separation SFP* [40] 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;

(5) *all secret and private keys exported controlled by the TSF shall be encrypted or protected by split-knowledge procedure using an Endorsed algorithm* [41].

FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to: No other components.

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_UCT.1.1 The TSF shall enforce the *Red-black separation SFP*[42] **by providing the ability** to *transmit and receive*[43] user data in a manner protected from unauthorised disclosure.

Application note 19: 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.

FDP_UIT.1 Data exchange integrity

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

[40] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[41] [assignment: *additional exportation control rules*]

[42] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[43] [selection: *transmit, receive*]

[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

FDP_UIT.1.1 The TSF shall enforce the *Red-black separation SFP*[44] to be able to *transmit and receive*[45] user data in a manner protected from *modification [selection: deletion, insertion, replay]* [46] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether *modification [selection: deletion, insertion, replay]* [47] has occurred.

FDP_RIP.2 Full residual information protection

Hierarchical to: FDP_RIP.1 Subset residual information protection

Dependencies: No dependencies.

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, deallocation of the resource from*] all objects.

Audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [selection, choose one of: *minimum, basic, detailed, not specified*] level of audit; and

c) *other auditable events*

c.1) Start-up after power-up,

c.2) Maintenance with software download if supported by the TOE,

c.3) Authentication failure handling (FIA_AFL.1): the reaching of the threshold for the unsuccessful authentication attempts and the actions,

c.4) *Timing of authentication (FIA_UAU.1): all unsuccessful authentication attempts of the authentication mechanism with the following information: claimed Identity of the user,*

c.5) 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;

c.6) 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;

[44] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[45] [selection: *transmit, receive*]

[46] [selection: *modification, deletion, insertion, replay*]

[47] [selection: *modification, deletion, insertion, replay*]

c.7) Cryptographic key destruction (FCS_CKM.4): permanent stored keys;

c.8) Failure with preservation of secure state (FPT_FLS.1): start-up after failure detection of the TSF and secure mode,

c.9) Management of TSF data (FMT_MTD.1/AUDIT): Export and clear of audit data,

c.10)Management of security functions behaviour (FMT_MOF.1/Adm, FMT_MOF.1/CO),

c.11)[assignment: *additional specifically defined auditable events*] [48].

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: *other audit relevant information*].

Application note 20: The ST writer shall perform the missing operations in the elements FAU_GEN.1.1 and FAU_GEN.1.2. The ST writer should consider the following additional auditable events if applicable:

c.12)input of permanent stored secret key with the following information Identity of the key, Identity of the user;

c.13)input of permanent stored private key with the following information Identity of the key, Identity of the user;

c.14)input of root public key with the following information Identity of the key, Identity of the user.

The ST writer should consider protection against denial of service due to logging of unsuccessful authentication attempts according to Timing of authentication (FIA_UAU.1).

For some situations it is possible that audit records of some events cannot be automatically generated. This is usually due to the audit functions not being operational at the time these events occur. Such events need to be documented in the Administrative Guidance, along with recommendation on how manual auditing should be established to cover these events.

(end of the application note)

FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

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.

FAU_SAR.1 Audit Review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

[48] [assignment: *other specifically defined auditable events*]

FAU_SAR.1.1 The TSF shall provide *Crypto Officer and Administrator*[49] with the capability to read *all audit data*[50] 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.

FAU_SAR.2 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit Review

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.

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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

FAU_STG.1.2 The TSF shall be able to *prevent*[51] unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.3 Action in Case of Possible Audit Data Loss

Hierarchical to: No other components.

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall *support the following actions*

(1) stop of normal operation except functions for audit management (FMT_MDT.1/Audit),

(2) action to prevent audit data loss as defined in FAU_STG.4,

(3) *[assignment: actions to be taken in case of possible audit storage failure]*[52],

if the audit trail exceeds *an Administrator settable percentage of storage capacity*[53].

Application note 21: The Administrator configures the behaviour of the audit function by selection between actions (1) or (2) or (3) in the element FAU_STG.3.1 (cf. FMT_MOF.1/Adm for management of TSF). The *normal operation* described in clause (1) includes all actions that may cause generation of audit data like initiation of user sessions (except a session of the Administrator), key management, and maintenance with software download. The *functions for audit management* in clause (1) include identification of user (FIA_UID.1, authentication of user with Administrator role (FIA_UAU.1) and the export and clearing of audit data (FMT_MTD.1/Audit).

FAU_STG.4 Prevention of Audit Data Loss

[49] [assignment: *authorised users*]

[50] [assignment: *list of audit information*]

[51] [selection, choose one of: *prevent, detect*]

[52] [assignment: *actions to be taken in case of possible audit storage failure*]

[53] [assignment: *pre-defined limit*]

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss.

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall *overwrite the oldest stored audit records* ***except those taken by the Crypto Officer and Administrator***[54] and [assignment: *other actions to be taken in case of audit storage failure*] if the audit trail is full.

Application note 22: If the selection of the auditable actions is configurable then FAU_SEL.1 shall be incorporated into the ST. FMT_MTD.1/Audit shall address the selection of auditable events and the assignment shall describe the "selection of auditable events".

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Application note 23: 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.

Management of TSF and protection of TSF data

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

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

(1) management of security functions behaviour (FMT_MOF.1/Adm and FMT_MOF.1/CO),

(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,

(5) *[assignment: list additional of security management functions to be provided by the TSF]*[55]*.*

FMT_SMR.2 Restrictions on security roles

Hierarchical to: FMT_SMR.1 Security roles

Dependencies: FIA_UID.1 Timing of identification

[54] [selection, choose one of: *"ignore auditable events","prevent auditable events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"*]

[55] [assignment: *list of security management functions to be provided by the TSF*]

FMT_SMR.2.1 The TSF shall maintain the roles: *End User Role, Crypto Officer Role, Administrator Role, Unidentified User Role, Unauthenticated User Role, [assignment: other roles]*[56].

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 Administrator Role must not be assigned to the End User Role or the Crypto Officer Role,*

(2) *Any user identity assigned to the Crypto Officer Role must not be assigned to the End User Role or the Administrator Role,*

(3) *[assignment: other conditions for the different roles]*[57]

are satisfied.

Refinement:

If the TOE provides maintenance functionality the TOE shall

(5) maintain the Maintenance Personal Role,

(6) any user identity assigned to the Administrator Role or Crypto Officer Role must not be assigned to the Maintenance Personal Role.

Application note 24: The ST writer may introduce other roles depending on the TOE life cycle, e.g., Personalization Agent Role as sub-set of the Administrator Role. If the TOE does not provide any maintenance functionality the Maintenance Personal Role is superfluous.

FMT_MOF.1/Adm Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1/Adm The TSF shall restrict the ability to *determine the behaviour of and modify the behaviour of*[58] the functions *audit*[59] to *Administrator*[60].

Application note 25: The Administrator is allowed to configure the actions of the audit function in case of possible audit data loss according to FAU_STG.3. The Administrator is not allowed to disable or enable the audit function.

FMT_MOF.1/CO Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

[56] [assignment: *authorised identified roles*]

[57] [assignment: *conditions for the different roles*]

[58] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

[59] [assignment: *list of functions*]

[60] [assignment: *the authorised identified roles*]

FMT_MOF.1.1/CO The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions *[assignment: list of functions except audit function]*[61] to *Crypto Officer*[62].

Refinement: If bypass mode is supported by the TOE then the TSF shall indicate through the Status output interface/port when the TOE is in bypass mode.

Application note 26: The ST writer shall perform the missing operation in the element FMT_MOF.1.1/CO according with the management of security functions behaviour supported by the TOE. The operation should address management functions like these

(1) disabling the encryption TSF when entering the bypass mode,

(2) enabling the encryption TSF when leaving the bypass mode,

(3) temporarily enabling or disabling of cryptographic functions, e.g., signature-creation.

Application note 27: The management of the audit function is restricted to the Administrator (cf. FMT_MOF.1/Adm). If maintenance mode is supported by the TOE than additional requirements shall be described by an iteration of the component FMT_MOF.1/CO because the mode transition into the error mode may be caused automatically by hard errors or by users in the maintenance role. Maintenance should include requirements like these:

(4) temporarily disabling cryptographic operation with keys by destruction of plaintext operational keys and CSP when entering the maintenance mode until other keys are imported or generated,

(5) temporarily disabling cryptographic operation with keys by destruction of maintenance keys and CSP when leaving the maintenance mode until operational keys are imported or generated.

FMT_MTD.1/Admin Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/Admin The TSF shall restrict the ability to *create, clear and delete*[63] the *Reference Authentication Data* [64] to *Administrator*[65].

FMT_MTD.1/User Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/User The TSF shall restrict the ability to *modify* [66] the *Reference Authentication Data*[67] to *the authorized user*[68] ***for their own Reference Authentication Data***.

[61] [assignment: *list of functions*]

[62] [assignment: *the authorised identified roles*]

[63] [selection: *change_default, query, modify, delete, clear,[assignment: other operations]*]

[64] [assignment: *list of TSF data*]

[65] [assignment: *the authorised identified roles*]

[66] [selection: *change_default, query, modify, delete, clear,[assignment: other operations]*]

[67] [assignment: *list of TSF data*]

FMT_MTD.1/Audit Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/Audit The TSF shall restrict the ability to *export and clear*[69] the *audit data*[70] to *Administrator*[71].

FMT_MSA.1/Key_Man_1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [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

FMT_MSA.1.1/Key_Man_1 The TSF shall enforce the *Key Management SFP*[72] to restrict the ability to *change_default and query*[73] the security attributes *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*[74] to *Crypto Officer*[75].

FMT_MSA.1/Key_Man_2 Management of security attributes

Hierarchical to: No other components.

Dependencies: [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

FMT_MSA.1.1/Key_Man_2 The TSF shall enforce the *Key Management SFP*[76] to restrict the ability to *modify or delete*[77] 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*[78] to *none*[79].

[68] [assignment: *the authorised identified roles*]

[69] [selection: *change_default, query, modify, delete, clear,[assignment: other operations]*]

[70] [assignment: *list of TSF data*]

[71] [assignment: *the authorised identified roles*]

[72] [assignment: *access control SFP, information flow control SFP*]

[73] [selection: *change_default, query, modify, delete, [assignment: other operations]*]

[74] [assignment: *list of security attributes*]

[75] [assignment: *the authorised identified roles*]

[76] [assignment: *access control SFP, information flow control SFP*]

[77] [selection: *change_default, query, modify, delete, [assignment: other operations]*]

[78] [assignment: *list of security attributes*]

[79] [assignment: *the authorised identified roles*]

FMT_MSA.1/Key_Man_3 Management of security attributes

Hierarchical to: No other components.

Dependencies: [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

FMT_MSA.1.1/Key_Man_3 The TSF shall enforce the *Key Management SFP* [80] to restrict the ability to *modify* [81] the security attributes *Key access control rules, CSP access control rules*[82] to *Crypto Officer* [83].

Application note 28: The ST writer may define additional management of security attributes consistent with this component by iteration. The SFR FMT_MSA.1/Key_Man_3 of management of security attributes ensures that the Crypto officer may change the access control rules for a cryptographic key or a CSP depending on the (local) users (cf. also to FPT_TDC.1).

FMT_MSA.2 Secure security attributes

Hierarchical to: No other components.

Dependencies: [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

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* [84].

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the *Key Management SFP, Cryptographic Operation SFP and Mode_Trans SFP*[85] to provide *restrictive*[86] default values for security attributes that are used to enforce the SFP.

[80] [assignment: *access control SFP, information flow control SFP*]

[81] [selection: *change_default, query, modify, delete, [assignment: other operations]*]

[82] [assignment: *list of security attributes*]

[83] [assignment: *the authorised identified roles*]

[84] [assignment: *list of security attributes*]

[85] [assignment: *access control SFP, information flow control SFP*]

[86] [selection, choose one of: *restrictive, permissive,[assignment: other property]*]

FMT_MSA.3.2 The TSF shall allow the *Crypto Officer*[87] to specify alternative initial values to override the default values when an object or information is created.

TSF protection

FPT_TDC.1 Inter-TSF basic TSF data consistency

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret *security attributes of cryptographic keys, key components and CSP*[88] 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*[89]

when interpreting the TSF data from another trusted IT product.

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: *self test fails*[90].

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.

FPT_EMSEC.1 TOE Emanation

[87] [assignment: *the authorised identified roles*]

[88] [assignment: *list of TSF data types*]

[89] [assignment: *list of interpretation rules to be applied by the TSF*]

[90] [assignment: list of types of failures in the TSF]

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

(1) *confidential authentication data*,

(2) *[assignment: list of types of other TSF data]*[91]

and

(1) *"red data" containing confidential information,*

(2) *plaintext cryptographic secret or private key,*

(3) *cryptographic key components,*

(4) confidential CSP,

(5) *[assignment: list of types of other user data]*[92].

FPT_EMSEC.1.2 The TSF shall ensure [assignment: *type of users*] are unable to use *any interface or port with exception identified below* [93] to gain access to

(1) confidential authentication data (except the authentication interface/port during authentication process of the user),

(2) *[assignment: list of types of other TSF data]*[94]

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: list of types of other user data]*[95].

Application note 29: The ST writer shall perform the missing operation in the elements FPT_EMSEC.1.1 and FPT_EMSEC.1.2. The types of emanation shall include all forms of side channels (power consumption, electromagnetic emanation, and timing) emitted by the TOE that may contain confidential information about the listed assets. The limits shall be specified to prevent attacks through analysis of the emissions in the intended operational environment. The exceptions in element FPT_EMSEC.1.2 comprise the intended use of these interfaces respective ports. For example, the data input and output interfaces for "red data" contain the confidential information about confidential red data but the data input and output interfaces for "black data" must not contain confidential information about the corresponding "red data" for user not knowing the decryption key. They must not provide information about the plaintext of any cryptographic secret or private key without any exception of interfaces or

[91] [*assignment: list of types of TSF data*]

[92] [*assignment: list of types of user data*]

[93] [*assignment: types of interfaces/ports*]

[94] [*assignment: list of types of TSF data*]

[95] [*assignment: list of types of user data*]

ports (e.g., through a side channel analysis). If a cryptographic secret or private key is exported in encrypted form the information about the plaintext depends on knowledge of the key encryption key.

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]*] to demonstrate the correct operation of [selection: *[assignment: parts of TSF], the TSF*].

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

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

FPT_TST.2 TSF 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 *initial start-up self-test, power-up self-test, self-test at the request of the authorised user [assignment: other self-tests]*[96] the TSF shall *inhibit all output via the data interfaces/ports, and [assignment: list of additional actions to be performed]*[97].

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: list of additional actions to be performed]*[98].

[96] [assignment: *list of self-tests*]

[97] [assignment: list of actions to be performed]

[98] [assignment: list of actions to be performed]

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: list of additional actions to be performed]*[99].

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, if applicable, the following conditions: i) when a critical cryptographic algorithm or critical TSF operation is invoked, ii) pair-wise consistency test for newly generated asymmetric key-pairs, iii) on software/firmware load test, iv) on manual key entry, and v) and on bypass events.

If the TOE provides *generation of public/private key pairs*, then the following pair-wise consistency tests for public and private keys shall be performed. If the keys are used to perform an Endorsed key transport method, then the 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. If the keys are used to perform the calculation and verification of digital signatures, then the 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.

If *manual import of cryptographic keys or key components* into the TOE is supported, then the following manual key entry tests shall be performed. The cryptographic key or key components shall have an Endorsed EDC applied, or shall be entered using duplicate entries. If the EDC cannot be verified, or the duplicate entries do not match, the test shall fail.

If *load of software or firmware into the TOE* is supported, then 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.

If the TOE implements a *bypass capability* where the services may be provided without cryptographic processing, then the following bypass tests shall be performed to ensure that a single point of failure of TOE components will not result in the unintentional output of plaintext. The TSF shall test for the correct operation of the services providing cryptographic processing when a switch takes place between an exclusive bypass service

[99] [assignment: list of actions to be performed]

and an exclusive cryptographic service. If the TOE can automatically alternate between a bypass service and a cryptographic service, providing some services with cryptographic processing and some services without cryptographic processing, then the TSF shall test for the correct operation of the services providing cryptographic processing when the mechanism governing the switching procedure is modified.

(End of refinement.)

Application note 30: 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 [6]) 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.

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist *physical manipulation and probing*[100] to the *TSF*[101] by responding automatically such that the SFRs are always enforced.

Refinement:

If the TOE is a single-chip cryptographic module the TOE shall resist physical manipulation and probing at any time. If the TOE is a multiple-chip cryptographic module 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 31:

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

For single-chip TOE the supporting documents for smart cards and similar devices apply to the TOE for resistance to physical attacks. The TSF will implement appropriate mechanisms to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TSF can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that security functional requirements are enforced. Hence, “automatic response” means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

The requirement for automated response of the TOE is fulfilled due to physical protection mechanisms of the TOE if a physical tampering attack causes serious damage to the TOE such that the TOE will not function and will not compromise any internal secret (i.e., confidential CSP like secret or private cryptographic keys or confidential TSF data).

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,

[100] [assignment: physical tampering scenarios]

[101] [assignment: list of TSF devices/elements]

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.
End of Application note.

6.2 Security Assurance Requirements for the TOE

EAL4 augmented with ADV_IMP.2, ALC_CMC.5, ALC_DVS.2 and AVA_VAN.5. These assurance requirements are:

Development activities (Class ADV)
- Security Architecture (Component ADV_ARC.1)
- Functional Specification (Component ADV_FSP.4)
- Implementation Representation (Component ADV_IMP.2)
- TOE Design (Component: ADV_TDS.3)

Guidance documents activities (Class AGD)
- Operational User Guidance (Component AGD_OPE.1)
- Preparative Procedures (Component AGD_PRE.1)

Life cycle support (Class ALC)
- CM Capabilities (Component ALC_CMC.5)
- CM Scope (Component ALC_CMS.4)
- Delivery (Component ALC_DEL.1)
- Development Security (Component ALC_DVS.2)
- Life Cycle Definition (Component ALC_LCD.1)
- Tools and Techniques (Component ALC_TAT.1)

Security Target evaluation (Class ASE)
- Conformance Claims (Component ASE_CCL.1)
- Extended Components Definition (Component ASE_ECD.1)
- ST Introduction (Component ASE_INT.1)
- Security Objectives (Component ASE_OBJ.2)
- Security Requirements (Component ASE_REQ.2)
- Security Problem Definition (Component ASE_SPD.1)
- TOE Summary Specification (Component ASE_TSS.1)

Tests activities (Class ATE)
- Coverage (Component ATE_COV.2)
- Depth (Component ATE_DPT.2)
- Functional Tests (Component ATE_FUN.1)
- Independent Testing (Component ATE_IND.2)

Vulnerability assessment (Class AVA)
- Vulnerability Analysis (Component AVA_VAN.5)

6.2.1 Development activities (Class ADV)

ADV_ARC.1 Security architecture description

Dependencies: ADV_FSP.1 Basic functional specification

ADV_TDS.1 Basic design

Developer action elements:

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation elements:

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

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

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialisation process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

Evaluator action elements:

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

Refinement:

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

(ii) 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) Crypto officer modes
(3) Key/CSP entry modes.
(4) User modes
(5) Self-test modes
(6) Error modes
(7) Bypass modes if exist any
(8) Maintenance modes if TOE provides maintenance functionality.

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.

If bypass modes exist the Finite state model shall demonstrate, that for all transitions into any bypass mode, two independent internal actions are required for the transition into each bypass mode.

If bypass modes exist, the security architecture description shall demonstrate that functions solely intended for bypass are not executable in any other mode of operation.

If maintenance modes exist the security architecture shall demonstrate that the mode transition entering or exiting maintenance mode shall destruct all plaintext secret and private keys and unprotected CSPs.

If maintenance modes exist, the security architecture description shall demonstrate that functions solely intended for maintenance are not executable in any other mode of operation.

Refinement for Evaluator action element ADV_ARC1.1E:

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 32: 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 (Crypto officer modes, Key/CSP entry modes, User modes, Self-test modes, Error modes, Bypass modes Maintenance 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.

Application note 33: Self-protection that is addressed in FPT_EMSEC.1 shall be described in the security architecture. The security architecture description shall demonstrate that the TSF protects itself from emitting side channels (power consumption, electromagnetic emanation, and timing) that contain confidential information about the assets listed in FPT_EMSEC.1.

Application note 34: Self protection and non-bypassability that is addressed in FPT_PHP.3 shall be described in the security architecture. The security architecture description shall demonstrate that the TSF protects itself from malfunction due to accidental or deliberated environmental stress or perturbation, in order to deactivate, modify, or circumvent security functions of the TOE and to enable attacks against assets of the TOE. The security architecture description should consider that self-protection and non-bypassability is also sustained with regard to the ageing process of hardware components under environmental stress.

Application note 35: Construction may support self-protection against undetected physical probing inside the enclosure by means, e.g., require at least one 90 degree bend or obstruction with a substantial blocking material.

Application note 36: For a single-chip TOE the supporting documents for smart cards and similar devices should be considered for tamper resistance.

ADV_FSP.4 Complete functional specification

Dependencies: ADV_TDS.1 Basic design

Developer action elements:

ADV_FSP.4.1D The developer shall provide a functional specification.

ADV_FSP.4.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

ADV_FSP.4.1C The functional specification shall completely represent the TSF.

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

ADV_FSP.4.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.4.4C The functional specification shall describe all actions associated with each TSFI.

ADV_FSP.4.5C The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.

ADV_FSP.4.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

ADV_FSP.4.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.4.2E The evaluator *shall determine* that the functional specification is an accurate and complete instantiation of the SFRs.

Refinement:

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 37: 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.

ADV_IMP.2 Complete mapping of the implementation representation of the TSF

Dependencies: ADV_TDS.3 Basic modular design

ALC_TAT.1 Well-defined development tools

ALC_CMC.5 Advanced support

Developer action elements:

ADV_IMP.2.1D The developer shall make available the implementation representation for the entire TSF.

ADV_IMP.2.2D The developer shall provide a mapping between the TOE design description and the entire implementation representation.

Content and presentation elements:

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.

ADV_IMP.2.2C The implementation representation shall be in the form used by the development personnel.

ADV_IMP.2.3C The mapping between the TOE design description and the entire implementation representation shall demonstrate their correspondence.

Evaluator action elements:

ADV_IMP.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

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.

ADV_TDS.3 Basic modular design

Dependencies: ADV_FSP.4 Complete functional specification

Developer action elements:

ADV_TDS.3.1D The developer shall provide the design of the TOE.

ADV_TDS.3.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements:

ADV_TDS.3.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.3.2C The design shall describe the TSF in terms of modules.

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

ADV_TDS.3.4C The design shall provide a description of each subsystem of the TSF.

ADV_TDS.3.5C The design shall provide a description of the interactions among all subsystems of the TSF.

ADV_TDS.3.6C The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.

ADV_TDS.3.7C The design shall describe each SFR-enforcing module in terms of its purpose and interaction with other modules.

ADV_TDS.3.8C The design shall describe each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces, interaction with and called interfaces to other modules.

ADV_TDS.3.9C The design shall describe each SFR-supporting or SFR-non-interfering module in terms of its purpose and interaction with other modules.

ADV_TDS.3.10C The mapping shall demonstrate that all behaviour described in the TOE design is mapped to the TSFIs that invoke it.

Evaluator action elements:

ADV_TDS.3.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.3.2E The evaluator *shall determine* that the design is an accurate and complete instantiation of all security functional requirements.

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 ventilation physical design approach if applicable. This description shall demonstrate that if the TOE (hardware) contains ventilation holes or slits, then the holes or slits shall be constructed in a manner that prevents undetected physical probing inside the enclosure.

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.

6.2.2 Guidance documents (Class AGD)

AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements:

AGD_OPE.1.1D The developer shall provide operational user guidance.

Content and presentation elements:

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

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.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements:

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

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.

The guidance documentation shall describe how the user is able to initiate and is informed about the result of the self-tests as specified in FPT_TST.1.

For some situations it is possible that some events cannot be automatically generated. This is usually due to the audit functions not being operational at the time these events occur. Such events need to be documented in the Administrative Guidance, along with recommendation on how manual auditing should be established to cover these events.

AGD_PRE.1 Preparative procedures

Dependencies: No dependencies.

Developer action elements:

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements:

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements:

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

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

6.2.3 Life cycle support (Class ALC)

ALC_CMC.5 Advanced support

Dependencies: ALC_CMS.1 TOE CM coverage

ALC_DVS.2 Sufficiency of security measures

ALC_LCD.1 Developer defined life-cycle model

Developer action elements:

ALC_CMC.5.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.5.2D The developer shall provide the CM documentation.

ALC_CMC.5.3D The developer shall use a CM system.

Content and presentation elements:

ALC_CMC.5.1C The TOE shall be labelled with its unique reference.

ALC_CMC.5.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.5.3C The CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.

ALC_CMC.5.4C The CM system shall uniquely identify all configuration items.

ALC_CMC.5.5C The CM system shall provide automated measures such that only authorised changes are made to the configuration items.

ALC_CMC.5.6C The CM system shall support the production of the TOE by automated means.

ALC_CMC.5.7C The CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.

ALC_CMC.5.8C The CM system shall identify the configuration items that comprise the TSF.

ALC_CMC.5.9C The CM system shall support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.

ALC_CMC.5.10C The CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.

ALC_CMC.5.11C The CM system shall be able to identify the version of the implementation representation from which the TOE is generated.

ALC_CMC.5.12C The CM documentation shall include a CM plan.

ALC_CMC.5.13C The CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.5.14C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

ALC_CMC.5.15C The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.5.16C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

Evaluator action elements:

ALC_CMC.5.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ALC_CMC.5.2E The evaluator *shall determine* that the application of the production support procedures results in a TOE as provided by the developer for testing activities.

ALC_CMS.4 Problem tracking CM coverage

Dependencies: No dependencies.

Developer action elements:

ALC_CMS.4.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.4.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.

ALC_CMS.4.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.4.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements:

ALC_CMS.4.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ALC_DEL.1 Delivery procedures

Dependencies: No dependencies.

Developer action elements:

ALC_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation elements:

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

Evaluator action elements:

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

ALC_DVS.2 Sufficiency of security measures

Dependencies: No dependencies.

Developer action elements:

ALC_DVS.2.1D The developer shall produce development security documentation.

Content and presentation elements:

ALC_DVS.2.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.2.2C The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

Evaluator action elements:

ALC_DVS.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.2.2E The evaluator *shall confirm* that the security measures are being applied.

ALC_LCD.1 Developer defined life-cycle model

Dependencies: No dependencies.

Developer action elements:

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

Content and presentation elements:

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

Evaluator action elements:

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

ALC_TAT.1 Well-defined development tools

Dependencies: ADV_IMP.1 Implementation representation of the TSF

Developer action elements:

ALC_TAT.1.1D The developer shall identify each development tool being used for the TOE.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of each development tool.

Content and presentation elements:

ALC_TAT.1.1C Each development tool used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

ALC_TAT.1.3C The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

Evaluator action elements:

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

6.2.4 Security Target evaluation (Class ASE)

ASE_CCL.1 Conformance claims

Dependencies: ASE_INT.1 ST introduction

ASE_ECD.1 Extended components definition

ASE_REQ.1 Stated security requirements

Developer action elements:

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

Content and presentation elements:

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

Evaluator action elements:

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

ASE_ECD.1 Extended components definition

Dependencies: No dependencies.

Developer action elements:

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

Content and presentation elements:

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or 68on-conformance to these elements can be demonstrated.

Evaluator action elements:

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

ASE_ECD.1.2E The evaluator *shall confirm* that no extended component can be clearly expressed using existing components.

ASE_INT.1 ST introduction

Dependencies: No dependencies.

Developer action elements:

ASE_INT.1.1D The developer shall provide an ST introduction. Content and presentation elements:

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall identify the TOE.

ASE_INT.1.4C The TOE overview shall summarise the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

Evaluator action elements:

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

ASE_INT.1.2E The evaluator *shall confirm* that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

ASE_OBJ.2 Security objectives

Dependencies: ASE_SPD.1 Security problem definition

Developer action elements:

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D The developer shall provide a security objectives rationale.

Content and presentation elements:

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

Evaluator action elements:

ASE_OBJ.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ASE_REQ.2 Derived security requirements

Dependencies: ASE_OBJ.2 Security objectives

ASE_ECD.1 Extended components definition

Developer action elements:

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirements rationale.

Content and presentation elements:

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C All operations shall be performed correctly.

ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

Evaluator action elements:

ASE_REQ.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ASE_SPD.1 Security problem definition

Dependencies: No dependencies.

Developer action elements:

ASE_SPD.1.1D The developer shall provide a security problem definition.

Content and presentation elements:

ASE_SPD.1.1C The security problem definition shall describe the threats.

ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C The security problem definition shall describe the OSPs.

ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

Evaluator action elements:

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

ASE_TSS.1 TOE summary specification

Dependencies: ASE_INT.1 ST introduction

ASE_REQ.1 Stated security requirements

ADV_FSP.1 Basic functional specification

Developer action elements:

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

Content and presentation elements:

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

Evaluator action elements:

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

ASE_TSS.1.2E The evaluator *shall confirm* that the TOE summary specification is consistent with the TOE overview and the TOE description.

6.2.5 Tests (Class ATE)

ATE_COV.2 Analysis of coverage

Dependencies: ADV_FSP.2 Security-enforcing functional specification

ATE_FUN.1 Functional testing

Developer action elements:

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation elements:

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

Evaluator action elements:

ATE_COV.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ATE_DPT.2 Testing: security enforcing modules

Dependencies: ADV_ARC.1 Security architecture description

ADV_TDS.3 Basic modular design

ATE_FUN.1 Functional testing

Developer action elements:

ATE_DPT.2.1D The developer shall provide the analysis of the depth of testing.

Content and presentation elements:

ATE_DPT.2.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems and SFR-enforcing modules in the TOE design.

ATE_DPT.2.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

ATE_DPT.2.3C The analysis of the depth of testing shall demonstrate that the SFR-enforcing modules in the TOE design have been tested.

Evaluator action elements:

ATE_DPT.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Functional testing

Dependencies: ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements:

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

ATE_IND.2 Independent testing – sample

Dependencies: ADV_FSP.2 Security-enforcing functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

ATE_COV.1 Evidence of coverage

ATE_FUN.1 Functional testing

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator *shall execute* a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator *shall test* a subset of the TSF to confirm that the TSF operates as specified.

6.2.6 Vulnerability assessment (Class AVA)

AVA_VAN.5 Advanced methodical vulnerability analysis

Dependencies: ADV_ARC.1 Security architecture description

ADV_FSP.2 Security-enforcing functional specification

ADV_TDS.3 Basic modular design

ADV_IMP.1 Implementation representation of the TSF

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Developer action elements:

AVA_VAN.5.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.5.1C The TOE shall be suitable for testing.

Evaluator action elements:

AVA_VAN.5.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.5.2E The evaluator *shall perform* a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.5.3E The evaluator *shall perform* an independent, methodical vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.

AVA_VAN.5.4E The evaluator *shall conduct* penetration testing based on the identified potential vulnerabilities to determine that the TOE is resistant to attacks performed by an attacker possessing High attack potential.

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.

Table 2: Coverage of Security Objective for the TOE by SFR

	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		x							x		x				
FCS_CKM.2/Import		x								x	x				
FCS_CKM.2/Export		x						x			x				
FCS_CKM.4		x									x	x			
FTP_ITC.1								x		x	x				
FCS_COP.1	x	x													
FCS_RNG.1		x							x						
FIA_ATD.1			x												
FIA_UID.1			x												
FIA_UAU.1			x												
FIA_UAU.6			x												
FIA_UAU.7			x												
FIA_USB.1			x												
FIA_AFL.1			x												
FDP_ACC.2/Key_Man				x	x						x				
FDP_ACF.1/Key_Man				x	x						x	x			
FDP_ACC.2/Oper				x	x										
FDP_ACF.1/Oper				x	x										
FDP_ACC.2/Mode_Trans				x											
FDP_ACF.1/Mode_Trans				x	x										
FDP_ITC.2		x								x	x				
FDP_ETC.2		x						x			x				
FDP_UCT.1	x							x		x	x				
FDP_UIT.1	x							x		x	x				
FDP_RIP.2															x
FAU_GEN.1							x								
FAU_GEN.2							x								
FAU_SAR.1							x								
FAU_SAR.2							x								
FAU_STG.1							x								
FAU_STG.3							x								
FAU_STG.4							x								
FPT_STM.1					x		x								
FMT_SMF.1				x							x				
FMT_SMR.2				x		x					x				

	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
FMT_MOF.1/Adm				x			x								
FMT_MOF.1/CO				x											
FMT_MTD.1/Admin			x												
FMT_MTD.1/User			x												
FMT_MTD.1/Audit							x								
FMT_MSA.1/Key_Man_1				x							x				
FMT_MSA.1/Key_Man_2				x							x				
FMT_MSA.1/Key_Man_3				x							x				
FMT_MSA.2				x	x						x				
FMT_MSA.3				x					x		x				
FPT_TDC.1								x		x	x				
FPT_FLS.1													x		
FPT_EMSEC. 1	x														x
FPT_PHP.3														x	
FPT_TST.1													x		
FPT_TST.2													x		

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

- FCS_COP.1 requires the necessary cryptographic operations needed for encryption, decryption of data containing confidential information and integrity protection for data containing integrity sensitive information.
- 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, FCS_CKM.2/Import, FCS_CKM.2/Export, FCS_CKM.4, FCS_COP.1 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 Administrator, the Cryptographic Administrator, the End user roles, *Unidentified User Role, Unauthenticated User Role* and the Maintenance Personal if TOE supports maintenance functionality.

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 Administrator 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.
- 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_MOF.1/Adm limits the management of audit TSF behaviour to the users in the Administrator role.
- FMT_MOF.1/CO limits the management of TSF (except audit TSF) behaviour to the users in the Crypto officer role.

- 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 and FMT_MSA.3 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_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_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.

The SFR FDP_ACF.1/Mode_Trans and the refinement to the SAR ADV_ARC.1 ensures that operational keys and CSP can not be used in maintenance mode and maintenance 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 Crypto Officer and Administrator 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 Crypto Officer and Administrator.
- 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 Administrator settable percentage of storage capacity by one of the selectable actions (1) stop normal operation except functions for audit management (FMT_MDT.1/Audit) or (2) action to prevent audit data loss (FAU_STG.4) or (3) assigned other actions.
- FAU_STG.4 shall prevent loss of audit data if the audit trail is full by overwriting the oldest stored audit records except those taken by the Crypto Officer and Administrator.

- FMT_MOF.1/Adm limits the management of audit TSF behaviour (as defined by FAU_STG.4) to the users in the Administrator role.
- FMT_MTD.1/Audit restricts the ability to export and clear the audit data to Administrator.
- 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, 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_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 Crypto officer for operational keys and the Maintenance Personal role for maintenance keys).
- FMT_MSA.1/Key_Man_1, FMT_MSA.1/Key_Man_2 FMT_MSA.2 and FMT_MSA.3 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_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 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 requires restrictive values of security attributes for cryptographic keys and limits the ability to specify their initial value to the Crypto 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_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_ACF.1/Key_Man limits key destruction to users in the Crypto 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

The security objective for the TOE environment OE.Assurance is provided by the security assurance requirements EAL4 augmented with AVA_VAN.5.
The security objectives for the TOE environment OE.Key_Generation, OE.Red-Black-Sep, OE.Audit_Analysis, OE.Personal and OE.Key_Availabilty will be provided by technical and organisational security measures. There is no need to specify these security measures on the abstract level of this protection profile.

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
FAU_STG.4	FAU_STG.1 Protected audit trail storage	FAU_STG.1
FCS_CKM.1	[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, 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, FCS_CKM.4
FCS_CKM.2/Import	[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	FDP_ITC.2, FCS_CKM.1, FCS_CKM.4

SFR	Dependencies	Support of the Dependencies
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
FCS_COP.1	[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, 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, FMT_MSA.3
FDP_ACF.1/Mode_Trans	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	FDP_ACC.2/Mode_Trans, FMT_MSA.3
FDP_ACF.1/Oper	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	FDP_ACC.2/Oper, FMT_MSA.3
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_ITC.2	[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], FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.2/Key_Man, FDP_ACC.2/Oper (hierarchical to FDP_ACC.1), FTP_ITC.1, FPT_TDC.1,

SFR	**Dependencies**	**Support of the Dependencies**
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_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_RIP.2	No dependencies	n. a.
FIA_AFL.1	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/Adm	FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions	FMT_SMR.2 (hierarchical to FMT_SMR.1), FMT_SMF.1
FMT_MOF.1/CO	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],	FDP_ACC.2/Key_Man, FDP_ACC.2/Oper (hierarchical to FDP_ACC.1)

SFR	**Dependencies**	**Support of the Dependencies**
	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_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
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),
FMT_MSA.3	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_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
FPT_STM.1	No dependencies	No dependencies
FPT_TDC.1	No dependencies	No dependencies
FPT_TST.1	No dependencies	No dependencies

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

Table 3: Dependencies between the SFR for the TOE

6.3.3 Security Assurance Requirements Rationale

The EAL4 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. 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 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 the 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

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

6.3.4 Security Requirements – Mutual Support and Internal Consistency

The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together form a mutually supportive and internally consistent whole.

The analysis of the TOE´s security requirements with regard to their mutual support and internal consistency demonstrates:

The dependency analysis in section 7.2.2 Dependency Rationale for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and non-satisfied dependencies are appropriately explained.

The assurance class EAL4 is an established set of mutually supportive and internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 7.2.3 Security Assurance Requirements Rationale shows that the assurance requirements are mutually supportive and internally consistent as all (sensitive) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements could only arise if there are functional-assurance dependencies which are not met, a possibility which has been shown not to arise in sections 7.2.2 Dependency Rationale and 7.2.3 Security Assurance Requirements Rationale. Furthermore, as also discussed in section 7.2.3 Security Assurance Requirements Rationale, the chosen assurance components are adequate for the functionality of the TOE. So the assurance requirements and security functional requirements support each other and there are no inconsistencies between the goals of these two groups of security requirements.

7 PP Application Notes

The application notes are included in the text above.

8 Glossary and Acronyms

8.1 Glossary

Term	PP CM (all security levels)
Administrator	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.
Authentication interface/ port	Data interface respective port used for input of confidential authentication data.
Authentication keys	General term for keys used for authentication of data (i.e. Data authentication keys) or the identity of an entity (i.e. Entity authentication keys)
Authentication reference keys	Private key for proof of their own identity claimed in an asymmetric authentication protocol
Authentication verification keys	Public Key assigned to a claimed identity of an entity for verification of the knowledge of a private key by means asymmetric authentication protocol
Automated key transport	The transport of cryptographic keys, usually in encrypted form, using electronic means such as a computer network (e.g., key transport/agreement protocols).
Backup data	User data and TSF data of the TOE that are integrated in a backup file.
Backup key components	Cryptographic key components that are used for the encryption of confidential backup data, e.g., for the encryption of cryptographic keys and other critical security parameters.
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.
Bypass mode	Mode of operation in which the cryptographic module provides services without cryptographic processing (e.g., transferring plaintext through the cryptographic module).
Bypass state	State related to the bypass mode in the Finite state model (cf. ADV_ARC.1).
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.
Control input interface/	Interface respective port intended for all input commands, signals,

Term	PP CM (all security levels)
port	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.
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.
Crypto 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. (The "cryptographic administrator" is some times called "crypto officer" in the guidance documentation) (the same as *Cryptographic administrator)*
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 checksum	A checksum that is created by performing a cryptographic algorithm. The cryptographic checksum can be associated with the original data in order to provide a mechanism to verify that the original data has not been changed.
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	A parameter used in conjunction with a cryptographic algorithm

Term	PP CM (all security levels)
(key)	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)
Data input interface/port	Interface respective port intended for 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:	Interface respective port intended for 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).
Data path	The physical or logical route over which data passes; a physical data path may be shared by multiple logical data paths.
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

Term	PP CM (all security levels)
	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 non-repudiation.
Electromagnetic compatibility (EMC)	The ability of electronic devices to function satisfactorily in an electromagnetic environment without introducing intolerable electromagnetic disturbances to other devices in that environment.
Electromagnetic emanation analysis (EMEA)	Analysis of electromagnetic emissions from a device, equipment, or system to gain information about its internal secrets or processes
Electromagnetic interference (EMI)	Electromagnetic emissions from a device, equipment, or system that interfere with the normal operation of another device, equipment, or system.
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.
End User	An authorized user assumed to perform general security services, including cryptographic operations and other Endorsed security functions.
Endorsed	For this protection profile, endorsed by the certification body for the evaluation of products of an intended type and resistance against attacks with attack potential addressed by the vulnerability analysis component in the security target[102].
Endorsed mode of operation	For this protection profile, a operational mode of the cryptographic module that employs only Endorsed security functions (e.g., installation, start-up, normal operation, maintenance; not to be confused with a specific mode of an Endorsed security function, e.g., DES CBC mode)
Endorsed security function	For this protection profile, a security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either a) specified in an Endorsed

[102] Endorsed algorithms and functions could be similar to the list of cryptographic algorithms and parameters published for qualified electronic signatures by the notified body Bundesnetzagentur in Germany or the Approved algorithms published by NIST in the USA.

Term	PP CM (all security levels)
	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 mod'le's normal operating range.
Error detection code (EDC)	A code computed from data and comprised of redundant bits of information designed to detect, but not correct, unintentional changes in the data.
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.
Hash-based message authentication code (HMAC)	A message authentication code that utilizes a keyed hash.
Higher Order Side Channel Analysis	A side channel analysis that additionally analyzes the masking of a device, equipment, or system in order to gain information about its internal secrets or processes.
Information processing	The organisation, manipulation and distribution of information.
Initialization vector (IV)	A vector used in defining the starting point of an encryption process within a cryptographic algorithm.
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.
Internal secrets	Confidential data inside the cryptographic boundary not intended for export (e.g., secret or private plaintext keys, authentication reference data).
IT system	For this protection profile, an IT system using the TOE to protect user data during transmission over or storage on media to which

Term	PP CM (all security levels)
	unauthorised user have access to.
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).
Key encrypting key	A cryptographic key that is used for the encryption or decryption of other keys.
Key establishment	The process by which cryptographic keys are securely distributed among cryptographic modules using manual transport methods (e.g., key loaders), automated methods (e.g., key transport and/or key agreement protocols), or a combination of automated and manual methods (consists of key transport plus key agreement).
Key interface/port	Data interface respective port used for the input and output of plaintext cryptographic key components and CSPs.
Key loader	A self-contained unit that is capable of storing at least one plaintext or encrypted cryptographic key or key component that can be transferred, upon request, into a cryptographic module.
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 transport	Secure transport of cryptographic keys from one cryptographic module to another module.
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)
Logical external interface	A logical entry or exit point of a cryptographic module that provides access to the module for logical information flows representing physical signals (see also the term “port” for the physical aspects of a logical external interface). In the CC terminology it covers all logical external interfaces of the TOE (direct or indirect interfaces to the TSF or interfaces to the non-TSF portion of the TOE, cf. CEM paragraph 529 for details).
Non-operational CSP	CSP used only for self test (e.g., for known answer tests) and maintenance operation (e.g., to test the operation of the cryptographic module after software update or repairing hardware components). Non-operational must not be used for protection of user the confidentiality or integrity of data by cryptographic operation.
Maintenance mode	Mode of operation for maintaining and servicing a cryptographic module, including physical and logical maintenance testing.

Term	PP CM (all security levels)
Maintenance state	State related to the Maintenance 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.
Masking	Computational process of adding random numbers to data in order to protect the confidentiality of the data against side channel analysis.
Message authentication with appendix	A digital signature scheme which requires the message as input to the verification algorithm. The signature is attached to the message
Message authentication with message recovery	A digital signature scheme with message recovery is a digital signature scheme for which a priori knowledge of the message is not required for the verification algorithm.
Microcode	The elementary processor instructions that correspond to an executable program instruction.
Operating conditions	Any environmental condition being accidental or induced outside of the normal range intended for the TOE may affect the correct operation or compromise of confidential information. These conditions include but are not limit to voltage of power supply, temperature, emanation which TOE environmental conditions.
Operational CSP	CSP used for protection of user the confidentiality or integrity of data by cryptographic operation.
Output data	Data containing information that is produced from a cryptographic module.
Password	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.
Personal identification number (PIN)	An alphanumeric code or password used to authenticate an identity.
Permanent stored keys	Keys remains stored in the TOE after power off or reset.
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 (direct or indirect interface to the TSF or interface to the non-TSF portion of the TOE, cf. CEM paragraph 529 for details).
Power interface/port	Interface respective port providing all external electrical power supply.

Term	PP CM (all security levels)
Power On/Off mode	Mode of operation that indicates whether the cryptographic module is supplied by a power source. These modes may distinguish between different power sources (e.g., primary, secondary, backup power source or none) being applied to a cryptographic module.
Power On/Off state	State related to the Power On/Off mode in the Finite state model (cf. ADV_ARC.1).
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.
Public key certificate	A set of data that uniquely identifies an entity, contains the entity's public key, and is digitally signed by a trusted party, thereby binding the public key to the entity.
Random Number Generator	Random Number Generators (RNGs) used for cryptographic applications produce a sequence of zero and one bits that may be combined into sub-sequences or blocks of random numbers. There are three basic classes physical true RNG, non-physical true RNG, and deterministic RNG. A physical true RNG produces output that dependents on some physical random source inside the TOE boundary only. A non-deterministic true RNG gets its entropy from sources from outside the TOE boundary (e.g., by system data like RAM data or system time of a PC, output of API functions etc. or human interaction like key strokes, mouse movement etc.). A deterministic RNG consists of an algorithm that produces a sequence of bits from an initial random value (seed).
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.
Removable cover	A cover designed to permit physical access to the contents of a cryptographic module.
Reset	Action to clear any pending errors or events and to bring a system to normal condition or initial state (e.g., after power-up).

Term	PP CM (all security levels)
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.
Seed key	A secret value used to initialize a cryptographic function or operation.
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.
Self-test state	State related to the Self-test mode in the Finite state model (cf. ADV_ARC.1).
Shutdown	Shutdown of the TOE initiated by the user (may not include reset after detection of error or power-off due to loss of power supply).
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.
Signature-creation key	Private key for the creation of digital signatures
Signature-verification key	Public key for the verification of digital signatures
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.
Software	The programs and data components, usually stored on erasable media (e.g., disk), that can be dynamically written and modified during execution.
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.
Status information	Information that is output from a cryptographic module for the purposes of indicating certain operational characteristics or modes of the module.
Status output interface/ port	Interface respective port intended for 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

Term	PP CM (all security levels)
	of a cryptographic module.
System software	The special software within the cryptographic boundary (e.g., operating system, compilers or utility programs) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, and associated programs, and data.
Tamper detection	The automatic determination by a cryptographic module that an attempt has been made to compromise the physical security of the module.
Tamper evidence	The external indication that an attempt has been made to compromise the physical security of a cryptographic module. (The evidence of the tamper attempt should be observable by an user subsequent to the attempt.)
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.
TEMPEST	A name referring to the investigation, study, and control of unintentional compromising emanations from telecommunications and automated information systems equipment. Note, TEMPEST is not limited to electromagnetic emanation.
Template Attack	Multivariate side channel analysis of the power or electromagnetic emission from a device, equipment, or system to gain information about its internal secrets or processes.
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.
Trusted channel	A means by which a TSF and a remote trusted IT product can communicate with necessary confidence to support the TSP.
Trusted path	A means by which a user and a TSF can communicate with necessary confidence to support the TSP.
Unauthenticated User	An identified user not being authenticated and having rights as identified in the component FIA_UAU.1.

Term	**PP CM (all security levels)**
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
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE (includes both authorized and unauthorized entities).
User Mode	Mode of operation in which the cryptographic module performs security services, cryptographic operations, and other functions at the request of the authorised user.
User State	State related to the User mode in the Finite state model (cf. ADV_ARC.1).
Verification authentication data	Data provided by an entity in an authentication attempt to prove their identity to the TOE.

8.2 Acronyms

Acronym	Term
A.xxx	Assumption
CC	Common Criteria
CSP	Critical Security Parameter
n.a.	Not applicable
O.xxx	Security objective for the TOE
OE.xxx	Security objective for the TOE environment
OSP	Organisational security policy
SAR	Security assurance requirements
SFR	Security functional requirement
T.xxx	Threat
TOE	Target of Evaluation
TSF	TOE security functionality

9 Literature

Common Criteria

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and General Model, Version 3.1, Revision 1, September 2006, CCMB-2006-09-001

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security Functional Requirements, Version 3.1, Revision 2, September 2007, CCMB-2007-09-002

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security Assurance Requirements, Version 3.1, Revision 2, September 2007, CCMB-2007-09-003

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 2, September 2007, CCMB-2007-09-004

Cryptography

[5] ISO/IEC 14888-3: Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms, 1999

[6] NIST: FIPS PUB 186-2 Digital signature standard (DSS), 2000 January 27 with Change Notice 1, October 2001

10 Annex

10.1 Backup (informal)

This chapter describes additional security problem definition, security objectives and security functional requirements for back-up. The ST writer may use this information in case the TOE supports back-up.

10.1.1 Security Problem Definition

A.Data_Store *Storage and Handling of TOE data*

The TOE environment ensures the confidentiality, integrity and availability of their security relevant data for TOE initialisation, start-up and operation if stored or handled outside the TOE. The TOE environment ensures the availability of the backup data.

Examples of the TOE data are verification authentication data, cryptographic key material and documentation of TOE configuration data.

T.Malfunction *Malfunction of TOE*
Internal malfunction of TOE functions may result in the modification of keys and CSP, misuse of TOE services, disclosure or distortion of TOE or denial of service for authorised users. This includes the destruction of the TOE as well as hardware failures which prevent the TOE from performing its services. This includes also the destruction of the TOE by deliberate action or environmental failure. Technical failure may result in an insecure operational mode violating the integrity and availability of the TOE services.

T.Insecure_Init *Insecure Initialisation of the TOE*
Unauthorised personnel or authorised personnel without using adequate organisational controls may initialise the TOE with insecure system data, management data or user data. An attacker may manipulate the backup data to initialise the TOE insecurely by the restore procedure.

T.Compromise_Backup *Compromise of backup data*
An attacker may have access to the backup data to compromise confidential cryptographic keys, CSPs and TSF data and use this knowledge to compromise the confidentiality and integrity of user data protected under these secondary assets.

Securtiy objectives for the TOE

O.Protect_Exported_Data *Protection of Data Exported by the TOE*

The TOE shall apply integrity and confidentiality protection mechanisms to all assets requiring integrity or confidentiality protection when they are exported from the TOE or imported into the TOE for the purpose of backup and restore. Operations for backup and restore shall be performed under dual personal control and audited where the audit data shall associate these events with the identity of the users.

Security objectives for the TOE environment

OE.Recovery Secure Recovery in Case of Major Failure

Recovery plans and procedures shall exist that allow a secure and timely recovery in the case of a major problem with the TOE (i.e. if TOE is blocked in its secure state after a failure, service discontinuity or detected physical tampering). These procedures shall ensure that the confidentiality and integrity of security relevant data for TOE initialisation, start-up and operation are maintained and that the recovery does not result in a situation that allows personnel to extend the TOE services they are allowed to use.

10.1.1.1 Extension of Class FDP with Family FDP_BKP

The TOE supports backup of cryptographic keys, CSP, other user data and TSF data to restore the operational mode of the same crypto module or for a new crypto module in the event of a system failure or other serious error. The export, import and protection of the backup data are combined in a specific way. The TOE ensures the confidentiality of the backup data and detects loss of the integrity of the backup data. The availability of the backup data will be ensured by the TOE environment.

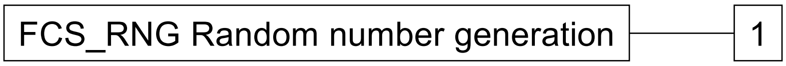
This component is necessary to specify a unique requirement of certificate issuing and management components that is not addressed by the Common Criteria. The specific requirements address the protection of cryptographic keys, key components, CSP and TSF data for backup and recovery.

Backup and recovery (FDP_BKP)

Family behavior

This family defines export and import of the backup data. The TOE ensures the confidentiality of the backup data and detects loss of the integrity of the backup data. The availability of the backup data will be ensured by the TOE environment.

Component leveling:


FCS_RNG Random number generation

1

FDP_BKP.1 Backup and recovery provides export, import and protection of the backup data.

Management: FDP_BKP.1

There are no management activities foreseen.

Audit: FDP_BKP.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Use of the backup function,

b) Use of the recovery function,

c) Unsuccessful recovery because of detection of modification of the backup data.

FDP_BKP.1 Backup and recovery

Hierarchical to: No other components.

Dependencies: [FCS_CKM.1 Cryptographic key generation or

FCS_CKM.2 Cryptographic key distribution or
FDP_ITC.1 Import of user data without security attributes]
FCS_COP.1 Cryptographic operation

FDP_BKP.1.1 The TSF shall be capable of invoking the backup function on demand.

FDP_BKP.1.2 The data stored in the backup shall be sufficient to recreate the state of the TOE at the time the backup was created using only: (1) a copy of the same version of the TOE as was used to create the backup data; (2) a stored copy of the backup data; (3) the cryptographic key(s) needed to decrypt the backup data; (4) the cryptographic key(s) needed to verify the cryptographic checksum of the backup data.

FDP_BKP.1.3 The TSF shall include a recovery function that is able to restore the state of the TOE from a backup.

FDP_BKP.1.4 The cryptographic keys, other critical security parameters and other confidential backup data shall be exported in encrypted form only.

FDP_BKP.1.5 The backup data shall be checked for modification through the use of cryptographic checksums. Modified backup data shall not be used for recovery.

10.1.2 Security Functional Requirements for TOE supporting Back-up

FCS_COP.1/Backup_Enc Cryptographic operation – Encryption of Backup data

Hierarchical to: No other components.

Dependencies: [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
MT_MSA.2 Secure security attributes

FCS_COP.1.1/Backup_Enc The TSF shall perform *encryption and decryption*[103] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of* ***Endorsed*** *standards*].

FCS_COP.1/Backup_Int Cryptographic operation – Backup Integrity protection

Hierarchical to: No other components.

Dependencies: [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
MT_MSA.2 Secure security attributes

FCS_COP.1.1/Backup_Int The TSF shall perform *calculation and verification of cryptographic checksums*[104] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following:

[103] [assignment: *list of cryptographic operations*]

[104] [assignment: *list of cryptographic operations*]

[assignment: *list of* ***Endorsed*** *standards*].

Application note 38: The standards for encryption, decryption, calculation and verification of cryptographic checksums shall be assigned from the list of endorsed algorithms only.

FDP_ACC.2/Backup Complete access control

Hierarchical to: FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.2.1/Backup The TSF shall enforce the *Backup SFP*[105] on

(1) Subjects: Crypto officer, Administrator

(2) *Objects: cryptographic keys, CSPs, backup data, backup key components* [106]

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

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

FDP_ACF.1/Backup Security attribute based access control - Backup

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/Backup The TSF shall enforce the *Backup SFP*[107] to objects based on the following:

(1) *Subjects with the security attributes: Identity of the user the subject is bind to, Role of this user;*

(2) *Objects with the security attributes: none*[108]..

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

(1) *Crypto officer under dual person control of another user in the Crypto officer role or Administrator role is allowed (a) to backup cryptographic keys, CSP and backup data (FDP_BKP.1), (b) to restore cryptographic keys, CSP and backup data (FDP_BKP.1),*

(2) *Crypto officers are allowed to enter backup key components (FCS_CKM.2/Import)* [109].

FDP_ACF.1.3/Backup The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes that explicitly authorise access of subjects to objects*].

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

(1) *no role is allowed without dual control of an Crypto officer (a) to*

[105] [assignment: *access control SFP*]

[106] [assignment: *list of subjects and objects*]

[107] [assignment: *access control SFP*]

[108] [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*]

[109] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

backup cryptographic keys, CSP and backup data (FDP_BKP.1), (b) to restore cryptographic keys, CSP and backup data (FDP_BKP.1),

(2) *any other role than Crypto officer is not allowed to import a backup key component (FCS_CKM.2)* [110]*.*

Application note 39: "Dual person control" requires at least two subjects bind to two different users authenticated for the required role authorized to perform the required actions. One of them shall be an authorized Crypto officer. FCS_CKM.2/Import enforces requirement for manually-entered key components similar to dual control: the Crypto officers are allowed to import only one of at least two key components but import of these key components may be performed in different points of time.

[110] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

10.1.3 Backup and recovery (FDP_BKP.1)

FDP_BKP.1 Backup and recovery

Hierarchical to: No other components.

Dependencies: [FCS_CKM.1 Cryptographic key generation or
FCS_CKM.2 Cryptographic key distribution or
FDP_ITC.1 Import of user data without security attributes]
FCS_COP.1 Cryptographic operation

FDP_BKP.1.1 The TSF shall be capable of invoking the backup function on demand.

FDP_BKP.1.2 The data stored in the backup shall be sufficient to recreate the state of the TOE at the time the backup was created using only:

(1) a copy of the same version of the TOE as was used to create the backup data;

(2) a stored copy of the backup data;

(3) the cryptographic key(s) needed to decrypt the backup data;

(4) the cryptographic key(s) needed to verify the cryptographic checksum of the backup data.

FDP_BKP.1.3 The TSF shall include a recovery function that is able to restore the state of the TOE from a backup.

FDP_BKP.1.4 The cryptographic keys, other critical security parameters and other confidential backup data shall be exported in encrypted form only.

FDP_BKP.1.5 The backup data shall be checked for modification through the use of cryptographic checksums. Modified backup data shall not be used for recovery.

10.1.4 Audit

The ST writer shall extend the list of auditable events in the SFR element FAU_GEN.1.1 with the events

c.12) back-up of cryptographic keys, CSP and backup data (FDP_BKP.1),

c.13) restore of cryptographic keys, CSP and backup data (FDP_BKP.1).

Note the import of backup key components is already defined as auditable event c.5) in the SFR element FAU_GEN.1.1. The TOE associate the audit data of these events with the identity of the users as required in the SFR element FAU_GEN.1.2.

10.1.5 Rationale

The following thoughts may help the ST writer to provide rationale for the security objectives and the security functional requirements.

The assumption **A.Data_Store "**Storage and Handling of TOE data" is covered by the security objective for the environment OE.Recovery "Secure Recovery in Case of Major Failure", second sentence.

The threat **T.Malfunction** “Malfunction of TOE” is covered by adequate reaction in case of malfunction based on security mechanisms of the TOE required by O.Protect_Exported_Data “Protection of Data Exported by the TOE” and implemented by organisational security measures required by security objective for the environment OE.Recovery “Secure Recovery in Case of Major Failure”.

The threat **T.Insecure_Init** “Insecure Initialisation of the TOE” is covered by the security objectives for the TOE O.Protect_Exported_Data “Protection of Data Exported by the TOE” (cf. dual personal control) together with O.I&A “Identification and authentication of users”, O.Roles “Roles known to TOE”, and for the environment OE.Recovery “Secure Recovery in Case of Major Failure” and OE.Personal “Personal security”

The threat **T.Compromise_Backup** “Compromise of backup data “ is prevented by the security objective O.Protect_Exported_Data “Protection of Data Exported by the TOE” requiring protection of the confidentiality and integrity of the backup data and audit of .the Operations for backup and restore.

All SFR FCS_COP.1/Backup_Enc, FCS_COP.1/Backup_Int, FDP_ACC.2/Backup, FDP_ACF.1/Backup and FDP_BKP.1 Backup and recovery are mapped to the security object O.Protect_Exported_Data “Protection of Data Exported by the TOE”. Further more FAU_GEN.1 (with the addition described above) contributes to O.Protect_Exported_Data.

The following table provides the Dependency Rationale:

SFR	**Dependencies**	**Support of the Dependencies**
FCS_COP.1/Backup_Enc	[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, FCS_CKM.4
FCS_COP.1/Backup_Int	[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, FCS_CKM.4
FDP_ACC.2/Backup	FDP_ACF.1 Security attribute based access control	FDP_ACF.1/Backup
FDP_ACF.1/Backup	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.2/Backup FMT_MSA.3

SFR	Dependencies	Support of the Dependencies
FDP_BKP.1	FCS_CKM.1 Cryptographic key generation or FCS_CKM.2 Cryptographic key distribution or FDP_ITC.1 Import of user data without security attributes] FCS_COP.1 Cryptographic operation	FCS_CKM.1, FCS_CKM.2/Import, FCS_CKM.2/Export, FDP_ITC.2, FCS_COP.1/Backup_Int, FCS_COP.1/Backup_Enc